SMART RESILIENCE INDICATORS FOR SMART CRITICAL INFRASTRUCTURES

Initial Framework for Resilience Assessment

Report Title:	Initial Framework for Resilience Assessment		
Author(s):	Maike Vollmer (Fraunhofer INT), Gerald Walther (Fraunhofer INT), Aleksandar Jovanović (EU-VRi), Nicolas Schmid (R-Tech) Knut Øien (SINTEF), Tor Olav Grøtan (SINTEF), Amrita Choudhary (USTUTT), Roswitha Kokejl (USTUTT), Katarina Buhr (IVL), Anja Karlsson (IVL), Rainer Egloff (SwissRe)		
Responsible Project Partner:	Fraunhofer INT	Contributing Project Partners:	Fraunhofer INT, SINTEF, IVL, EU-VRi, USTUTT, SwissRe, R-Tech

Document data:	File name (QMS compliant):	D1 1 Initial Framework_v18jk29072016		
	Pages:	52	No. of annexes:	1
	Status:	Final	Dissemination level:	PU/CO
Project title:	SmartResilience: Smart Resilience Indicators for Smart Critical Infrastructures		GA No.:	700621
			Project No.:	12135
WP title:	Establishing the project baseline and the common framework		Deliverable No:	D1.1
Date:	Due date:	July, 2016	Submission date:	July 29, 2016
Keywords:	Resilience, definition, concept, framework			
Reviewed by:	Thomas Knape, IAI		Review date:	July 8, 2016
	Dr. Miloš Jovanović, Fraunhofer INT		Review date:	July 8, 2016
Approved by Coordinator (EU-VRi):	Prof. Dr. Aleksandar Jovanović		Approval date:	July 29, 2016

Euskirchen, July 2016

 The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under the Grant Agreement No 700621.

Project Contact

EU-VRi – European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart, Germany
Visiting/Mailing address: Lange Str. 54, 70174 Stuttgart, Germany
Tel: +49 711 410041 27, Fax: +49 711 410041 24 – www.eu-vri.eu – info@eu-vri.eu
Registered in Stuttgart, Germany under HRA 720578

SmartResilience Project

Modern critical infrastructures are becoming increasingly smarter (e.g. the smart cities). Making the infrastructures smarter usually means making them smarter in the normal operation and use: more adaptive, more intelligent etc. But will these smart critical infrastructures (SCIs) behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI as its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) which one has to look at?

These are the main questions tackled by SmartResilience project. The project envisages answering the above questions in several steps by:

- identifying existing indicators suitable for assessing resilience of SCIs
- identifying new smart resilience indicators including those from Big Data
- developing a new advanced resilience assessment methodology based on smart RIs and the "resilience in cube (the innovative project tool providing the possibility to define one compound resilience indicator), including the resilience matrix
- developing the interactive SCI Dashboard tool
- applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study. The SCIs considered (in 8 European countries!) deal with energy, transportation, health, and water.

This approach will allow benchmarking the best-practice solutions and identifying the early warnings, improving resilience of SCIs against new threats and cascading and ripple effects. The benefits/savings to be achieved by the project will be assessed by the reinsurance company participant. The consortium involves seven leading end-users/industries in the area, seven leading research organizations, supported by academia and lead by a dedicated European organization. External world leading resilience experts will be included in the Advisory Board.

Executive Summary

This report is targeting a framing of what SmartResilience actually wants to measure – "resilience" –, taking relevant research results and existing guidelines and standards into account. This is especially challenging due to the vast variety of understandings, definitions, concepts, and applications of the term, including usages in different research areas or fields of application. In addition, for the reason of this variety, a huge number of articles and reports discussing the term, its understandings and usages on a theoretical basis have been developed. Even several comprehensive reviews on the term, including qualitative and quantitative literature analyses as well as expert interviews, have already been conducted.

SmartResilience starts with an initial concept of (critical infrastructure) resilience, which was already defined in the proposal phase of the project. Up-to-date comprehensive reviews on definitions and concepts of resilience, including critical infrastructure resilience, have been available from recent results prepared in the framework of projects that answer to the call topic EU H2020 DRS-07-2014 "Crises and disaster resilience – operationalizing resilience concepts". The resulting reports have been reviewed, identifying results that seem useful for the SmartResilience resilience definition and concept. Reviewing approaches and identifying aspects that seem useful for SmartResilience from selected additional sources (international and US organisations, industry, standards) complemented the basis for framing the (still initial) SmartResilience resilience definition and concept.

The initial definition has only slightly been changed, resulting in:

Resilience of an infrastructure is the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption.

However, the concept of resilience in a broader sense (including further framing questions such as resilience "of what" is in focus, what is the relation to vulnerability or risk management, how should the different levels and components of resilience be categorised) has been complemented, and slightly changed. Several aspects that were concluded based on the reviews, are described in this report as issues to be considered and decided on when working on the actual methodology (WP3), and/ or its application to specific SCI's (WP2, WP5). This includes questions such as if a "transformative" character should be included as a main component of resilience, or if "ability" and "capacity" should be distinguished, but also what to consider when identifying relevant issues for the resilience of specific SCI's.

As further instrument for creating and maintaining a common understanding, a first version of a glossary of terms that are relevant for SmartResilience has been developed, is online accessible, and will be continuously updated throughout the project.

Table of Contents

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
BBK	German Federal Office of Civil Protection and Disaster Assistance
BMI	German Federal Ministry of the Interior
CI	Critical infrastructure
CIR	Critical infrastructure resilience
CRO	Chief Risk Officer
FEMA	Federal Emergency Management Agency
ISO	International Organization for Standardization
LÜKEX	Interministerial and Interstate Crisis Management Exercise
OECD	Organisation for Economic Co-operation and Development
SAG- S	Strategic Advisory Group on Security
SCI	Smart Critical Infrastructure
SFI	Strategic Foresight Initiative
STEEP	Social, Technological, Economic, Environmental and Political
UNISDR	United Nations Office for Disaster Risk Reduction
USDHS	United States Department of Homeland Security

1 Introduction

SmartResilience is targeting an advanced methodology to analyse the resilience of smart critical infrastructures, and to apply this methodology using (smart) indicators, which as one of the first steps requires a robust frame regarding terminology and concept. This is especially true considering the amount and variety of usages of the term "resilience", different concepts, including different attributes of resilience, and different views on the relation to other terms such as risk or vulnerability. A common understanding is even more challenging due to the variety of stakeholders, regarding the addressees of SmartResilience, but even within the project's consortium. Thus, this report derives the SmartResilience initial framework for resilience assessment.

An initial definition and concept of resilience to be applied in the project has already been described in the proposal phase, which is now revisited. Comprehensive reviews on resilience, its concepts and different usages, have recently been conducted by projects that answer to the call topic EU H2020 DRS-07-2014 "Crises and disaster resilience – operationalizing resilience concepts". SmartResilience is not repeating such a review, but is evaluating the results on their usability for SmartResilience. Even though these reviews should already cover all relevant types of sources, approaches of selected organisations, which are considered most relevant in this context, are analysed separately, in order to make sure that they are included appropriately. Based on the revisited initial definition and concept, together with the evaluated results of the reviews conducted within the DRS-07-2014 projects, as well as approaches of main organisations, a concept of resilience for the SmartResilience project is derived.

The definitions of resilience, risk, vulnerability, and many other terms relevant for SmartResilience, are stored in a glossary, accessible in the member area of the SmartResilience website (http://www.smartresilience.eu-vri.eu/). Within task 1.1, initial definitions are derived, which might be adapted in the further work of the project. WP3 (where the methodology is being developed) will start with the adapted concept of resilience presented in this report and the corresponding working definition of resilience; however, the definition of resilience and other terms may still evolve during the project. This means that work performed in WP3 may lead to further adjustments of the concept and definition of resilience. However, even if terms may change during the course of the project, we need a common understanding of basic terms from the start of the project, even if they are further developed and perhaps not finalized before the very end of the project. The development of the initial glossary is led by the project's coordinator, who will also take care of required adaptations in the further course of the project and ensure that the definitions are actively used in the project.

From this background, chapter 2 in this report comprises the review results of existing definitions and concepts of resilience (the initial definition and concept from the project's proposal; the results from reviews conducted within ongoing EU projects; definitions and concepts from selected relevant organisations), and how the results could be exploited for SmartResilience. In chapter 3, developed based on the results of chapter 2, the different dimensions of resilience, and the relation to the concepts of vulnerability and risk management are derived. Several further framing issues, which were identified during the reviews, are described, and the dynamic SmartResilience glossary is introduced. Chapter 4 concludes on the changes and further development of the initial definition and concept of resilience, as well as on some further implications for upcoming work in the project.

2 Review of resilience definitions and concepts

2.1 Approach and scope

As explained above, the concept of resilience for SmartResilience (chapter 3) will be based on reviews of existing work, which can be assigned to three different groups:

The preliminary definition and concept as used in the proposal is revisited in chapter 2.2, with a stronger view on the project's specific needs, following the further developed understanding of the project.

Ongoing EU H2020 projects funded under the call topic DRS-07-2014, running between May 2015 and May 2018, namely IMPROVER, DARWIN, RESILENS, RESOLUTE, and SMR, have as part of their basic working steps, recently conducted reviews on the term resilience. This includes comprehensive quantitative and qualitative literature reviews as well as expert interviews on the term resilience in general, and partly in the context of critical infrastructure. Their results are reviewed in chapter 2.3, presenting summaries of findings that seem relevant for the SmartResilience resilience definition & concept.

In order to assure that approaches from institutions are appropriately covered, which are considered most relevant by the (interdisciplinary) authors of this report, these approaches are reviewed in chapter 2.4. The selection of sources/ organisations is based on the assumption that besides the EU perspective, the SmartResilience approach should consider major international organisations (UN, OECD), the US perspective, the industry perspective, as well as already established standards. The EU perspective is covered by the reviews conducted within the EU H2020 projects named above. Especially the IMPROVER project directly addresses the EU perspective of critical infrastructure resilience, which is summarized in chapter 2.3.1. The UNISDR's definition of resilience is a definition most used in the field of disaster risk reduction, and OECD has developed resilience guidelines, of which several aspects appear very useful for SmartResilience, as explained in chapters 2.4.2 and chapter 3. For the US, the main US organisation of emergency management (FEMA) was chosen. The review of standards complements the review of additional sources in chapter 2.4. Also in this chapter, summaries of the different approaches are presented, followed by conclusions on what is useful/ not useful for the definition and concept of resilience in SmartResilience.

Definitions of terms used in the reviewed approaches will also enrich the SmartResilience glossary, which is introduced within chapter 3.

2.2 Preliminary definition & concept of resilience

The preliminary definition used in the SmartResilience project proposal is:

Resilience of an infrastructure is the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption (adapted from [37])

Resilience management goes beyond risk management to address the complexities of large integrated systems and the uncertainty of future threats, as it includes risk analysis as a central component[1]. Risk analysis depends on characterization of the threats, vulnerabilities and consequences of adverse events to determine the expected loss of critical functionality [37]).

[1] This understanding is changed later for SmartResilience as explained in chapter 3.2, assuming that resilience *builds on* risk analysis, rather than including it.

In the resilience management framework (refer Figure 1), risk in a system is interpreted as the total reduction in critical functionality and the resilience of the system is related to the slope of the absorption curve and the shape of the recovery curve — indicating the temporal effect of the adverse event on the system. The dashed line suggests that highly resilient systems can adapt in such a way that the functionality of the system may improve with respect to the initial performance, enhancing the system's resilience to future adverse events and the concept of resilience stresses upon these aspects.

The understanding of resilience was illustrated in the proposal (Figure 3, p. 11) using a U-curve in a system functionality versus time axis system. This illustration was rather opaque, and we will present the concept somewhat more gradually in the following part.

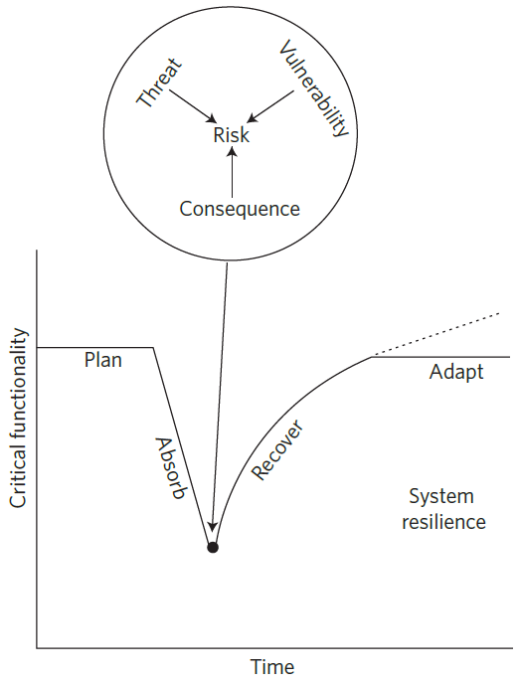

Figure 1: A resilience management framework [37]

The term resilience has been used in several disciplines before it entered the safety area rather recently. In mechanics, for example, it appeared as early as 1858. Several scientific disciplines characterise the functionality as a more or less smooth V-curve or U-curve. This has also been done within critical infrastructure resilience, as shown in Figure 2.

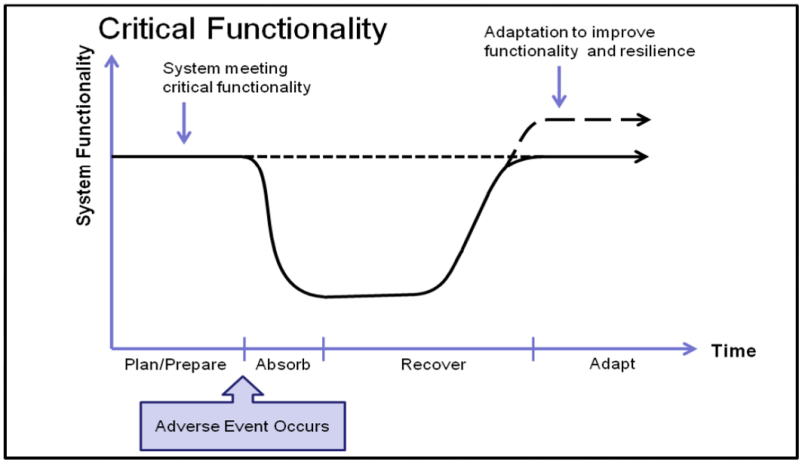

Figure 2: Critical infrastructure system functionality curve [37]

In some of the disciplines, particular attention is paid to the curve itself, e.g. the steepness of the absorption curve or the slope of the recover curve.

In SmartResilience, this curve is not of main interest as a measure of resilience. Resilience is measured indirectly through the status of the resilience dimensions/phases using resilience indicators. In addition, the four resilience dimensions/phases in Figure 2 (plan/prepare, absorb, recover and adapt) have been extended to seven resilience dimensions/phases. (Figure 3 already includes an additional (as compared to the proposal) eighth resilience dimension – risk understanding.)

Finally, in SmartResilience, we focus on smart functionality, not just any system functionality; thus, the functionality axis is adjusted accordingly. This is illustrated in Figure 3.

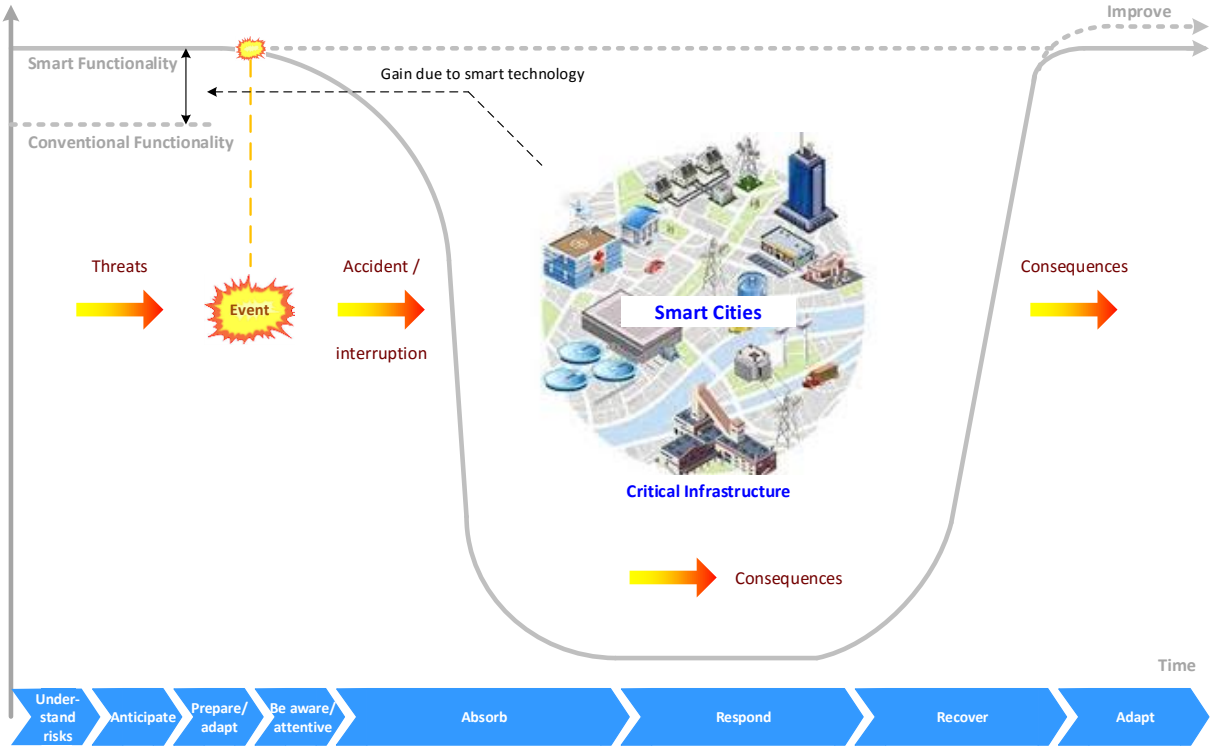

Figure 3: System functionality curve for smart critical infrastructures (smart functionality)

Figure 3 illustrates that smart critical infrastructures may increase the system functionality (from conventional to smart functionality), but at the same time the smart technology may increase the vulnerability of the infrastructure system. This is indicated in Figure 4.

