End users' challenges, needs and requirements for assessing resilience

Report Title:	*D1.3 End users' challenges, needs and requirements for assessing resilience*		
Author(s):	Katarina Buhr, Anja Karlsson, Johan M. Sanne, Nils Albrecht, Néstor Alfonzo Santamaría, Stian Antonsen, Dmitry Bezrukov, Dragana Blazevic, Lars Bodsberg, Amrita Choudhary, Gábor Csapó, Gerard Desmond, Aleksandar Jovanovic, Peter Klimek, Thomas Knape, István Macsári, József Németh, Nicolas Schmid, Zoltán Székely, Sebastian Warkentin.		
Responsible Project Partner:	IVL	**Contributing Project Partners:**	HNP, UTSTUTT, SINTEF, MUV, BZN, NIS, SRH, EU-Vri, SWH, CoL, CCC

Document data:	File name (QMS compliant):	SmartResilience-D1.3_v07bc07032018		
	Pages:	118	No. of annexes:	8
	Status:	Final	Dissemination level:	PU
Project title:	**SmartResilience**: Smart Resilience Indicators for Smart Critical Infrastructures		GA No.:	700621
			Project No.:	12135
WP title:	WP1: Establishing the project baseline and the common framework		Deliverable No:	D1.3
Date:	Due date:	March 7, 2018	Submission date:	March 7, 2018
Keywords:	Resilience, assessment, indicator, challenge, need, requirement, end user, stakeholder.			
Reviewed by:	A. Heinke		Review date:	October 25, 2016
	R. Schneider		Review date:	October 25, 2016
Approved by Coordinator (EU-VRI):	A. Jovanovic		Approval date:	March 7, 2018

Stockholm, October 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 and respond/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. (#1) By identifying existing indicators suitable