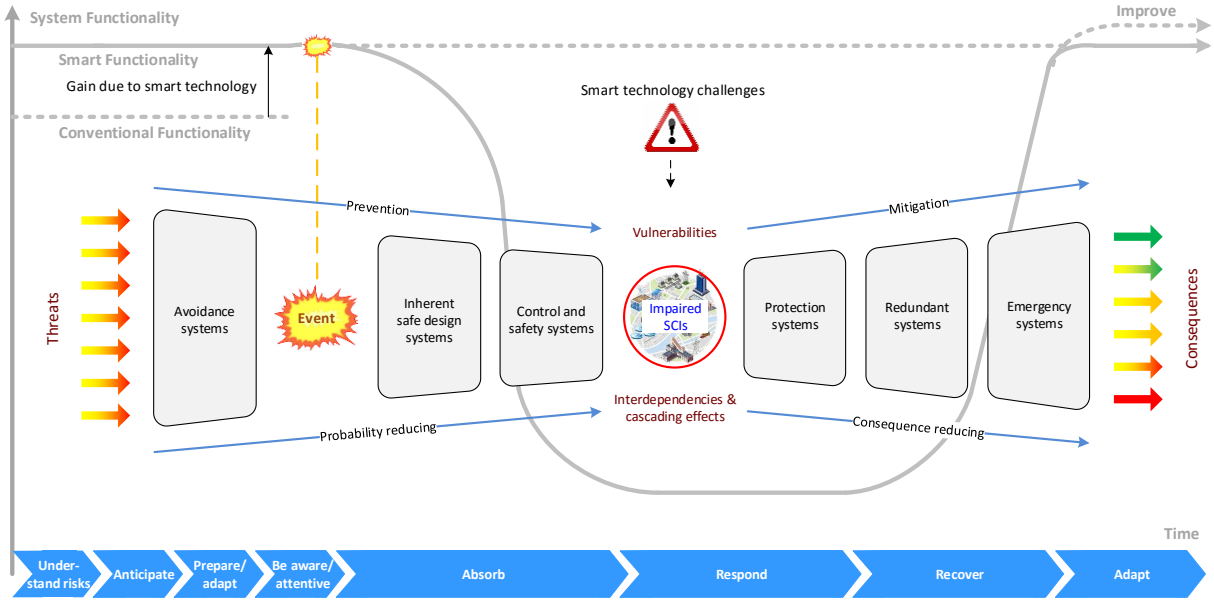

Figure 4: Smart functionality and smart technology vulnerabilities

Figure 4 also provides a brief overview of general types of barrier systems contributing to the resilience of the (smart) critical infrastructures. Increased vulnerability due to smart technology can manifest in either increased propensity for failures/events or less reliable barriers, both leading to reduced functionality.

The U-curve in Figure 4 is a simplified conceptual curve that is representative for a single event/disruption affecting a single critical infrastructure. Since many critical infrastructures in general and smart critical infrastructures in particular, are interconnected, these systems also need to be resilient with respect to interdependencies and cascading effects. This is indicated in Figure 4, but it is not represented by the single U-curve.

A second critical infrastructure being affected, will have the phases displaced compared to the first affected infrastructure, e.g. the absorption phase of the second may coincide with the response phase of the first. In addition, if the functionality axis represents the total functionality of several critical infrastructures, then the absorb curve will not be a straight downward slope, but it will have several "steps" or "plateaus" on its way to the bottom of the curve. This is not easily represented by a single U-curve, and it is one reason why the curve itself will not be used for the measuring of resilience.

To measure resilience we use indirect indicators measuring the resilience dimensions/phases through “issues”, not direct measures of the curve or slope of functionality.

A final comment to Figure 4 is that the U-curve visualises consequences in terms of loss of functionality. In addition, the disruptive event may lead to other consequences not visualised, e.g. loss of lives. As an example, a terrorist attack on a subway may lead to immediate deaths and injuries, and destruction of the subway leading to loss of subway transportation for a certain period. Only the latter is reflected by the U-curve.

Figure 5 shows the SmartResilience concept as illustrated in the proposal. The "infographics" in Figure 5 is an attempt to provide a complete overview of the technical part of the work in the project, i.e. excluding the "administrative" WPs (WP6 and WP7). It is somewhat "overloaded" and we will not go into details. It is included here, since it was part of the proposal.

WP1 is amongst others related to the clarification of the definition and concept of resilience, as illustrated in the upper part of Figure 5.

It should be noticed, as mentioned above, that *risk understanding* has been added as an eighth resilience attribute, as a preparation for the project’s kick-off meeting. Arguments for this can be found in chapter 2.4.2.

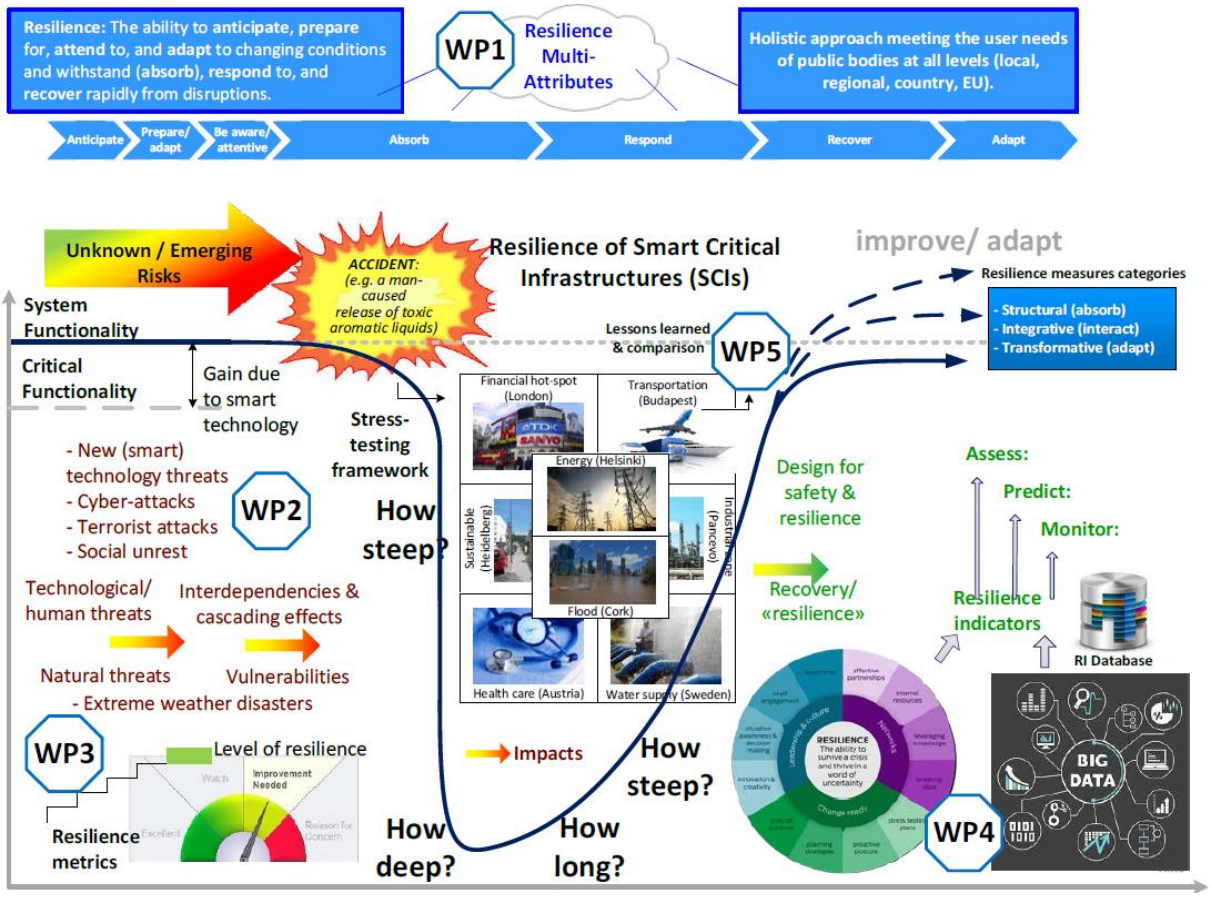

Figure 5: The SmartResilience concept (Figure 3, p.11 in proposal)

2.3 Reviews conducted under current EU H2020 projects

2.3.1 Review conducted within the IMPROVER project

2.3.1.1 IMPROVER

The project *Improved risk evaluation and implementation of resilience concepts to critical infrastructure – IMPROVER* (June 2015 – Mai 2018) is developing a European Resilience Management Guideline, and will demonstrate the Guideline through pilot implementation. IMPROVER aims to improve European critical infrastructure resilience to crises and disasters through the implementation of resilience concepts to real life examples. The improvement shall arise through the development of a methodology for implementing combinations of societal, organisational and technological resilience concepts to critical infrastructure based on risk evaluation techniques and informed by a review of the positive impact of different resilience concepts on critical infrastructure.[2]

2.3.1.2 IMPROVER's review process

As a basic deliverable of IMPROVER, the project developed a report "International Survey" (D1.1, [38]), providing an overview of the existing scientific literature regarding the concept of resilience, focusing on critical infrastructure resilience. It also comprises information on the definitions and implementation of the concepts of resilience in different countries and continents. In order to achieve the envisaged information, an extensive literature review was conducted, a workshop was held, and personal interviews with critical

[2] http://improverproject.eu/discover/, accessed July 19, 2016

infrastructure operators and resilience experts in Europe were conducted. The report elaborates on different aspects of the concept of resilience in general, of community resilience, of critical infrastructure resilience, and describes results of the case studies in different continents. Currently available and used here is the version delivered in May 2016 (not yet formally accepted) [38].

2.3.1.3 Main findings of IMPROVER's review relevant for this report

Findings from the IMPROVER "International Survey", which seem relevant for this report, are the following:

Resilience in most cases is either understood as the ability to ***bounce back,*** or to ***adapt***. While bouncing back means to return quickly after a shock to the pre-defined state, adaptation means a change of the entity or system, while providing the same service or filling the same operational niche as before [38].

Regarding the **relation of resilience to vulnerability**, there are different understandings, mainly as a result of different definitions of the two terms. Key parameters of vulnerability are seen in the exposure, susceptibility, and coping/ adaptive capacity of elements. Often discussed is the question, if the resilience and vulnerability should be treated as positive and negative poles on the same continuum, or as two completely different concepts. Some authors follow the first approach, amongst others concluding that vulnerability of a system results from reduced resilience. However, other authors see an overlap between the two concepts, assuming that many characteristics influence only the vulnerability or only the resilience of a system, while other characteristics influence both [38].

Regarding the **relation of resilience to risk management**, three different perspectives (in policies on critical infrastructure protection, identified by Suter [44]) are named: Resilience as *the new goal of risk management*, resilience as *an alternative to risk management*, and resilience as *part of risk management* ([44], [38]).

The IMPROVER report also elaborates on the relation betweem **concepts for critical infrastructure resilience** and other resilience concepts.

While there are not many national, official definitions of a concept of critical infrastructure resilience, several national policy and strategy reports include resilience as a key component in their critical infrastructure protection programs. But even for critical infrastructure, there is no commonly accepted definition. (The Council Directive 2008/114/EC defines it as *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."* [8])

Definitions of resilience in the context of critical infrastructure have evolved from resilience definitions in other fields, and include similar attributes. However, following Australia's 2010 Critical Infrastructure Resilience Strategy, resilience in the context of critical infrastructure refers to

- *"coordinated planning across sectors and networks,*
- *responsive, flexible and timely recovery measures, and*
- *the development of an organizational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly."* [1].

Especially the focus on "planning across sectors", and the "ability to provide a minimum level of service during interruptions", seem noteworthy, as compared to other definitions of resilience. However, the focus on performance, and acceptable level of inoperability, faces the problem of measurement – it can be measured for example by the amount of services delivered, the availability of critical facilities, or the number of people served, which refer to different dimensions of resilience ([41], cited in [38]). Besides approaches focusing on **performance**, also several approaches focusing on the **structure** or topology of a system were identified, which for example can include aspects of identifying critical nodes, or questions on centrality [38].

The two perspectives – performance and structure – have also been identified in another review (Francis & Bekera), cited in the IMPROVER report. Francis & Bekera argue that the objective of resilience is to retain predetermined dimensions of system performance and identity or structure in view of forecasted scenarios. *"Factors that affect resilience are robustness (ability to withstand a given level), resourcefulness (level of preparedness to effectively combat an adverse event), redundancy (degree of substitutability of elements of a system), rapidity (ability to return to normal operating capacity in a timely manner), interconnectedness, cross-functional stakeholders, anticipative capacity, stakeholders' cooperation, capacity to recognize threats,*

evaluation of the model used to obtain and retain competence, capacity to prepare for future protection efforts, and ability to reduce likely risks" ([17], cited in [38]).

Regarding the **relation of critical infrastructure resilience to other resilience concepts**, an approach of Labaka et al. is described, which seems relevant for SmartResilience: for events that start with failure in one critical infrastructure, and then due to interdependencies and cascading effects also affects other critical infrastructure, and the society, two types of resilience are defined: (a) the resilience level of the CI where the triggering event occurs (internal resilience) and (b) the resilience level of the rest of the external involved agents (external resilience). They further propose a framework of critical infrastructure resilience, which links critical infrastructure resilience to several resilience concepts, i.e. technical resilience, organisational resilience, economic resilience and ultimately social resilience ([36], cited in [38]).

A further link between critical infrastructure resilience and community resilience is seen in the sense that following a disaster, the needs of a community are likely to change, which can also place new demands on infrastructure services. This can concern for example new locations to meet and socialize, when the common facilities are destroyed [38].

In principle, proved by personal interviews with critical infrastructure operators in Europe, it is found that resilience is not a well-established concept in the context of critical infrastructure, but that it is rather measured through other concepts or attributes [38].

The IMPROVER D1.1 further comprises an elaboration of "**critical infrastructure resilience as a concept and practice in the European context**". While no policy could be found that directly addresses critical infrastructure resilience, the issue has been indirectly addressed through other concepts such as critical infrastructure protection, civil protection and disaster risk management, as well as external development and humanitarian assistance. Similar, while there is no official EU-level definition of "critical infrastructure resilience", "critical infrastructure" is defined [8], and "resilience" in other contexts as well. Resilience in official EU documents in most cases refers to societal resilience. A document "EU Approach to Resilience: Learning from food crisis" provides the definition: "Resilience is the ability of an individual, a household, a community, a country or a region to withstand, to adapt, and to quickly recover from stresses and shocks" [9].

On national level, however, there are several definitions of critical infrastructure resilience. The ongoing FP7 project CIPRNet collected several definitions, available in an online source[3].

2.3.1.4 Conclusions for SmartResilience

The question on understanding resilience as "bouncing back" versus "adapt" shall be considered in the discussion of which dimensions to include in the definition and concept of resilience. The same accounts for the elaboration how resilience relates to other concepts such as vulnerability and risk management – both will be derived in chapter 3.

Even though main focus of this report is a definition and concept of resilience, also the investigations on concepts for critical infrastructure resilience are highly relevant, when applying the concept of resilience to smart critical infrastructure. The Australian definition of critical infrastructure resilience highlights a focus on "planning across sectors", and the "ability to provide a minimum level of service during interruptions", as compared to other definitions. It seems useful to consider the performance as well as structure perspective, when working on the interdependencies and cascading effects in the project. This will be taken up in chapter 3 as well. Also the relation of different types or concepts of resilience (e.g. critical infrastructure resilience – other resilience concepts) is relevant for the resilience concept in the broader sense (i.e. the framing question on "what" is in focus of resilience analysis).

The work in SmartResilience should respect the existing EU approaches, for which the IMPROVER investigations of critical infrastructure resilience as a concept and practice in the European context provide a

[3] https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Resilience, accessed July 28, 2016

useful frame. However, with regard to a definition and concept of (critical infrastructure) resilience, there seem to be no specific frameworks to follow.

2.3.2 Review conducted within the DARWIN project

2.3.2.1 DARWIN

The DARWIN project ("Expect the unexpected and know how to respond", running June 2015 – Mai 2018) is focused on improving responses to expected and unexpected crises affecting critical societal structures during natural and man-made disasters. The goal is to develop state of the art resilience guidelines and innovative training modules for crisis management aimed at all involved managers and operators in the context of crisis. This includes critical infrastructure managers, crisis and emergency response managers, service providers, first responders and policy makers.[4] An initial step of DARWIN was to conduct a systematic review of definitions and concepts of resilience.

2.3.2.2 DARWIN's review process

The DARWIN review, included in D1.1 "Consolidation of resilience concepts and practices for crisis management" [54], entailed two approaches. First, a systematic literature survey has been conducted on concepts and approaches to resilience from a range of disciplines, identifying associated indications of maturity of operationalisation or implementation into practice (for example, through guidelines and tools). This first iteration of the review generated 5560 hits and a subsequent one with altered search criteria reduced it to 1692. Eventually, a total of 440 articles were identified, which were then read in full and analysed by the project team.

Second, an interview study of relevant stakeholders involved in crisis management, identifying resilience and brittleness aspects from significant crises and everyday practices was carried out. These interviews were held with actors in the 'health care and emergency and crisis management' sectors as well as with 'air navigation service providers' [54].

2.3.2.3 Main findings of DARWIN's review relevant for this report

In the following, main findings of the DARWIN project, which seem relevant for SmartResilience, are summarized:

In the systematic literature review, 300 definitions of resilience were identified, representing a diversity of contexts, and differing in scope and components. As most common domains, **community resilience and ecological resilience** have been identified, but also a rise in dominance in additional domains, including infrastructure resilience. The emphasis and primacy of components differ among different contexts, however, some general characteristics could be identified. Regarding "what" is resilient, **system and community** were identified as the two major elements. Regarding the mechanism how to achieve resilience, **ability and capacity** constitute the most common terms. This is also reflected in the two major actions in receiving resilience – actions aimed at **adapting**, and actions aimed at **bouncing back**. Only few definitions include actions that are targeted to prevention. The phases encompassed in the definitions are diverse, indicating that the concept addresses **all periods of time**. The results of the literature review reveal that "researchers within the resilience domain put emphasis on the phases before and during the event when addressing needs and issues, and on both planning and responding when discussing solutions and practices". However, many of the identified solutions and practices address **information and communication**, **involvement and engagement of stakeholders** as well as **measuring or assessing resilience**. In addition, a few solutions and practices aim at improving **education and training** of personnel and other stakeholders.

Further, the different perspectives of **community resilience as opposed to practitioner resilience** (resilience of a specific organisation, with a specific purpose) is highlighted, while the interplay of both could play a crucial role in crisis situations. It has also been noticed that the interaction between resilience and other paradigms, including risk management, have often been investigated.

[4] http://www.h2020darwin.eu/, accessed July 28, 2016

The review further revealed that the general level of maturity of the approaches described in the literature is toward the lower half of the maturity spectrum, roughly between the concept and early demonstration stages [54].

2.3.2.4 Conclusions for SmartResilience

The identification of over 300 definitions of resilience symbolizes the significant challenge to proposing a single resilience definition that can be agreed on. DARWIN has identified several criteria to which a concept of resilience should pay attention. For example, several questions need to be answered: Is the focus on the phases before, during, and after a crisis or disruption? Is it a system or a community that is resilient, or both? Is resilience adapting to situations or bouncing back or are they mutually beneficial ideas? Do we predominantly focus on crisis management, planning and responding? What is the role of information and communication and the involvement of stakeholders? And how do we measure resilience?

One finding of DARWIN that is particularly noteworthy is the analysis of the technology readiness levels of concepts and theories to improve critical infrastructure resilience. The literature review has shown that in this area, the readiness level is in a very early stage. This should be considered in the further work of SmartResilience.

2.3.3 Review conducted within the RESILENS project

2.3.3.1 RESILENS

The project RESILENS – Realising European ReSILiencE for Critical INfraStructure (May 2015 – April 2018) aims to move resilience from a conceptual understanding to applied, operational measures that integrate best practice from the related realm of risk management and vulnerability assessment. It will develop a European Resilience Management Guideline to assist in the application of resilience to critical infrastructure. This work entails the production of a Resilience Management Matrix and Audit Toolkit with which quantitative and qualitative assessments of critical infrastructure systems can be conducted to determine their level of resilience. These tools will be tested on three different critical infrastructure platforms – transport, electricity and water [6].

2.3.3.2 Description of the RESILENS's review process

A first deliverable of RESILENS, D1.1 "Resilience Evaluation and SOTA Summary Report", comprises a review of the current state-of-the-art (SOTA) in risk management, resilience and its application to critical infrastructure (CI), and provides a working definition of critical infrastructure resilience (CIR), including the relationship between resilience and risk management practices. The results of the RESILIENS D1.1 are used in RESILENS to compare the SOTA with current practices (identified through stakeholder engagement), and identify respective gaps. In contrast to the quantitative literature search conducted in DARWIN, RESILENS draws its definition and understanding of resilience from a qualitative discussion of key literature [6].

2.3.3.3 Main findings of RESILENS's review relevant for this report

In terms of a common understanding of resilience, D1.1 succinctly lays out a **definition of resilience** for the project: *"Resilience is the ability of a system or systems to survive and thrive in the face of a complex, uncertain and ever-changing future. It is a way of thinking about both short term cycles and long term trends: minimizing disruptions in the face of shocks and stresses, recovering rapidly when they do occur, and adapting steadily to become better able to thrive as conditions continue to change. Within the context of CI, the resilience process offers a cyclical, proactive and holistic extension of risk management practices."*

In addition to a general definition of resilience, the project also developed a **definition of critical infrastructure resilience** (CIR): *"A transformative, cyclical process, building capacities in technical, social and organisational resources, so as to mitigate as far as possible impacts of disruptive events, and based upon new forms of risk management, adaptability and the assessment of potential trade-offs between parts of a system"* [6].

Interesting for the envisaged elaboration of the **relation between resilience and risk management** in this report, is a chapter in RESILENS D1.1 explicitly addressing this issue. Four perspectives are presented and commented there, which are presented together in Table 1.

Table 1: Perspectives on the relation of resilience and risk management [6]

Resilience as…		Description	RESILIENS comments
1	A goal of risk management	Many documents describe resilience as the overarching goal of protection policies and risk management as the method to achieve this goal. Resilience replaces or complements the concept of protection, which was previously defined as the goal of risk management activities.	Perspective 1, which understands resilience as the outcome of risk management, is the traditional, normative approach to risk and resilience within CI's, and thus one that is easily integrated into existing policies. However, it is challenged by complexity, the uncertainty presented by unpredictable events, as well as the interdependency of sectors and thus the cascading effects of impacts.
2	A part of risk management	Resilience is understood as a part of risk management. Activities to strengthen resilience are needed in order to deal with the so-called "remaining risks", i.e. risks that have not been identified or underestimated and are thus not covered by appropriate protection (preventive) measures.	Perspective 2, views resilience as part of existing risk management approaches and brings together probabilistic analysis with coping strategies. In effect, the resilience of a system is about having sufficient capacity to address any residual risks. However, within this perspective, resilience is difficult to define, whilst there is a further suggestion that it is still somewhat normative and could stifle innovation or more transformational change.
3	An extension of risk management	This transitionary perspective recognises the importance of risk management to CI operation, but proposes that these practices need to be extended to encompass resilience practice that integrates social and organisational factors, as well as building capacity to change.	Perspective 3 has been formulated for the RESILENS project and recognises that whilst risk assessment is fundamental to CI practice at present, that there is a requirement to extend this process to consider resilience as part of a more dynamic system that includes social, technical and organisational factors. Furthermore, this perspective can be considered as one of transition to the more transformative understanding of resilience as offered by perspective 4.
4	An alternative to risk management	Challenges the traditional methods of risk management and promotes resilience as a new way of dealing with risks in a complex environment. It is argued that a probabilistic risk analysis is not an adequate approach for socio-technicalsystems that are confronted with non-linear and dynamic risks and are themselves characterized by a high degree of complexity. Instead of preventing risks and protecting the status quo, such systems should enhance their resilience by increasing their adaptive capacities.	Perspective 4 presents resilience as a transformative alternative to risk management. It is based upon the principle that probabilistic risk analysis is inadequate for the complex, non-linear and dynamic, socio-technical nature of today's challenges, and that probabilistic approaches will always fail to assess the risks of 'The Black Swan'101 appropriately. This 4th perspective is slippery and underdeveloped, but advocates redundancy, flexibility and self-organisation rather than risk assessment. It is further suggested that in a resilient society, there should be few CI's. Appropriately, this perspective presents a challenge to CI approaches and is unlikely to be widely accepted, although the Australian national approach draws from this perspective

2.3.3.4 Conclusions for SmartResilience

The RESILENS definitions are highly useful for SmartResilience as they are already curtailed to Critical Infrastructure, and shall be considered for the SmartResilience resilience definition and concept (chapter 3). The different perspectives on the relation of resilience and risk management provide a good basis to define the SmartResilience understanding of the relation. It is further particularly interesting that RESILENS understands CIR as a new form, or rather extension, of risk management despite claims of its transformative nature. It therefore sits between those who simply consider resilience as risk management under a new guise and those who advocate that resilience is something entirely new.

2.3.4 Review conducted within the RESOLUTE project

2.3.4.1 RESOLUTE

RESOLUTE (RESilience management guidelines and Operationalization appLied to Urban Transport Environment, May 2015 – April 2018) aims to improve resilience in the urban transport environment. The project recognises the ongoing profound transformation of urban environments in view of ecological, human and overall safety and security needs, as well as the growing importance of mobility within every human activity. It addresses the need to develop related efforts in increasing resilience, and to create a European Resilience Management Guide.[5] In the first phase a review work was done in order to identify and evaluate resilience concepts and methods.

2.3.4.2 Description of the RESOLUTE's review process

As presented in the RESOLUTE D2.1 "State of the art review and assessment report", the project conducted a qualitative study focusing on four tasks: 1) review of the resilience literature, 2) review of risk analysis and management guidelines at national and EU level, 3) review of applied tools and methods, 4) review of training programs and assessment. On the basis of this review a RESOLUTE conceptual framework has been drafted with the aim of steering further work in RESOLUTE [16].

2.3.4.3 Main findings of RESOLUTE's review relevant for this report

The literature review showed that the definition of the resilience concept varies according to different domains but also that it builds on a common need **to address high complexity, variability and uncertainty**. This, according to the authors, increasingly challenges current risk management practices. It is found quite often in the literature that the term resilience has been used mainly as a new terminology to leverage previously existing approaches and views. Nevertheless, it is also found in the literature that significant advances have been made in risk management approaches, tools and assessments, even though not always successfully addressing complexity and uncertainty [16].

As the **fundamentals of resilience**, three conditions are described (based on [53] and [34]):

- "**Avoidance** relates to the ability to foresee potential threats and prevent something bad from happening.
- **Survival** implies that the system, while experiencing disturbance, maintains operations, even if partially incapacitated. This means that the system is able to cope with ongoing trouble and therefore, prevent something bad from becoming worse.
- **Recovery** refers to the ability of the system to repair itself and regain desired performance after something bad has happened" [16].

The major findings of the literature review also comprise a **summary of key resilience definitions**, and related key words, which shall indicate resilience issues in these domains (see RESOLUTE D2.1 [16], p. 39f). These keywords comprise for example "sustainability", "absorb change and disturbance" "regenerate", or "react and recover". According to the authors, many of the definitions can be clearly demarcated along two types of resilience:

[5] http://www.resolute-eu.org/, accessed July 28, 2016

- **"Engineering resilience** is considered a more "classical" view, emanating from physics models. It assumes a system exists around an equilibrium state and its resilience is defined in terms of the ability to resist departure from, or rapidly return to that equilibrium after significant disturbances [19]. From this perspective, efforts aim at maintaining a degree of constancy in the system by containing its variability.
- **Ecological resilience** assumes that systems can reorganise themselves and therefore, contemplates the possibility of systems shifting from one domain of stability to an entirely different one. In this sense, resilience is defined by the magnitude of disturbance that a system can absorb (avoid) before it shifts from one set of mutually reinforcing processes and structures to a new one [18]. The focus is set on the persistency of relations among parts of the system. Like many plants that bend with the wind instead of stiffly attempting to resist it, ecological resilience assumes the possibility of the system shifting to new equilibrium states in order to ensure its basic structure and function [52]."

While the engineering perspective aims to achieve and **maintain a condition of stability**, the ecological perspective aims at creating capacity to **cope with variability** [16].

2.3.4.4 Conclusions for SmartResilience

The "fundamentals of resilience" should be reflected in some way in the SmartResilience resilience definition/ concept, while not necessarily in literally terms. The list of definitions and key words might be useful and contribute to a basis for upcoming work in SmartResilience on specific aspects (e.g. specific types of SCI's), which might require supplementary issues or approaches of resilience, in addition to those included in the overall definition and concept. Aspects of both the engineering resilience as well as the ecological resilience seem relevant for SmartResilience and shall thus be reflected in the resilience SmartResilience resilience definition/ concept.

2.3.5 Review conducted within the SMR project

2.3.5.1 SMR

Smart Mature Resilience (SMR, running June 2015 – May 2018) aims to develop a guideline to assist European city decision-makers in developing and implementing resilience measures. It focuses on three core areas: Critical Infrastructure, Climate Change, and Social Dynamics. As Europe's cities continue to grow, the project addresses the urgent need for far-reaching and holistic approaches to enhance cities' capacity to resist, absorb, accommodate and recover from the potentially critical effects of hazards. It aims at supporting and building on the nexus of key resilient cities across Europe, in order to create a strong backbone for all of Europe's cities to support one another in overcoming the challenges arising from risks ahead.[6]

2.3.5.2 Description of SMR's review process

As part of their preliminary background work, SMR conducted reviews of literature, of worldwide approaches to resilience, predominantly in the area of city resilience and climate change, and of resilience approaches of cities that are part of SMR, presented in the SMR deliverable D1.1 [43]. The systematic literature review was conducted in a similar manner to the DARWIN approach using the Scopus database.

The review entailed five steps: Step 1 included the initial search in Scopus using pre-defined criteria, generating 2993 hits. In step 2, subject areas were excluded within the initial search, selected based on relevance to the project. In Step 3 the scope was further narrowed down to include only the "200 most cited", "200 most recent" and "200 most relevant" ones (according to Scopus relevance criteria). The 600 articles selected were reviewed based on title and abstract. Criteria for inclusion in the full review were based on project relevance. In Step 4 all articles were quality checked by a second rater to ensure the relevance of the papers selected for the SMR project. Step 5 included a full review of the remaining (119) articles [43].

[6] http://smr-project.eu/, accessed July 28, 2016

2.3.5.3 Main findings of SMR's review relevant for this report

Similar to DARWIN, SMR identified a large number of definitions for resilience (around 120). These definitions were further categorised based on dimensions (the field of resilience in question, largely based on the research areas of the authors), temporal aspects (before, during, or after an event), characterizations (description of resilience as a property, process, capability, ability, capacity, or characteristics), and behaviours (absorb, adapts, recover, or self-organize). It was found that most common definitions entailed three aspects: "**absorb shocks**", "**ability to adapt**", and "**ability to recover or 'bounce-back'**". It is noteworthy however that many discussions of resilience do not give a specific definition at all. Rather, these articles explore discussions around resilience and entail what they believe to be important aspects of resilience. The SMR authors attribute this lack of a definition in some articles to the author's awareness that resilience might be a fuzzy concept that occasionally incorporates conflicting definitions. Other authors might also stress the importance of a pragmatic and applied attitude towards resilience, which might not be best served by subscribing to a particular definition. According to SMR, most papers in this category come from national and international organizations and deal with issues of sustainability [43].

In addition to the discussion of resilience definitions, the SMR deliverable D1.1 also identified 22 **frameworks for resilience** in the literature analysis, which are summarized in a table (see table 7 in SMR D1.1 [43], possibly useful for upcoming work in SmartResilience). The description comprises the main objectives of the frameworks, target areas in which the frameworks are intended to be used, as well as key attributes. The area most frequently addressed was "natural hazards/climate change", followed by "community resilience". Regarding the attributes or indicators used in the framework, a large variety was identified, which according to the authors reflects the lack of consensus and unification, but also the many aspects that are important to be resilient, and the many ways to increase resilience [43].

The insights gained from D1.1 are taken up in D1.2 [42] and expanded to encompass a review of the European sectorial approaches. This analysis entailed a discussion of the various EU funded projects. Given that critical infrastructure is one of the central focus areas of SMR, the review resulted in **a map showing which critical infrastructure (CI) projects focus on which type of threats** (see figure 7 in SMR D1.2 [42], possibly useful for upcoming work in SmartResilience).

A further analysis of the EU CI projects identified seven key themes, which are further discussed in detail in D1.2 [42]:

- CI Dependency and Interdependency
- CI Cascading Effects
- CI Risk and Vulnerability Analysis
- CI Resilience and CI Protection
- CI SmartGrid and Cyber Attack
- CI and Urban Resilience
- Other CI Themes.

Despite the in-depth review of these projects and initiatives, SMR also concludes that "it is apparent that there is a huge variety of policy suggestions across the numerous EU projects targeting resilience. Lacking empirical evaluations of the long-term impact of those policies it is currently not possible to highlight particular policies as "best practice", i.e., being superior to others" [42].

In their final deliverable D1.3 of the first work package [2], SMR defines resilience for the project. However, they do not use one definition but rather come up with **a list of tentative definitions for resilience for different environment and with regard to different systems**. The outcome for critical infrastructure resilience is as follows:

- "CI RESILIENCE from CI Literature
  Resilient infrastructure can resist damage and loss of function, absorb, adapt to, or rapidly recover from a potentially disruptive event, can quickly restore its continuity and support city's CI-based services.
- COMMUNITY AND SOCIAL RESILIENCE from CI Literature
  Community and Social Resilience refers to a network of individual's adaptive capacity, including capability to detect abnormal events, to prepare and plan, self-organise, inform the local

government, mobilise resources. It also comprises capability to cope with disruption, and capability to resist, adapt and recover from it. Collaboration capacity with the neighbourhood in the city and forming social cohesion to withstand hazard will be part of community and social resilience.

- URBAN OR CITY RESILIENCE from CI Literature
  The urban or city resilience consists of a mixture of resilient built-in environment, resilient design, resilient citizens, and resilient organisations. Resilient built environment should be designed, located, built, operated and maintained in a way that maximizes the ability of built assets, associated support systems (physical and institutional) and the people that reside or work within these built assets, to withstand, recover from, and mitigate the impacts of extreme natural hazards and human-induced threats. The citizens in the city should be able to handle and respond to unexpected situations resulting from malfunctioning CIs, changes of social, economic and environmental stresses, and also be proactive during a crisis and have the ability to recover by themselves. The organisations at the city level have capacity to support all transformation by rapid changes taking place in urban key areas.
- ORGANISATIONAL/LOCAL GOVERNMENT RESILIENCE from CI Literature
  Organisational resilience covers all management capacity such as planning, leadership, training, experience, and information management. It includes the capacity to improvise, innovate and expand the operations between impact and early recovery and the capability to conduct proper risk assessment and risk management.
- INDIVIDUAL RESILIENCE from CI Literature
  Individual resilience is a person's own resilient capabilities – the adaptive capacity of individuals to react or adapt positively to hazards or unexpected events.
- ECONOMIC RESILIENCE from CI Literature
  Economic resilience is the capacity to reduce direct and indirect losses, maintaining function such as continuous production.
- CBRNE RESILIENCE from CI Literature
  Capability of the responders to detect CBRNE events, to respond and to recover from occurring incidents.
- COMMUNICATION RESILIENCE from CI Literature
  Communication resilience is the capacity to provide communication infrastructure in a steady state. In addition, citizens have capacity to absorb and preparedness to make use of different crisis management communication technologies to withstand hazards" [2].

2.3.5.4 Conclusions for SmartResilience

The main identified aspects of resilience definitions, "absorb shocks", "ability to adapt", and "ability to recover or 'bounce-back'", are all reflected in the initial SmartResilience definition of resilience. The summary of frameworks, which is referred to, as well as the overview highlighting which type of threats which EU projects deal with will be very useful when identifying indicators and methods for specific cases (e.g. SCI's). Similar is true for the 'solution' of using different definitions for different systems and different functions (e.g. communication, government, urban…), which will be discussed in chapter 3. It could also be useful for discussions with end-users of SmartResilience.

2.4 Resilience definitions and concepts from selected organisations/ sources

In this chapter, definitions and concepts of resilience as defined/ used by selected sources, which are assumed to be most relevant for SmartResilience, are reviewed. These sources cover the following: UNISDR, whose definition of resilience is a definition most used in the field of disaster risk reduction; OECD, who developed resilience guidelines, of which several aspects appear very useful for SmartResilience; the main US organisation of emergency management (FEMA); the industry perspective; and pertinent standards.

Each sub chapter includes a description of the respective source, pointing out its relevance for the purpose of this report, the source's concept of resilience, and conclusions for SmartResilience.

2.4.1 Resilience definition and concept by UNISDR

2.4.1.1 The UNISDR

The United Nations Office for Disaster Risk Reduction (UNISDR) was established in 1999 as a secretariat to facilitate the implementation of the International Strategy for Disaster Reduction (ISDR), reflecting a major shift from the traditional emphasis on disaster response to disaster reduction. UNISDR is mandated by the United Nations General Assembly to serve as the focal point in the United Nations system for the coordination of disaster reduction and to ensure synergies among the disaster reduction activities of the United Nations system and regional organizations [49].

The work within UNISDR is guided by the Sendai Framework for Disaster Risk Reduction (2015-2030), which was adopted in March 2015 after comprehensive stakeholder consultations and inter-governmental negotiations at the Third UN World Conference in Sendai, Japan. The Sendai Framework is a 15-year voluntary, non-binding agreement that maps out a broad, people-centered approach to disaster risk reduction, succeeding the Hyogo Framework for Action. UNISDR has been tasked to support the implementation, follow-up and review of the Sendai Framework [49].

Resilience is one of several key terms used by the UNISDR related to their work of coordinating and promoting disaster risk reduction on global, national, regional and local level.

2.4.1.2 Understanding of resilience by UNISDR

The UNISDR defines resilience as "*The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions*" [47]. The UNISDR further mentions terms such as disaster resilience, economic resilience, social resilience, health resilience, cultural resilience and environmental resilience, but without pertinent definitions of these terms [48].

For UNISDR, the concept of resilience is closely related to the terms risk and disaster risk reduction[7] where disaster risk reduction is seen as a means to strengthen resilience. This is for example expressed in the overall objective of the Sendai Framework:

"Prevent new and reduce existing disaster risk through the implementation of integrated and inclusive economic, structural, legal, social, health, cultural, educational, environmental, technological, political and institutional measures that prevent and reduce hazard exposure and vulnerability to disaster, increase preparedness for response and recovery, and ***thus strengthen resilience"*** [48].

The UNISDR works along the following definition of risk: "The combination of the probability of an event and its negative consequences". This definition takes inspiration from the definition of the ISO/IEC Guide 73 [20]. The UNISDR highlights that the word "risk" can be understood either as emphasizing the concept of chance or possibility, such as in "the risk of an accident"; or emphasizing consequences, in terms of "potential losses".

With regards to vulnerability, the UNISDR applies the following definition: "The characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard". Vulnerability may refer to e.g. physical, social, economic, and environmental factors. It varies significantly within a community and over time. This definition identifies vulnerability as a characteristic of the system, community or society which is independent of its exposure.

The need for increased resilience of critical infrastructure is also underlined by the UNISDR, where one of seven global targets of the Sendai Framework is to "*Substantially reduce disaster damage to critical infrastructure and disruption of basic services, among them health and educational facilities, including*

[7] UNISDR definition of Disaster Risk Reduction: "*The concept and practice of reducing disaster risks through systematic efforts to analyse and manage the causal factors of disasters, including through reduced exposure to hazards, lessened vulnerability of people and property, wise management of land and the environment, and improved preparedness for adverse events*".

through developing their resilience by 2030". This is further highlighted when putting forward the main priorities of the disaster risk reduction work until 2013, one priority being promoting "*…the resilience of new and existing critical infrastructure, including water, transportation and telecommunications infrastructure, educational facilities, hospitals and other health facilities, to ensure that they remain safe, effective and operational during and after disasters in order to provide live-saving and essential services"* [48].

2.4.1.3 Conclusions for SmartResilience

The UNISDR's focus on resilience for "a system, community or society" suits SmartResilience well since it allows for an analysis of an entire infrastructure which typically involves a number of organizations and therefore requires an analytical scope outside the single organization. At the same time, it poses a challenge to define appropriate boundaries for the "system, community or society". However, SmartResilience address this challenge i.e. through actor analyses that are carried out in initial stages to guide parts of the analysis. It should be kept in mind that a demarcation to a specific geographical location is likely to be useful in each case study of SmartResilience. This focus, however, does not mean that SmartResilience should oversee important processes to enhance resilience that takes place at organizational level.

Furthermore, all relevant steps included in the UNISDR definition of resilience ("resist, absorb, accommodate to and recover") have been recognized by SmartResilience (which also includes some additional dimensions compared to UNISDR). Similar to SmartResilience, the UNISDR also recognizes the close relation to the concepts of risk and disaster risk reduction, and vulnerability. The UNISDR recognition of the need for increased resilience of critical infrastructure is particularly relevant for SmartResilience.

2.4.2 Resilience definition and concept by OECD

2.4.2.1 The OECD guidelines for resilience systems analysis

The Guidelines for resilience systems analysis developed by OECD [26] is a step-by-step guidance on how to analyze risk and build a roadmap to resilience in order to enable effective development in developing countries.

"Resilience has been a key focus of the Organisation for Economic Co-operation and Development (OECD) since the financial crisis of 2008. The development and humanitarian communities also picked up on the concept, prompted by a ground-breaking 2011 review of the United Kingdom's humanitarian programme, and later as a better way to respond to major food emergencies in the Horn of Africa, and then in the Sahel.

The guidance is aimed at professionals who are grappling with what resilience actually means, and how to get key stakeholders to develop a shared vision of both the risks that exist in their particular context, and what to do about them; both now, and in the longer term. We have called the outcome of the analysis a roadmap to resilience because it is just that – a shared view of the way forward towards a more resilient future.

The OECD will continue to support the resilience roadmap process as it is rolled out in contexts prone to natural, climate, economic and/or geo-political shocks. Our members – major humanitarian and development assistance providers – will use this approach to re-think their programming through a risk lens. We will also support other organisations and states who seek to embed this approach into their programme design processes"[39].

In these guidelines, resilience is understood as "what to do about the risks" (that faces developing countries). Resilience here means that states can better withstand environmental, political, economic and social shocks and stresses. They refer to examples such as Bangladesh has become more resilient against floods as the government's ability to warn and evacuate people and control infectious diseases has improved.

Interesting to notice is that OECD has (as many others) struggled to introduce the concept of resilience. People found it difficult to understand what resilience actually meant. Was it just another 'buzzword' or 'fad' inserted into proposals to attract new funding?

"Everybody is talking about resilience. The idea that people, institutions and states need the right tools, assets and skills to deal with an increasingly complex, interconnected and evolving risk landscape, while retaining the ability to seize opportunities to increase overall well-being, is widely accepted.

In reality, however, it has not been easy to translate this sound idea into good practice, mostly because people in the field don't yet have the right tools to systematically analyse resilience, and then integrate resilience aspects into their development and humanitarian programming" [39].

OECD believes that resilience provide added value, compared with traditional risk management, as described below.

2.4.2.2 Understanding of resilience in the OECD guidelines for resilience systems analysis

In the OECD guidelines [39]. resilience, risk and vulnerability is defined as follows:

Resilience	The ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty
Risk	The combination of the probability of an event and its negative consequences
Vulnerability	An expression of susceptibility to harm, and exposure to hazard

OECD states that we know a great deal about different risks in developing countries; however, we don't yet share 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.

Therefore, when it comes to the relation between resilience and risk, resilience is about "what to do about the risks". However, isn't this part of risk management? What is the relation between resilience and risk management?

According to OECD [39], resilience systems analysis builds on, rather than replaces, traditional risk management approaches, by:

- adding elements that address the complexity and inter-linkages of different risks. It takes into account, for example, how disasters can also trigger economic shocks, and how conflicts can also leave people more exposed to disaster
- going beyond the “known knowns”, on which traditional risk management is based, to also account for uncertainty and change, by exploring how long-term trends (stressors) such as climate change, governance and insecurity, economic marginalisation and volatility, environmental degradation, and demographic changes can change the nature and impact of shocks in the future
- merging risk forecasting with critical reflection on how the system has performed in the past
- focusing on the system, not the risk, aiming to strengthen the systems that people use to support their all-round well-being, no matter what risks they face, building on existing capacities
- understanding the importance of power relations in helping or hindering resilience
- taking into account both large scale (covariate) and small scale (idiosyncratic) shocks, given that frequent, low impact events, like illness, can also have a devastating impact on people’s lives.

In order to describe the resilience systems analysis approach, it is necessary to introduce some of the illustrations in OECD [39], starting with the conceptual framework (Figure 6), followed by the system under analysis (Figure 7), and ending with the three different types of capacities (Figure 8).

We will not go into details of the approach, only discuss it in relation to the preliminary definition and concept of SmartResilience (as described in chapter 2.2). For details of the approach, we refer to [39].

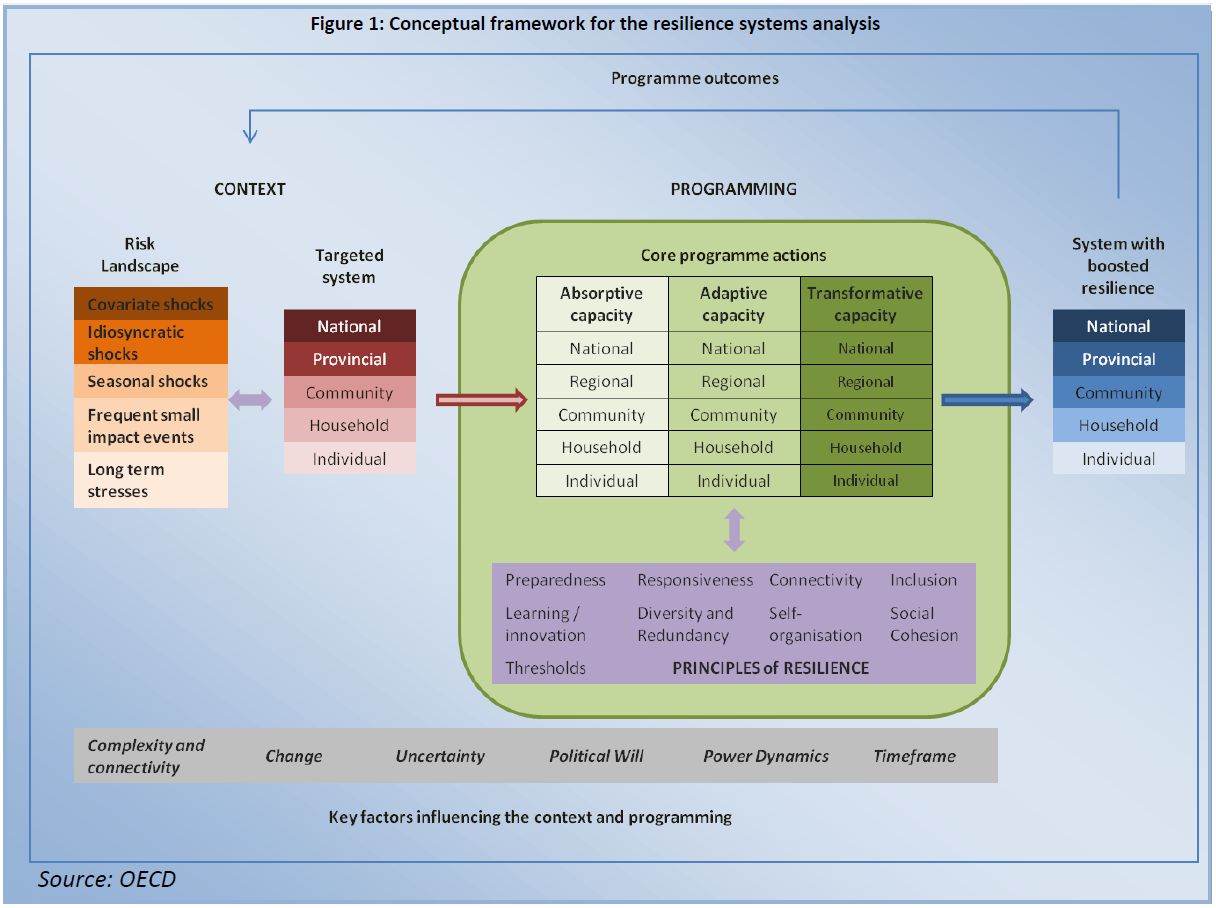

Figure 6: OECD conceptual framework for resilience systems analysis (Figure 1 in [39])

The context consists of the risk landscape (with various categories of shocks/events/stresses) and the targeted system (analysed at different levels). Programming includes the actions identified as necessary to strengthen resilience, which (when implemented) affects the context.

It is worth noting that establishing the risk landscape, i.e. knowing which risks you need to be resilient against, is part of the resilience systems analysis. This is why it has been suggested, in the perspective of WP3, to include risk understanding as the first "resilience dimension/ability/phase" (cf. chapter 2.2).

The system under analysis (targeted system) is based on a very broad definition of "system". According to OECD [39] a system is *"a unit of society (e.g. individual, household, a group of people with common characteristics, community, nation), of ecology (e.g. a forest) or a physical entity (e.g. an urban infrastructure network)"*.

Based on their specific context, OECD has linked the systems to the Sustainable Livelihood Approach, under which the well-being of a community depends on a system with six different categories of assets or "capitals" as illustrated in Figure 7. The specific assets will differ from context to context.

The definition of "system" is very broad, but it could be e.g. a (critical) infrastructure network, although this is only a small part of the considerations in the OECD guideline. The guideline covers all six categories of assets.

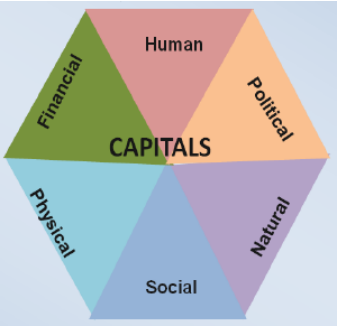

Figure 7: OECD "system" comprising six categories of assets/capitals (Figure 2 in [39])

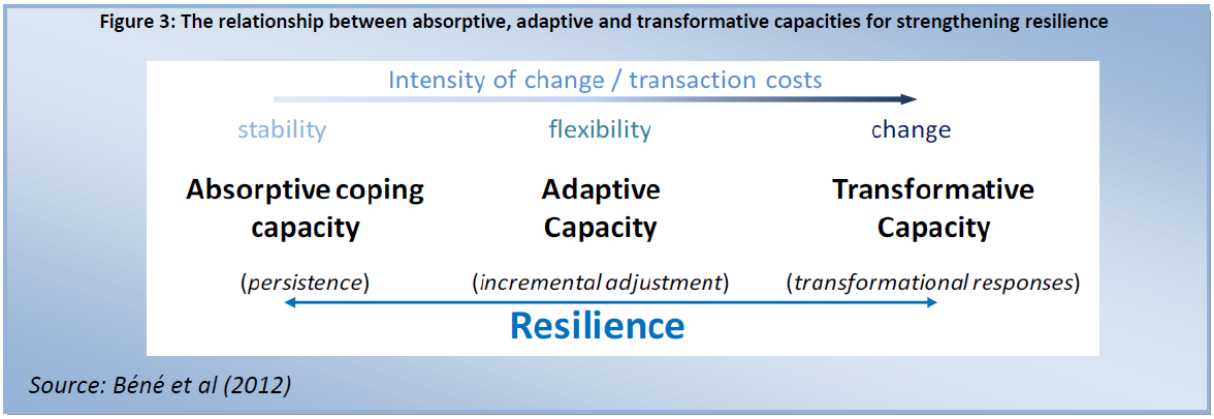

Figure 8: The three types of capacities used by OECD (Figure 3 in [39])

Figure 8 illustrates the three types of capacities for strengthening resilience, which is also included in Figure 6.[8] The three types of capacities (or abilities) are also reflected in the OECD definition of resilience:

The ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty.

In the definition, it is also a fourth ability; *recover*.

This can be compared to the working definition of resilience used in SmartResilience:

Resilience of an infrastructure is the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions.

It appears that the only additional capacity/ability mentioned in the OECD definition is "transforming" (considering *absorb* being similar to *withstand*). However, both in the OECD approach and the SmartResilience approach, the capacities/abilities referred to above are on a "level 1", whereas "sub-categories" or more specific "issues" are included on a "level 2" (cf. chapter 3 for discussion on different "levels" in resilience concepts).

OECD [39] describe *absorb* (or absorptive capacity) as: *The ability of a system to prepare for, mitigate or prevent negative impacts, using predetermined coping responses in order to preserve and restore essential basic structures and functions.*

Hence, at this second level, OECD includes abilities such as *prepare for* and *respond to*, which in SmartResilience currently are included on level 1.

[8] These capacities could also be compared with the categories of resilience elements as described in chapter 2.4.4: Structural, integrative and transformative resilience.

In addition, OECD defines *adapt* (or adaptive capacity) as: *The ability of a system to adjust, modify or change its characteristics and actions to moderate potential future damage and to take advantage of opportunities, so that it can continue to function without major qualitative changes in function or structural identity.*

Finally, *transform* (transformative capacity) is defined as: *The ability to create a fundamentally new system so that the shock will no longer have any impact.*

Compared to the preliminary understanding in SmartResilience, "adaptation" is treated more nuanced in the OECD guidelines. This can provide input for consideration of how to treat and detail "adaptation" in SmartResilience, since adaptation may be necessary at different stages (not only after restoration), and it may make sense to distinguish between different types of "change", as in [39].

When it comes to where (at what level) the relevant abilities should be included, this is to a large degree a matter of preference and suitability. Level 1 should be reflected in the definition of resilience. The working definition contains six resilience abilities/dimensions/phases, and adding more than a couple of additional abilities will make the definition difficult to comprehend. There is in principle no specific limits to the number of abilities included on level 2.

2.4.2.3 Conclusions for SmartResilience

The capacities related to adapt and transform may be useful to consider in SmartResilience resilience definition and concept, since OECD distinguishes between incremental change (adapt) and fundamental change (transform). It may also be useful to consider where to include *adaptation* in the resilience time line, since this may take place at several stages in the development of a disruption (and the preparations for disruptions).

The inclusion of a description of the *risk landscape* as part of the resilience systems analysis supports the idea of including *risk understanding* as a first phase/dimension/ability in SmartResilience. Understanding the risks you are facing is obviously a prerequisite for knowing what to do about them.

More generally, it is useful to include the arguments used by OECD on why resilience (systems analysis) complements risk management, because this is a main objection by many resilience sceptics, arguing that risk management suffice, and that there is no added value of resilience.

OECD is not focusing specifically on critical infrastructure protection, although this may be one of the specific assets within one of the six types of assets (the physical asset/capital).

The resilience systems analysis described by OECD [39] aims at providing a roadmap for resilience, which includes a set of actions to be included in programmes for development of developing countries. The actions will strengthen resilience where this is needed most. This goes far beyond the scope of SmartResilience, where we focus on the assessment of resilience. Defining actions, and implementing and following-up these actions, are not part of the SmartResilience scope.

OECD includes indicators to "measure resilience"; however, by this they mean several different types of "measures". They distinguish between five different types of indicators:

1. System resilience indicators (outcome indicators)
2. Negative resilience indicators
3. Process indicators
4. Output indicators
5. Proxy impact indicators

The last three are all related to the use, implementation and effect of the roadmap, i.e. the actions, which is not relevant for SmartResilience.

The first indicator type attempt to measure the resilience of main components of the system over time. In the context of the OECD guidelines, this means measuring the specific assets within each of the six capitals/assets. E.g., formal education is an asset within human capital, which is proposed measured by the indicator "proportion of girls, and boys, attending school".

A five level scale (0-4) is used to provide scores for each asset. This is summarized for each of the six capitals and the overall result presented in a spider diagram.

The negative resilience indicators look at whether people are using strategies to boost resilience that may have negative impacts on other areas of the system.

In particular, the first type of indicators, and perhaps the second type, may provide some ideas for the methodology in WP3.

2.4.3 Resilience definition and concept by USDHS/ FEMA

2.4.3.1 The USDHS/FEMA

As a component of the United States Department of Homeland Security (USDHS), the Federal Agency of Emergency Management (FEMA) is part of a larger preparedness team. Together, the organizations within DHS work towards a homeland that is safe, secure, and resilient to all hazards [14]. In 2011, FEMA announced the release of the country's first-ever National Preparedness Goal. The goal sets the vision for nationwide preparedness and identifies the core capabilities and targets necessary to achieve preparedness across the following five mission areas: prevention, protection, mitigation, response and recovery [51].

Reports on "Crisis Response and Disaster Resilience 2030" [9], FEMA's Strategic plan 2014-2018 [10], and USDHS websites were analyzed to understand the definition and concept of resilience embraced by FEMA.

2.4.3.2 Understanding of Resilience by USDHS/ FEMA

The term "resilience" as defined by USDHS is the "ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies" [51]. These changes could be acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters and their aim is to instill the mind-set of national preparedness as a shared responsibility of all levels of government, the private and non-profit sectors, and individual citizens [51].The resilience centric approach is critical for USDHS because of following reasons

- The United States officially recognized resilience in a national doctrine in the 2010 National Security Strategy, which states that United States must enhance their resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption [51].
- The U.S. Department of Homeland Security recognized resilience in the 2014 Quadrennial Homeland Security Review, which established a series of goals and objectives in the areas of critical infrastructure, global movement and supply chain systems, and cyberspace. Further, one of the five missions of this review was devoted to resilience, i.e. Mission 5 – Strengthening National Preparedness and Resilience [51].
- The September 2001 attack raised the terrorism threat and demanded a well-informed, highly agile strategy [50].
- The main reason why FEMA has strategically prioritized resilience is due to the need to explore future challenges the whole nation must withstand and the need of confronting the complexity that arises from the interaction of multiple drivers – such as demographic shifts, technology, environmental changes, and economic uncertainty [12]. The emergency management community faces increasing complexity and decreasing predictability in its operating environment [12].

2.4.3.3 Approach of Strategic Foresight Initiative and the priorities of FEMA

In order to deal with this challenge, FEMA in its Strategic Foresight Initiative (SFI), sought to identify the drivers (refer Figure 9) for change or reshaping the world, i.e. Social, Technological, Environmental, Economic and Political (STEEP) [12], and the interconnections between each of the drivers.

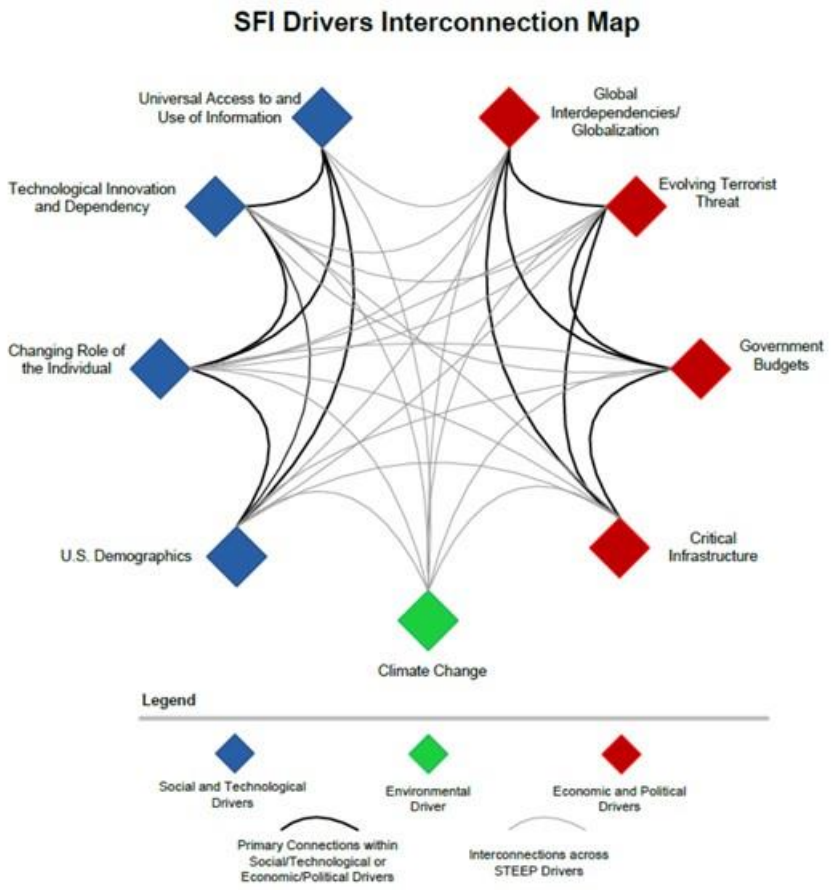

Figure 9: Strategic Foresight Initiative drivers' interconnection maps [12]

Each of these drivers of change possesses transformative capacity and to assess this, scenario planning was conducted to explore how these changes can impact the emergency management field over the next 20 years [14] and also the opportunity to play out varying driver conditions – and driver cross-impacts, and arrived at three high level strategic needs [12]:

1. "Essential Capabilities the community will need to build or enhance in order to meet future challenges;
2. Innovative Models and Tools emergency managers will need to optimize resources, anticipate events, or deal with complex and/or unprecedented problems; and
3. Dynamic Partnerships that will need to be formed or strengthened to meet such requirements or to absorb critical new skills and capabilities" [12].

Based on these needs, FEMA developed five strategic priorities and two imperatives [14], as shown in Figure 10.

- Priority 1—Be Survivor-Centric in Mission and Program Delivery.
- Priority 2—Become an Expeditionary Organization.
- Priority 3—Posture and Build Capability for Catastrophic Disasters.
- Priority 4—Enable Disaster Risk Reduction Nationally.
- Priority 5—Strengthen FEMA's Organizational Foundation.

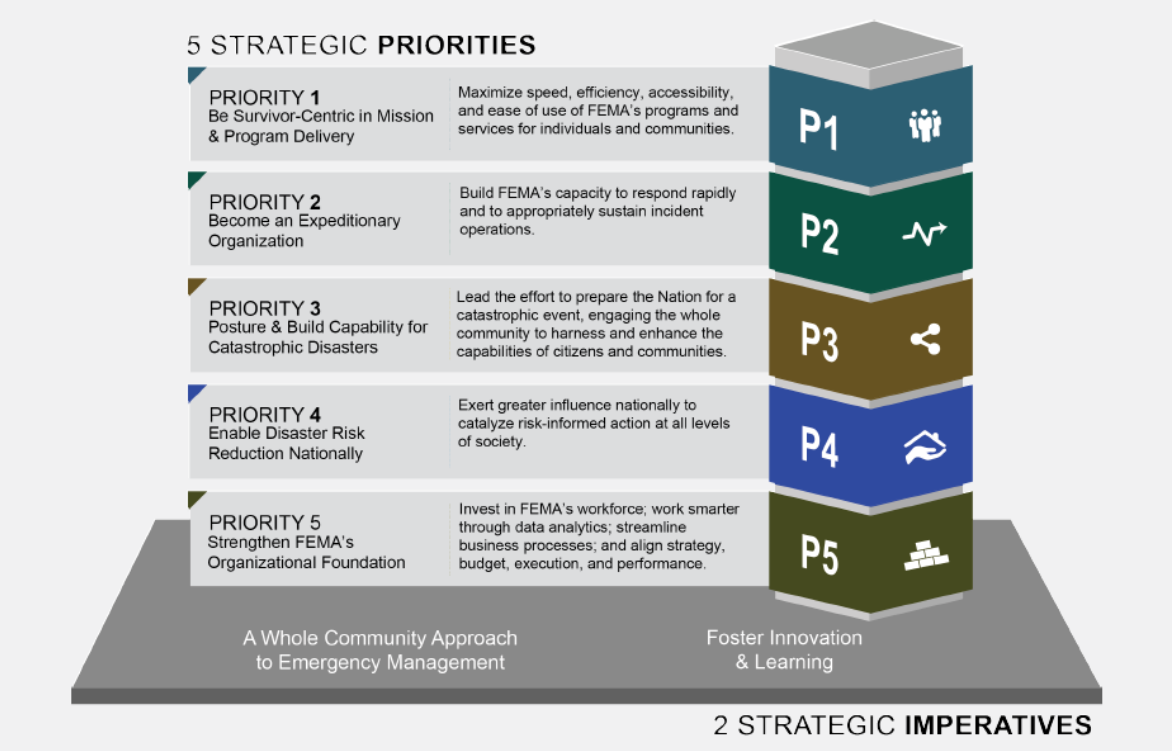

Figure 10: Five strategic priorities and two impertives for FEMA [14]

FEMA's two strategic imperatives shape and influence the approach the Agency takes in carrying out its mission and achieving its strategic objectives.

- Strategic Imperative 1—A Whole Community Approach to Emergency Management. The following principles frame this aspect
  - Plan *with* rather than *for* communities.
  - Engage and empower all parts of the community.
  - Better understand and help meet the needs of the community.
  - Strengthen what works well in communities on a daily basis.
- Strategic Imperative 2—Foster Innovation and Learning.

2.4.3.4 Conclusions for SmartResilience

The resilience definition USDHS/FEMA covers prepare, absorb, adapt, and recover attributes as explained in chapter 2.2. and does not essentially add any new aspect to the definition of resilience however, the concept of mapping the interconnections between social, technological, environmental, economic and political drivers could be useful for identifying the interconnectedness of critical infrastructure with other drivers.

In addition, the approach undertaken by FEMA to enhance resilience could be seen as a useful application-based case for enhancing the resilience of critical infrastructure i.e. the priorities and imperatives defined by FEMA to deal with the uncertainty and complexity posed by the drivers of change can be considered examples of the activities the SmartResilience project may be able to replicate within the policy recommendation, post the evaluation to the specific case studies. However, not all the aspects can be adapted and care must be undertaken as a resilience strategy has to consider the spatial and temporal scales while developing an approach suited for a specific environment.

Also, scenario planning to foresee the uncertain future needs that may influence the present policy decisions as an approach, could help the process of building resilience of smart critical infrastructure.

Last but not the least, FEMA is a federal agency and it may be relatively easier to implement the visions, priorities and imperatives set by a central organization, compared to the EU, where the harmonization of the resilience approach is dispersed due to different specifications for infrastructure in each member state.

2.4.4 Resilience definition and concept from an industry perspective

2.4.4.1 Initiatives by the industry

Another concept that seems promising for the project, and was used in the proposal, is the one from the Resilience Action Initiative, which focused on the enterprise resilience. Resilience action initiative involves large and globally active companies with the premise that in the ever growing demand scenario, the socio-economic systems will have to become more resilient to turbulences and this initiative sought to explore how multinational companies can help to strengthen the adaptive capacity of their own operations as well as the communities they interact with and depend on [45]. Furthermore, initiatives such as Chief Risk Officers (CRO) Forum is another relevant initiative by the insurance industry to raise the awareness of major risks relevant to society and the re/insurance industry, developing best practice solutions, standardizing disclosure and sharing knowledge of key emerging risks.

For the purpose of this review, Resilience action initiative was reviewed in depth.

2.4.4.2 Understanding and concept of resilience from an industry point of view

According to the initiative, "Resilience is the capacity of business, economic and social structures to survive, adapt and grow in the face of change and uncertainty related to disturbances, whether they be caused by resource stresses, societal stresses and/or acute events" [34].

The initiative suggested that in order to ensure the resilience of a system, the concept of resilience encompass three different levels[9]

- The STRUCTURAL resilience
- The INTEGRATIVE resilience and
- The TRANSFORMATIVE/ADAPTIVE resilience.

Emphasizing on these types allows shifting focal scale from the system itself through its interconnections with its environments to long-term adaptability. Each level has its costs and benefits and it is seen crucial that the managers of resilience have a tailor-made approach for each system to ensure required resilience.

STRUCTURAL RESILIENCE aims at the structural elements in developing resilience of the smart critical infrastructure system itself, to advance its performance continuity. It focuses on strategy and structure of the system and ensures the fundamental step to increase the resistance against any disruption. Since the focus is on resilience aspects that are internal to a system, it is easier to implement and control the structural resilience in a system. It comprises of three different lenses i.e. redundancy, modularity and requisite diversity, cf. Figure 11 [34].

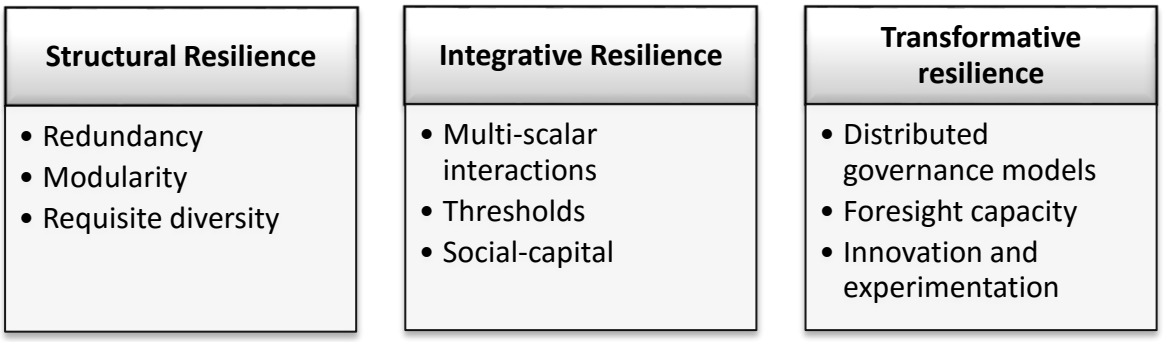

Figure 11: Resilience elements [34]

[9] These "levels" are not to be mixed up with the "levels" used in the SmartResilience concept as described in chapter 3.1, which refer to "dimensions", "issues", and "indicators" of resilience.

By introducing and keeping **redundancy** or putting in place buffers or spares in the system, it can absorb the impacts of shocks. These buffers create costs to the system; however, they provide protection during the critical failures and keep the system running. Furthermore, it is critical to assess the costs and benefits of this aspect to understand the trade-offs between resilience and efficiency.

Modularity can be understood as a form of decentralization, where the components of an infrastructure system are structurally separate, to avoid the cascading impact of failures, making it less vulnerable to shocks. It also improves the "exchangeability of individual components" and permits the system to be dynamic and flexible. Furthermore, it allows for scaling up or scaling down, thereby increasing the adaptive capacity of the system. On the other hand, the increased independence of the components could reversely impact the uniformity of the system, and thereby causing safety and risk tolerance problems. These issues can be overcome by governance frameworks based on principles, standards and strong culture.

Requisite diversity in areas relevant for a particular system at a particular time is crucial to develop an adequately responsive system. It could include people, systems, strategies, methods, services, suppliers [34].

INTEGRATIVE RESILIENCE stresses on the complex interconnections of an infrastructure system with its environment, for example, transportation with energy supply or disaster management infrastructure. Its premise is that a system is embedded in large complex natural-social-economic system, and that the system is the product of and influenced by various factors and stakeholders. Alternatively, it also constitutes the overall system. Thus, this approach requires an opening of focus from system or entity to a larger system it is connected with. The main concerns of integrative resilience are **multi-scaler interaction, thresholds and social capital**.

Multi-scalar interaction determines the emergent behavior of a system in relation to the scales of a larger system within which it is embedded. This idea is also acknowledged by the idea of systems thinking, which assumes that natural-social-economic systems consist of different scales. One way of mapping the interactions is to define the spatial scale of system at focus and take the step up and down in scale into consideration. Another way is to determine the temporal scale of the system and take diverse time scales into account. This approach is a necessary step to ensure successful and resilient systems.

Systems are called so as they are bounded by **thresholds**. Once these thresholds are reached, systems are vulnerable to changes. To ensure the resilience of a system from change or shocks, it is imperative to know the system drivers, respective thresholds, identify its systemic position and trajectory, increase its capacity to adapt and strive to strengthen the surrounding system's resilience against unwanted changes. Furthermore, it is crucial to track the status of the system and create feedback loops through which essential information about the position of the system with respect to the critical thresholds can be analyzed. Effective adaptation and mitigation of risk require time, and hence early detection. Best-possible understanding and effective communication of risks are crucial to ensure a resilient approach [34].

Social capital is a subtle element addressed by integrative resilience. Building social capital enables psychological change, creates trust in the advent of crises and supports in stressed situations. It requires long-term engagement of the stakeholders involved directly and indirectly such as government, businesses, consumers, suppliers, etc. This engagement ensures benefits beyond risk mitigation. An active engagement can boost citizen responsibility to own public infrastructure, protect against a possible perceived threat and raise concerns about the required changes to meet the present and future demands.

TRANSFORMATIVE RESILIENCE is the ability to "reorganize, restructure, and even reinvent when appropriate, both in response to and in anticipation of system changes". It allows for improving the adaptability of the critical infrastructure to both abrupt and slow yet critical changes and hence, leads to ultimate level of resilience. It adds a longer time scale and thus opens up the spectrum to allow and foster system's transformability. This proactive approach relies on **distributed governance models, foresight capacity, and innovation and experimentation** as its enablers.

Distributed governance suggests management should be done from multiple-points of authority involving multiple levels, rather than from a single decision-making point. However, it can be a problem rather than a solution due to delays in communication and response. Hence, taking this approach requires cautious planning.

Foresight capacity is the ability to "actively engage with future events that are inherently uncertain and have an unquantifiable probability of occurrence". It helps foresee the opportunities and also decrease the risk

exposure for the infrastructure. It requires identifying plausible future scenarios and devising their implications on current decisions and scopes in the uncertainty into the planning process, thereby, increasing the resilience and reducing the vulnerability from future risk events.

Innovation and experimentation relies on the principle of learning by doing [34]. A resilient system does not depend on one strategy, method, product, etc. rather it innovates and self-renews itself over time [34]. For example, in insurance industry, financial stress-testing of the system is conducted to understand possible scenarios and plan accordingly.

2.4.4.3 Conclusions for SmartResilience

These levels of resilience and their elements are important for the SmartResilience project, considering the aim of a holistic approach, and the targeted analysis of interdependencies between (smart) critical infrastructures, and cascading effects (see chapter 3). Thereby, especially the integrative resilience could be an important area to focus.

However, experience from the insurance partner (SwissRe) shows that

- A cautious approach needs to be taken while planning for distributive governance i.e. multiple points of authority to avoid communication and response delays.
- Alternatively, it is suggested to have a single point of management through 'single Resilience officers' to deal with all issues
- In addition, it is stressed upon the simplicity of system, for example simplifying the calculation of the damage for insurance payments or reducing the time of reimbursement by having a single point of contact.

2.4.5 Standards pertaining to SmartResilience

2.4.5.1 The standards for resilience

Safety and security are primary concerns in any system including critical infrastructure in the endeavor to improve the resilience. Every European citizen expects these critical infrastructures such as transport, energy, water, healthcare, etc. to be safe and reliable. One of the ways to address this expectation is to deploy standards as they provide benchmarks and standard operating guidelines. They are also instrumental in providing fundamental basis for government policies and legislations, they are often referenced by the regulators, and more importantly, they play a crucial role in European Union's policy for a better technical, legal and bureaucratic coordination in the market [7]. Furthermore, they offer a strong foundation for the development of new technologies in the industry by opening up the market access, provide economics of scale and increase awareness of consumers to make an informed decision [29].

The International Organization for Standardization is an independent, non-governmental international organization with a membership of 161 national standards bodies. It develops and publishes international standards.

2.4.5.2 Understanding of resilience in standards

As articulated in its ISO 22300 standard on Societal security -- Terminology, resilience is defined as "adaptive capacity of an organization in a complex and changing environment" [22].

Since standardization enhances the safety and resilience of smart critical infrastructures to deal with issues such as uncertainty and complexity related to unforeseen risks [24], a review of pertinent standards are considered as important building block in the framework of this report.

This review addresses an inventory prepared by the ISO Strategic Advisory Group on Security (SAG-S). It encompasses three broad areas [24].

1. The standards associated with targets such as people, infrastructure and other assets [33]
2. The standards associated with security threats [30]
3. The standards associated with temporal dimensions of a large scale natural disaster or terrorist attack [31]

The list of these standards is provided in Annex 1.

2.4.5.3 An Integrated Risk and Resilience Framework of Standards for SmartResilience

In order to structure the standards crucial for SmartResilience, an Integrated Risk and Resilience Framework of Standards has been developed (Figure 12), in which the standards have been categorized under the domain-specific standards, and under the risk and resilience standards.

Domain-specific standards include ISO 9001, 14001, 14011, 26000, 27000, 45000, application specific standards (e.g. water, energy, grid, transport, gas), and company specific standards (e.g. insurance). The risk and resilience standards comprise of standards such as ISO 31000, 31010, 23300, ISO Guide 73: 2009, ISO/IEC Guide 51: 2014, and international regulations.

Figure 12: Integrated Risk and Resilience Framework of Standards for SmartResilience (created by EU-VRi)

2.4.5.4 Conclusion about the considered standards for SmartResilience

These standards provide definitions and frameworks for developing a baseline for the SmartResilience concept. Moreover, they are internationally recognized and tested at different scales.

Many of the member states may already be using these standards, however a coherent deployment of these international standards within the EU could be a crucial aspect to increase the resilience of critical infrastructure and also to address the issue of harmonization across the member states, as also discussed in sub-chapter 2.4.4.4.

A most noteworthy point is that the standards reviewed are relevant in contributing to the resilience of smart critical infrastructure in different phases. For instance, the CWA 16449 is an important standard to assess the risks related to technology during the phase when the risks are emerging, while several standards are applicable during all phases, as Figure 13 illustrates. Furthermore, these standards also provide for indicators that can be used in WP4.

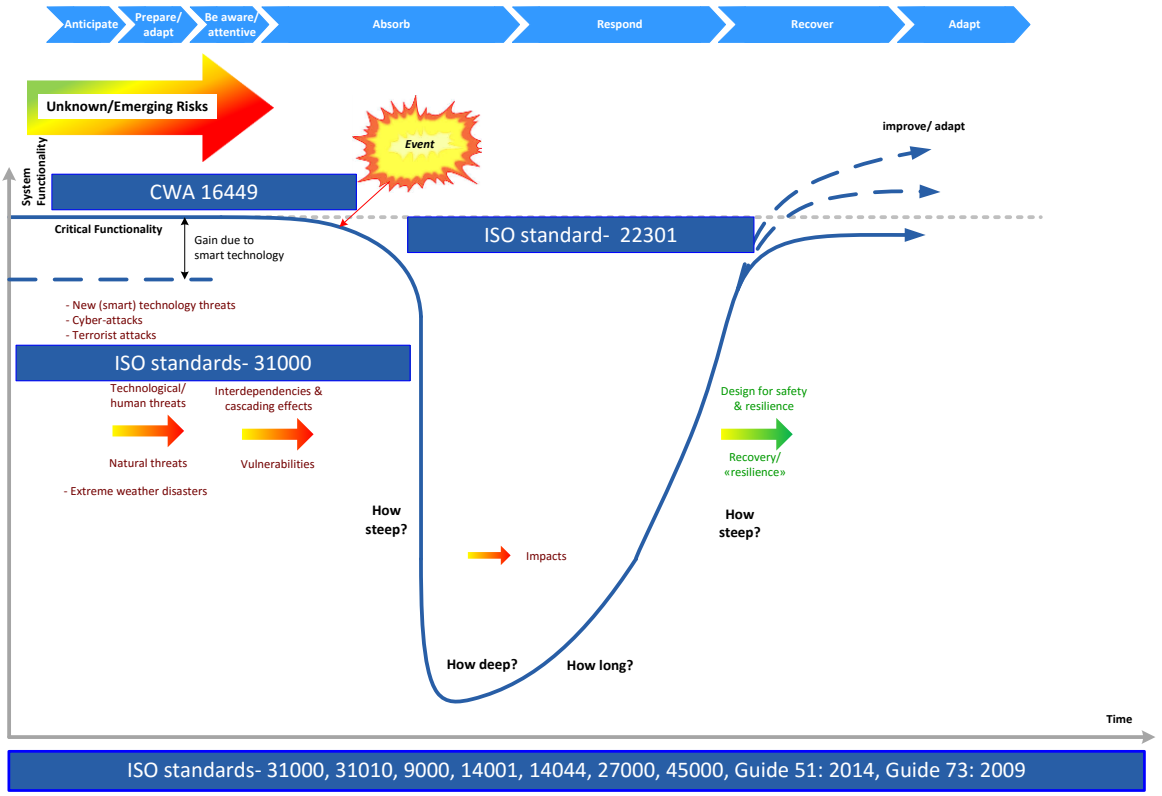

Figure 13: Standards relevant in different phases of the resilience cycle

Risk and resilience standards

ISO 22301 – Societal Security: Business Continuity Management System is one of the most important standards for the resilience of smart critical infrastructure during the response and recovery phase of the incident. It provides standards for the protection of society from, and **in response to incidents, emergencies and disasters** caused by intentional and unintentional human acts, natural hazards and technical failures [41]. It also stresses on the need for a well-defined incident response structure. This can ensure that when incidents occur, responses are escalated in a timely manner and people are empowered to take the necessary actions to be effective [41]. Life safety is emphasized and it also stresses that the organization must communicate with external parties who may be affected, for instance if an incident poses a noxious or explosive risk to surrounding public areas [41]. These aspects of the ISO 22301 standard could be applied to improve the transparency, reliability, adaptive capacity and hence, the resilience of critical infrastructure. Moreover, other standards are also equally essential for ensuring the success of resilience of smart critical infrastructure.

- **ISO 31000 standard for risk management** helps the systems to perform well in an environment of uncertainty. Hence, for critical infrastructures this standard is of high significance during all phases as the conditions these infrastructures operate in are subjected to changes and unknown risks, and require ability to manage these risks and adapt at a faster pace. This **standard is supported by ISO 31010**, i.e. risk assessment techniques on risk management. It can aid decision makers to comprehend risks that could affect the attainment of objectives and the adequacy of the controls previously in place. **ISO/IEC 31010:2009 focuses on risk assessment concepts, processes and the selection of risk assessment techniques**. Furthermore**, ISO Guide 73:2009, Risk management - Vocabulary complements ISO 31000** by providing a collection of terms and definitions relating to the management of risk [20].
- **The ISO/IEC Guide 51: 2014 guide offers practical guidance to drafters of standards to assist them to include safety aspects in standards.** This guide considers the complete life cycle of a system (including both the intended use and the reasonably foreseeable misuse) with the goal to achieve tolerable risk for people, property and the environment, and to minimize adverse effects on the environment. Since, the safety aspect is central to critical infrastructure, incorporating this guideline

into all the standards may reduce risk that can arise in the use of products or systems, including use by vulnerable consumers [25].

- CWA 16449 is complementary to the International Standard ISO 31000 and the Risk Governance Framework developed by the International Risk Governance Council. It is about improving and managing emerging technology-related risks, based on the integrated-risk and Emerging Risk Management Framework for new technologies in European industry. This standard is useful in the phase where the risks are in an emergent phase.
- Lastly, the international regulations provided by FEMA and SENDAI are elaborated in other sections within chapter 2.

Domain-specific standards

- ISO 9001 [41] , can ensure the quality and consistency as a base for all the management systems applied to improve the resilience during all phases of critical infrastructure resilience management.
- ISO 14001 and ISO 14044 could enhance the environmental performance of the infrastructure in a systemic way [27]
- ISO 26000 is based on the premise of developing a relationship between the society and the business or organization. It can help with integrating, implementing and promoting socially responsible behavior through policies and practices, help in identifying and engaging important stakeholders and with communicating commitments, performance and other information, thereby improving the transparency of the project [21]. Again, this standard needs to be integrated during all phases.
- ISO 27000 group of standards helps with keeping the information assets secure and enhancing cybersecurity, crucial for safety and security of critical infrastructure from any cyber-attacks. It includes people, processes and IT systems by applying a risk management process [23].
- Applying ISO 45000 standard providing guidelines for Occupational health and safety management (OHSM) prevents and combats significant injuries and diseases that may result in losses. It intends to improve safety, reduce workplace risks and create better, safer working conditions and hence, can improve the adaptive capacity of the critical infrastructure and its services [26].
- The application specific standards provided in annex 1 are directly related to the critical infrastructures under the purview of SmartResilience, such as water, energy, grids, transport, gas and pipelines, etc.

3 Framing resilience for SmartResilience

After reviewing the results of recently conducted comprehensive reviews on resilience definitions and concepts, and the approaches of important organisations including standards, the initial definition and concept as described in chapter 2.2 is now being updated. This shall provide a concept, which is used and possibly adapted in the further course of SmartResilience. In addition, further suggestions complementing the concept are derived.

The reviews provided useful insights not only regarding definitions and concepts of resilience, but also regarding further aspects that are considered useful for other parts in SmartResilience, which are also summarized in this chapter.

Insights are captured bearing in mind that the reviewed definitions, concepts and approaches are based on their specific objectives and contexts, which in most cases will differ from SmartResilience. Therefore, some are more useful for us than others. Some definitions, concepts and approaches are abstract, theoretical and quite complicated. Also, some approaches are application-oriented and could be seen as examples for identifying real application based indicators and their methodology in WP3 and 4. We aim at pragmatic, practical and easy to understand and communicate definitions, concept and approaches; however, for some parts of the project, more complex approaches may be needed.

3.1 "Dimensions" and "issues" of resilience

Following the initial definition, resilience comprises seven "dimensions/ phases" – we will call them **"dimensions"** from now on –, ***anticipate***; ***prepare/ adapt***; ***be aware/ attentive***; ***absorb***; ***respond***; ***recover***; and ***adapt***. In addition, an eighth dimension, ***risk understanding***, has been proposed.

As the "fundamentals" of resilience, the RESOLUTE project describes the conditions "avoidance", "survival", and "recovery" (cf. chapter 2.3.4). These conditions are mainly seen as reflected by the dimensions in our initial definition. However "avoidance" includes the aspect to "prevent something bad from happening", which can be a result of e.g. preparing or absorbing, but it is not directly addressed. It can be elaborated in WP3, if and in which way this aspect should be addressed.

The SMR project concludes after a comprehensive review of resilience articles that **"absorb shocks", "ability to adapt", and "ability to recover or 'bounce back'"** are components of most common definitions, which is totally in line with our initial definition. Regarding "adapt" and "bounce back", several definitions only aim at one of these directions, targeting either to return quickly after a shock to the pre-defined state ("bounce back"), or targeting a change of the entity or system, while providing the same service or filling the same operational niche as before ("adapt") (cf. results of the DARWIN and IMPROVER projects). Also the two types of resilience as described by the RESOLUTE project, "engineering resilience" and "ecological resilience", can be understood as representing these to point of views – bouncing back vs. adapting. Our definition is rather related to the latter, however: DARWIN sees a relation of the two components to the attributes **"ability" and "capacity"**, which are most commonly used. While we do not explicitly distinguish these two attributes (ability versus capacity), all dimensions of our initial definition can have an "ability aspect" and a "capacity" aspect. It could be analysed in WP3, if it is useful to distinguish between these two attributes.

As described in chapter 2.4, OECD has included a description of the *risk landscape* as part of the resilience systems analysis. This supports the idea of including ***risk understanding*** as a first dimension in SmartResilience. Understanding the risks you are facing is obviously a prerequisite for knowing what to do about them.

The capacities related to **adapt and transform** may be useful to consider, since OECD distinguishes between incremental change (adapt) and fundamental change (transform). It may also be useful to consider where to include *adaptation* in the resilience time line, since this may take place at several stages in the development of a disruption (and the preparations for disruptions). It is too early to decide on this now, and make changes to the initial definition with respect to "adapt/transform", but it can be followed-up in WP3.

In this context, it will also be helpful to reflect on findings from the RESILENS project. Following a qualitative discussion on key literature, RESILENS derives a definition of critical infrastructure resilience that includes the "transformative" character as a main component, and also lists key elements that indicate the transformative understanding of resilience (see chapter 2.3.3).

The UNISDR definition, on the other hand, does not include the "transform" characteristic, but rather concentrates on the "recover" or "bouncing back" attribute (see chapter 2.4.1).

The definition and approach undertaken by USDHS/FEMA includes "prepare", "absorb", "recover" and "adapt" and "transformative capacity" attributes.

The definition of resilience in Standard 22300 for Business continuity management stresses on the "adaptive capacity" attribute to deal with the complex and changing environment and focuses on the stage after an event has happened. However, there are other standards which apply during the remaining resilience cycle as illustrated in Figure 14.

From the industry perspective, the definition of resilience focuses on "absorb" and survive, and adapt and even better **"adapt to grow"** to deal with issues of change and uncertainty.

In SmartResilience, focusing on resilience, the dimensions described in Chapter 2.2 are the "aspects" we want to measure; however, we do not measure the dimensions directly. We first define *issues* that are important for the success of the dimension, e.g. the success of response. These issues are in turn measured by indicators.

The *dimensions*, e.g. response, are included as part of the resilience definition. We can denote this as **level 1**, whereas the more specific *issues* affecting the dimensions are at **level 2**. The *indicators* are then at **level 3**. This is illustrated in Figure 14, including illustration of the two different approaches of obtaining indicators, which will be pursued in SmartResilience.

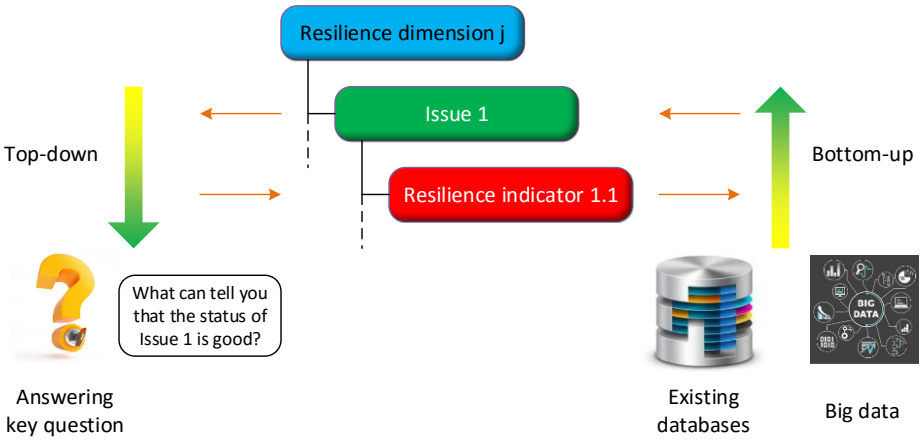

Figure 14: Dimensions, issues and indicators

When we refer to attributes of resilience being on two levels, we refer to level 1 as the dimensions included as attributes in the resilience definition, whereas other attributes are specified as issues on level 2. It is to some degree a matter of preference or suitability, whether a resilience attribute is included on level 1 or level 2.

When we try to measure and assess resilience, it is crucial that we **capture the most important resilience abilities (through dimensions and issues)**. The indicators can never be better than the suitability/relevance/ representativeness of the dimensions and issues we try to measure.

As described in chapter 2.4, OECD included only four dimensions in their definition of resilience (i.e. on "level 1"), whereas many more abilities were included in the subsequent explanation/definition of the dimensions (i.e. on "level 2").

3.2 Resilience and its relation to vulnerability and risk management

As amongst others described by the IMPROVER project, there are different understandings regarding the relation of resilience to vulnerability, mainly as a result of different definitions of the two terms. Key parameters of vulnerability are seen in the exposure, susceptibility, and coping/ adaptive capacity of elements. Often discussed is the question, if the resilience and vulnerability should be treated as positive and negative poles on the same continuum, or as two completely different concepts. Some authors follow the first approach, amongst others concluding that vulnerability of a system results from reduced resilience. However, other authors see an overlap between the two concepts, assuming that many characteristics influence only the vulnerability or only the resilience of a system, while other characteristics influence both. The SmartResilience understanding follows the latter, since there is **a *partial* overlap of the components of resilience** (see the "dimensions" described above) **with the parameters of vulnerability**.

Following the initial definition as described in chapter 2.2, resilience management "includes risk analysis as a central component". Thereby, risk analysis "depends on characterization of the threats, vulnerabilities and consequences of adverse events". The understanding of risk analysis being included in resilience management is slightly adapted:

According to OECD [39], resilience is about "what to do about the risks" (which in turn is increased due to vulnerabilities in the system in focus). Resilience systems analysis build on, rather than replaces, traditional risk management approaches. The "extensions" consist of e.g. complexity and inter-linkages of different risks, going beyond the "known knowns" to also account for uncertainty and change, understanding the importance of power relations, and cover risks at different levels or "layers of society" (i.e. households as well as communities). OECD stresses that resilience systems analysis *build on* traditional risk management approaches. This should indicate that, from an OECD point of view, resilience management does *not include* risk management in the sense that all of risk management is performed within resilience management. The risk analysis part of risk management is quite comprehensive. It would make sense that resilience management uses this as an input, instead of performing the risk analyses. One way to characterize the relation between resilience and risk is that resilience management has a very wide scope, building on risk management, which has a "correspondingly" deeper (but narrower) scope.

The perspectives as described by the RESILENS project comprise the understandings of resilience as (1) a goal of risk management, (2) a part of risk management, (3) an extension of risk management, and (4) an alternative to risk management. The SmartResilience understanding of **resilience management building on risk analysis**, following the OECD approach, thus sits somewhere between (3) and (4), since on the one hand, resilience does not comprise everything of what risk management covers, but on the other hand also cannot replace risk management, since e.g. risk analysis is seen as important basis for resilience, however not included in resilience.

This is also in line with other definitions (even though not explicitly discussing the relation of the two approaches), such as the UNISDR understanding "prevent new and reduce existing disaster risk … and thus strengthen resilience" (see chapter 2.4.1).

3.3 Resilience of what, for whom, and against which threats

Regarding the question, for which element(s) resilience is investigated ("**resilience of what**"), different views are possible.

The review conducted within the DARWIN project concluded in principal "two major entities, system and community […] as dominant concerning the element that is resilient".

In the SMR project, tentative definitions for resilience for different environments and with regard to different systems are given, e.g. for critical infrastructure resilience, community and social resilience, urban or city resilience, or organizational/ local government resilience.

OECD [39] focuses on six categories of assets or capitals, which a community depends on. The six assets/ capitals are human, political, natural, social, physical and financial. These assets/capitals affects the OECD

dimensions of resilience (absorptive, adaptive and transformative capabilities), and is comparable to the "issues" in SmartResilience (referred to in chapter 3.2). OECD has a very broad scope, so (critical) infrastructures would only be one possible type of asset/capital within the physical category. OECD is focusing on resilience of different layers of society, capturing any asset/capital that affects the society in focus.

The systems addressed in SmartResilience will cover both social and technical dimensions and how they are intertwined. In other words, SmartResilience interprets “system” as a socio-technical system, in line with perspectives found in the science, technology and studies (STS) literature. For all case studies, it will be necessary to define boundaries of the system, and it is likely that several different organizations will be covered even in one case study. As a complement, it will also be relevant to examine resilience at organizational level, i.e. to study how single organizations work with resilience. The International Standard Organization (ISO) offers excellent guiding to understand and analyse organizational resilience, by establishing the principles for organizational resilience and identifying the attributes and activities that support an organization in enhancing its resilience.

When **applying the concept of resilience to (smart) critical infrastructure**, it will be necessary to reflect on its specific characteristics. The effects of changes due an increased “smartness” of infrastructure, related challenges, and thus effects on the resilience of infrastructure, will be analysed in WP2. However, regarding the application to critical infrastructure, issues to be considered have already been identified (see findings from IMPROVER, chapter 2.3.1):

Due to the service character of critical infrastructure, the ability to provide a minimum level of service during interruptions, the identification of an acceptable level of inoperability, or the time needed to return to normal operability, are seen as important resilience factors. Another factor of critical infrastructure resilience is seen in redundancy, i.e. the substitutability of infrastructure components. Further, since infrastructures are usually strongly interconnected, a well-organised planning across sectors is seen as a relevant criterion for being resilient. However, it is also noted that these “performance” characteristics are not easy to measure. Also related to the interconnectedness, is the notion that it could be useful to analyse critical nodes, or centrally vs. locally installed steering components. These aspects reflecting specific characteristic of critical infrastructure resilience, could be integrated e.g. in terms of “issues” on level 2 of a resilience concept (cf. chapter 3.1). Another possibly very helpful source for identifying “issues” representing specific “dimensions” of resilience are the standards as described in chapter 2.4.5, which focus on different phases of the resilience cycle and/ or specific domains.

Related to elaborations on critical infrastructure resilience, also other approaches focusing on the **systemic characteristics/ interdependencies** are of specific interest for SmartResilience. For example, USDHS/FEMA uses a concept of interconnectedness between social, technical, environmental, economic and political drivers, to explore the impact on the emergency management field and further prepare for future unknown problems. This only reassures the focus of system characteristics and interdependencies. In this context, the three categories of resilience “structural resilience”, “integrative resilience”, and “transformative/ adaptive resilience” as used in the proposal, and further described in chapter 2.6, seems most promising.

For the relation of different elements or systems being in focus of a resilience assessment, different approaches a possible. For example, organizational aspects can be included in an overall analysis of a specific critical infrastructure, while “organizational resilience” can also be seen as separate approach, besides for example community resilience, or critical infrastructure resilience. It has also been proposed (see results of IMPROVER D1.1, chapter 2.3.1) to distinguish between “internal resilience”, i.e. resilience of the specific infrastructure that is affected, and “external” resilience, i.e. the resilience of all other elements or systems that are affected by the disruption of the infrastructure.

In SmartResilience, resilience of smart critical infrastructure is focussed, but since also diverse interdependencies and cascading effects are analysed, resilience of other systems is also addressed, directly or indirectly. E.g., for the analysis of specific parts of an SCI, it can make sense to analyse organizational issues, if this is a relevant aspect of resilience of this particular SCI. Since a holistic approach is targeted, it seems useful (to be further investigated in WP3) to concentrate on “smart critical infrastructure resilience”, and thereby include issues of involved elements, instead of introducing separate definitions of resilience for different environments/ systems. When elaborating the interdependencies, it could also be useful to analyse

if and in how far the possibility of changed needs from a community during a disaster placing new demands to infrastructure services, as mentioned in chapter 2.3.1, should be included in the methodology.

OECD [39] proposes four critical scoping questions which are important in order to set the right scope for the analysis. The scope should be narrow enough to ensure that it is workable, realistic and useful for practitioners. The four scoping questions are: (1) Resilience of what system?, (2) Resilience to what risks?, (3) Resilience for whom?, (4) Resilience over what timeframe?

The first question has been addressed above. We will now address also the second and third question, while the last question is not considered relevant for SmartResilience, since it is expected that the methodology and its indicators will capture the status quo, and is not per se developed for a specific resilience program.

Resilience to what risks? The risks in focus for SmartResilience include terrorist attacks, cyber-attacks, extreme weather events, as well as risks that are specific for each critical infrastructure such as urban floods or solar storms, and cross-cutting issues such as insurance or legislations. The most relevant risks will vary between different critical infrastructures / case studies.

Resilience for whom? This question depends to a large extent on the target layer(s) of society. In line with e.g. UNISDR, SmartResilience will focus on resilience for "a system, community or society". These three terms will capture the broader society, and all relevant organizations that have a stake in the issue, which is important for SmartResilience, since the project builds on case studies of critical infrastructures that involve more than one organization. In addition, it can also mean that a geographical location is specified.

3.4 Glossary for Smart Resilience

As part of an interactive homepage for the SmartResilience project, a glossary has been installed, available in the member area of http://www.smartresilience.eu-vri.eu/ (see screen shot below). The glossary is built on previous inputs from other European projects run by EU-VRi and R-Tech, with supplementary inputs specifically adapted to the SmartResilience project. After agreement with the project partners, the glossary can be made accessible for the public.

The glossary combines several features which make it very useful for the SmartResilience project:

1. First, the glossary is dynamic, since new definitions and terms can be added along the development of the SmartResilience project
2. Second, the glossary allows to insert multiple definitions for one term Multiple definitions are useful in the starting phase of the project, since the framework is not definitively set yet. At a later stage, the glossary will allow users to view definitions according to whether they are used in SmartResilience or not (by selecting the "SmartResilience glossary terms" in the search function). Of course, in case of multiple definitions, project partners need to come to an agreement about which definition should be used.
3. Third, the glossary includes term ID, definition, source and potentially also partner who proposed the term/definition
4. Finally, the word cloud which is integrated in the glossary increases the interactive dimension of the glossary

Figure 15 is showing a list of glossary terms relevant for the SmartResilience project, with source from the European Commission Directive 2008/114/EC. It also shows the various search functions the glossary offers; like search according to terms, definitions or sources. Another useful feature is the "export function" (as Excel or Word).

List of Glossary Items

Search for: Search

Selected source: Sres_COUNCIL DIRECTIVE 2008/114/EC
Record count: 6

Refresh Export to Excel Export to Word
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z **All**

Glossary Term	Definition	Source	View Answer
Critical infrastructure	Critical infrastructure means an asset means an asset system or part thereof located in Member States which is essential for the maintenance of vital societal functions health safety security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions	Sres_COUNCIL DIRECTIVE 2008/114/EC	
European critical infrastructure	European critical infrastructure or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure	Sres_COUNCIL DIRECTIVE 2008/114/EC	
Sensitive critical infrastructure protection related information	'Sensitive critical infrastructure protection related information means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations	Sres_COUNCIL DIRECTIVE 2008/114/EC	
Protection	Protection means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastrutures in order to deter, mitigate and neutralise a threat, risk or vulnerability	Sres_COUNCIL DIRECTIVE 2008/114/EC	
Owners/Operations of ECIs	Owners/Operations of ECIs means those entities responsible for investments in, and/or day-to-day operation of a particular asset, system or part thereof designated as an ECI under this Directive	Sres_COUNCIL DIRECTIVE 2008/114/EC	
risk analysis	Risk analysis means consideration of relevant threat scenarios in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure	Sres_COUNCIL DIRECTIVE 2008/114/EC	

Figure 15: Glossary Output Example

4 Conclusion and Outlook

4.1 Elements of the initial definition and concept not touched after review

Results of the reviews as described in chapter 2 led to revising, adapting and complementing the initial definition and concept, which was developed for the SmartResilience proposal. But this does not concern all parts of the initial understanding; specific aspects are totally in line with review results and do not require to be touched again.

This concerns the general understanding that resilience can be visualized via a V-, or U-curve in a time versus system functionality axis system (see figures in chapter 2.2). However, instead of specific characteristics of this curve such as its slope, indirect measurements of resilience using indicators are focused in SmartResilience. Also the view that this curve is not sufficient to represent interdependencies and cascading effects keeps unchanged.

Another aspect, which is not changed but seems important for the understanding of resilience of smart critical infrastructure, is the assumption that an increased smartness can increase functionality of a system, but also the vulnerability of functionality, influencing the resilience (see chapter 2.2).

4.2 Using, adapting, and further developing the resilience concept in SmartResilience

When starting this work, reviewing the results of already conducted comprehensive reviews on resilience, other concepts from relevant stakeholders, and revisiting the initial definition and concept, it was not clear to what extent the initial definition and concept would change afterwards. But since the initial definition was already tailored towards the specific use in SmartResilience, it is not too surprising that at least the specific definition is only slightly changed – by including "risk understanding" as further component, resulting in the definition:

Resilience is the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption.

This definition is supposed to serve as a starting point for the further work in SmartResilience. However, it is still an "initial" one, since it might be adapted in the further course of the project, especially the work package elaborating the overall methodology – WP3.

Besides complementing the specific definition by another dimension, the initial concept of resilience in a broader sense – including further framing questions such as resilience "of what" is in focus, what is the relation to vulnerability or risk management, how should the different levels and components of resilience be categorised – is adapted and complemented, as elaborated in chapter 3. This includes the understanding of resilience building on risk management (rather than including it). Further, the reviews revealed additional perspectives that might be included in the concept at a later stage, as a result of the upcoming work on the actual methodology (WP3), and the application to specific SCI's (WP2, WP5). Also the glossary (see chapter 3.4) will be updated continuously.

4.3 Further observations useful for SmartResilience

If during the reviews, we stumbled over aspects that do not directly feed into the discussion on concept and definitions of resilience, and its implications for other WPs, but that seemed to be relevant for other parts of SmartResilience, these aspects have not been ignored, but are summarised below.

A statement identified from the review of selected results from the DARWIN project (chapter 2.3.1) is that the *maturity* of approaches to improve critical infrastructure resilience is "towards the lower half of the maturity spectrum, roughly between the concept and early demonstration phases". This could be seen as a

"motivation" when developing, testing, and applying the SmartResilience methodology, i.e. to strive for mature methods and tools resulting from SmartResilience.

The SMR project (chapter 2.3.4) has included an overview on projects that deal with critical infrastructure, and mapped which project focuses on which type of threat. In the specific analysis of SCI's in WP2 and WP5, this could be a helpful source to exploit respective results from previous projects.

OECD (2014) includes *indicators to measure resilience* of main components of the system over time. They use a five level scale to provide scores for each asset/capital, summarize this for each of the six assets/ capitals, and finally provide an overall result for all six assets/capitals. This has similarities with the approach considered for SmartResilience, and may provide useful input to the development of the methodology in WP3.

References

[1] Australian Government (2010). Critical Infrastructure Resilience Strategy. ISBN: 978-1-921725-25-8. Available at: http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf.

[2] Bång, M., Rankin, A. (2016). SMR – Smart Mature Resilience. D1.3 Multidisciplinary Literature Synthesis. http://smr-project.eu/resources/literature/, accessed July 24, 2016.

[3] Boin, A. and Magnus E. (2009). Preparing the World Risk Society: Towards a New Security Paradigm for the European Union, in: Journal of Contingencies and Crisis Management, Volume 17, Issue 4: 285-294, Blackwell Publishing Ltd

[4] Boin, A.; Ekengren, M. and Mark R. (2013). The European Union as Crisis Manager. Patterns and Prospects, Cambridge University Press, New York

[5] Bremberg, N. and Malena. B. (2009). Uncovering the Diverging Institutional Logics of EU Civil Protection, in: Cooperation and Conflict, Vol. 44(3): 288–308. Sage Publications

[6] Clarke, J. et al. (2015). RESILENS – Realising European ReSILiencE for Critical INfraStructure. D1.1 Resilience Evaluation and SOTA Summary Report. http://resilens.eu/wp-content/uploads/2016/01/D1.1-Resilience-Evaluation-and-SOTA-Summary-Report.pdf, accessed July 24, 2016.

[7] ETSI. (2016). Why we need standards. Retrieved June 21, 2016, from http://www.etsi.org/standards/why-we-need-standards

[8] European Commission (2008). Council 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. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114, accessed July 21, 2016.

[9] European Commission (2012). Communication from the Commission to the European Parliament and the Council. The EU Approach to Resilience: Learning from food security crises. European Commission. COM(2012) 586 final. http://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf. Accessed July 22, 2016.

[10] Federal Ministry of the Interior. (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy)[online]. Berlin, Germany, 2009 [cit. 2014-10-28]. Available at: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

[11] Federal Ministry of the Interior. (2011). Cyber Security Strategy for Germany [online]. Berlin, Germany, 2011 [cit. 2014-10-29]. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

[12] FEMA. (2012). Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty. Federal Emergency Management Agency. Washington, DC. http://www.fema.gov/media-library-data/20130726-1816-25045-5167/sfi_report_13.jan.2012_final.docx.pdf

[13] Federal Office of Civil Protection and Disaster Assistance (BBK). 2014: LÜKEX Leaflet 2014, available at:

http://www.bbk.bund/de/SharedDocs/Downloads/BBK/DE/Publikationen/Broschueren_Fyler/Flyer_Luekex_2014_eng.pdf?__blob=publicationFile

[14] FEMA. (2012). Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty. Federal Emergency Management Agency. Washington, DC. http://www.fema.gov/media-library-data/20130726-1816-25045-5167/sfi_report_13.jan.2012_final.docx.pdf

[15] FEMA. (2014). FEMA Strategic Plan 2014–2018. Washington, DC. Retrieved from http://www.fema.gov/media-library-data/1405716454795-3abe60aec989ecce518c4cdba67722b8/July18FEMAStratPlanDigital508HiResFINALh.pdf

[16] Ferreira, P. and Simões, A. (2015). RESOLUTE D2.1 State of the art review and assessment report. http://www.resolute-eu.org/files/653460_State-of-the-Art-review-and-assessment-report.pdf, accessed July 24, 2016.

[17] Francis, R. & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering & System Safety, 121 (January), 90–103. http://dx.doi.org/10.1016/j.ress.2013.07.004, accessed on July 19, 2016.

[18] Gunderson, L. et al. (2002). Resilience of large-scale resource systems. In Gunderson, L., Holling, C. (eds) Resilience and the behaviour of large-scale system. Washington, DC, USA: Island Press Hale et al (1998).

[19] Holling, C. (2010). Engineering resilience versus ecological resilience. In Gunderson, L., Allen, C., Holling, C., (eds) Foundations of ecological resilience. (pp 51-66) Washington, DC, USA: Island Press.

[20] International Organization for Standardization. (2009). ISO/ IEC Guide 73:2009 Risk management - Vocabulary. Retrieved June 20, 2016, from http://www.iso.org/iso/home/standards/iso31000.htm

[21] International Organization for Standardization. (2010). Social responsibility. Retrieved June 20, 2015, from http://www.iso.org/iso/home/standards/iso26000.htm

[22] International Organization for Standardization. (2012). ISO 22300 Societal security — Terminology. Retrieved June 13, 2016, from https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-1:v1:en

[23] International Organization for Standardization. (2013). Information security management. Retrieved June 20, 2016, from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[24] International Organization for Standardization. (2014). ISO/TC 292 Security and resilience. Retrieved June 14, 2016, from http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=5259148

[25] International Organization for Standardization. (2014b). Safety aspects -- Guidelines for their inclusion in standards. Retrieved June 20, 2016, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53940

[26] International Organization for Standardization. (2015). Occupational health and safety. Retrieved June 20, 2016, from http://www.iso.org/iso/home/standards/management-standards/iso45001.htm

[27] International Organization for Standardization. (2015a). Environmental management systems - Requirements with guidance for use. Retrieved June 20, 2015, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60857

[28] International Organization for Standardization (2015). ISO 9000 - Quality management. Retrieved June 20, 2015, from http://www.iso.org/iso/iso_9000

[29] International Organization for Standardization. (2016). Benefits of International Standards. Retrieved June 17, 2016, from http://www.iso.org/iso/home/standards/benefitsofstandards.htm

[30] ISO Strategic Advisory Group - Security. (2014a). Inventory of security-related standards Threat Collection - 2014. Geneva. Retrieved from http://www.iso.org/sites/sags/documents/Threat Collection3282014 Final.pdf

[31] ISO Strategic Advisory Group - Security. (2014b). Inventory of security-related standards Timelines Collection. Geneva. Retrieved from http://www.iso.org/sites/sags/documents/Timelines Collection 3272014 Final.pdf

[32] ISO Strategic Advisory Group on Security (SAG-S). (2014). Inventory of standards. Retrieved June 14, 2016, from http://www.iso.org/sites/sags/

[33] ISO strategic advisory Group. (2014). Inventory of security-related standards Target Collection. Geneva. Retrieved from http://www.iso.org/sites/sags/documents/Target Collection 3282014 Final.pdf

[34] Jackson, S. (2010) Architecting resilient systems: Accident avoidance and survival and recovery from disruptions. Hoboken, New Jersey, USA: John Wiley & Sons.

[35] Kupers, R. (eds) (2014). Turbulence. A Corporate Perspective on Collaborating for Resilience. Amsterdam University Press, Amsterdam.

[36] Labaka, L., Hernantes, J., & Sarriegi, J. M. (2015). Resilience framework for critical infrastructures: An empirical study in a nuclear plant. Reliability Engineering & System Safety, 141, 92–105. http://dx.doi.org/10.1016/j.ress.2015.03.009, accessed on July 21, 2016.

[37] Linkov, I. et al. (2014). "Changing the Resilience Paradigm." Nature Climate Change 4(6):407–9. Retrieved (http://www.nature.com/doifinder/10.1038/nclimate2227).

[38] Melkunaite, I. (Ed.) (2016). IMPROVER – Improved Risk Evaluation and Implementation of Resilience Concepts to Critical Infrastructure. D1.1 International Survey. http://improverproject.eu/2016/06/23/deliverable-1-1-international-survey/, accessed on July 19, 2016.

[39] OECD (2014) Guidelines for resilience systems analysis, OECD Publishing

[40] Ostrom, E. (2010). "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." Transnational Corporations Review 2(2):1–12.

[41] Ouyang M., Dueñas–Osorio, L. & Min, X. (2012). A three–stage resilience analysis framework for urban infrastructure systems. Structural Safety, 36–37 (May–July), 23–31. http://dx.doi.org/10.1016/j.strusafe.2011.12.004, accessed on July 21, 2016.

[42] Radianti, J. (2016). SMR – Smart Mature Resilience. D1.2 Survey Report on EU-Sectoral Approaches. http://smr-project.eu/resources/eu-sectoral/, accessed July 24, 2016.

[43] Rankin, A., Bång, M. (2016): SMR – Smart Mature Resilience. D1.1 Survey Report on Worldwide Approaches. http://smr-project.eu/resources/worldwide/, accessed July 24, 2016.

[44] Suter, M. (2011). Focal Report 7: CIP Resilience and Risk Management in Critical Infrastructure Protection Policy. Exploring the Relationship and Comparing its Use. Center for Security Studies (CSS), ETH Zurich. https://www.files.ethz.ch/isn/164305/Focal-Report-7-SKI.pdf, accessed on July 21, 2016.

[45] Swiss Re. (2016). Swiss Re. Retrieved July 19, 2016, from http://reports.swissre.com/corporate-responsibility-report/2014/cr-report/risk-intelligence/the-resilience-action-initiative.html

[46] Tangen, S. (2012). Business continuity - ISO 22301 when things go seriously wrong. Retrieved June 17, 2016, from http://www.iso.org/iso/news.htm?refid=Ref1602

[47] United Nations International Strategy for Disaster Reduction. (2009). UNISDR Terminology on Disaster Risk Reduction, United Nations Office for Disaster Risk Reduction, Geneva. Available at: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

[48] United Nations International Strategy for Disaster Reduction. (2015). The Sendai Framework for Disaster Risk Reduction 2015-2030, United Nations International Strategy for Disaster Reduction, Geneva. Available at: http://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

[49] United Nations Office for Disaster Risk Reduction. Who we are, www.unisdr.org, accessed on June 14, 2016

[50] USDHS. (2014). The 2014 Quadrennial Homeland Security Review. US Department for Homeland Security. Washington, DC. Retrieved from https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

[51] USDHS. (2015). Resilience definition and practice. Retrieved June 7, 2016, from https://www.dhs.gov/topic/resilience

[52] Walker, B., Salt, D. (2006) Resilience thinking: sustaining ecosystems and people in a changing world. Washington, DC, USA: Island Press.

[53] Westrum, R. (2006). A typology of resilience situations. In Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering – Concepts and Precepts. (pp 55-65) Aldershot, UK: Ashgate.

[54] Woltjer, R. (2015). DARWIN D1.1 Consolidation of resilience concepts and practices for crisis management. http://www.h2020darwin.eu/images/documents/DARWIN_D1.1_Consolidate_resilience_concepts_and_practices_for_crisis_management.pdf, accessed July 22, 2016.

Annex 1 Relevant Standards for SmartResilience

Relevant inventory of standards for SmartResilience project from the list published by ISO Strategic Advisory Group - Security (SAG-S) in 2014 [24].

A.1.1 *Inventory of security-related standards Target Collection – 2014*

Scope: This list includes relevant standards associated with *targets* i.e. people, infrastructure and other assets, that may be vulnerable to security threats [33].

A.1.1.1 Information and Communications Technology (ICT)

Document Number	Title	Organization	Status
ISO/IEC 27000	Information Technology Security Techniques Collection	ISO	2016
ISO/IEC 27035 / ISO/IEC 27031	Information technology – Security techniques: incident management ISO/IEC 27035 / ISO/IEC 27031	ISO	2011
ISO/TR 13569	Financial services -- Information security guidelines	ISO	2005
ISO/TR 13569:2005	Financial services -- Information security guidelines	ISO	2005
ISO/IEC 10116	Information technology - Security techniques- Modes of operation for an n-bit block cipher	ISO	2006
ITU-T K.72	Protection of telecommunication lines using metallic conductors against lightning – Risk management	ITU-T	2011
ITU-T X.1520	Common vulnerabilities and exposures	ITU-T	2011
ITU-T X.Sup7	Supplement on overview of identity management in the context of cybersecurity	ITU-T	2009
BS 25999-1	Business continuity management. Code of conduct	BSI	2006

A.1.1.2 Energy

The energy target includes specific assets such as electric utilities, SmartGrid, gas and pipelines, and nuclear power plants. For this review, electric utilities and gas and pipelines standards are reviewed [33].

A.1.1.2.1 Electric utilities

Document Number	Title	Organization	Status
IEC/TR 62210	Power system control and associated communications - Data and communication security	IEC	2003
IEC 62351-SER	Power systems management and associated information exchange - Data and communications security - ALL PARTS&#38	IEC	2012

A.1.1.2.2 Gas and pipelines

Document Number	Title	Organization	Status
ANSI/NFPA 326-2010	Standard for the Safeguarding of Tanks and Containers for Entry, Cleaning, or Repair	NFPA	2009
ANSI/UL 558-2013	Standard for Safety for Industrial Trucks, Internal Combustion Engine-Powered	UL	2013
ISO/AWI 20074	Petroleum and natural gas industries -- Geological hazards risk management of oil and gas pipelines	ISO	2014

A.1.2 *Inventory of security-related standards Threat Collection - 2014*

Scope: This inventory of security threat standards and specifications identifies a collection of documents that provide guidance on meeting the needs posed by organizations concerned about security threats from man-made or natural disasters [30].

A.1.2.1 Natural Disasters

Natural disasters present a wide range of threats to the populace. These standards directly or indirectly address the natural disaster threat such as geological hazards including landslides, mudslides, glaciers and icebergs and meteorological hazards such as flood, flash flood, tidal surge, fire (e.g., forest, range, urban, wildland, and urban interface), snow, ice, hail, sleet, avalanche, windstorm, dust/sand storm – extreme temperatures, and lightning strikes [30], etc.

Document Number	Title	Organization	Status
ISO 31000	Risk assessment	ISO	2009
ISO 37120	Standard for sustainable and resilient cities	ISO	2014
ISO/DTR 37121	Sustainable development in communities -- Inventory and review of existing indicators on sustainable development and resilience in cities	ISO	Under review

A.1.2.2 Cybersecurity threats

Cybersecurity includes disruptive activities, or the threat thereof, against computers and/or networks, with the result of harm [30]. These are covers in the ICT Standards in section A.1.1.1 above in this chapter.

A.1.2.3 Criminal threats

Standards, which relate to criminal threat are those intended to aid in identifying criminals such as biometrics standards those that categorize criminal activities such as fraud and counterfeiting [30].

Document Number	Title	Organization	Status
ISO/IEC 19785-1	Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification	ISO/IEC	2006

A.1.3 *Inventory of security-related standards Timelines Collection – 2014*

Scope: This inventory is limited to those standards associated with timelines – that is, standards associated with the temporal dimension of a large scale natural disaster or terrorist attack. The relevant standard in the category of preparedness and response are listed below [31].

A.1.3.1 Preparedness

Document Number	Title	Organization	Status
ISO 22300	Societal security -- Terminology	ISO	2012
ISO 22301	Societal security -- Business continuity management systems --- Requirements	ISO	2012
ISO 22320	Societal security -- Emergency management - Requirements for incident response	ISO	2011
ISO/PAS 22399	Societal security - Guideline for incident preparedness and operational continuity management	ISO	2007
ISO/TR 22312	Societal security -- Technological capabilities	ISO	2011

A.1.3.2 Response

Document Number	Title	Organization	Status
ANSI INCITS 415-2006	Homeland Security Mapping Standard – Point Symbology for Emergency Management	ITI (INCITS)	
ASTM F1220	Standard Guide for Emergency Medical Services System (EMSS) Telecommunications	ASTM	1995 Reapproved in 2006
IWA 5:2006	Emergency preparedness	ISO	2006
IWA 6:2008	Guidelines for the management of drinking water utilities under crisis conditions	ISO	2008
ASIS BC GDL (2005)	Business Continuity Guideline - A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery	ASIS	2005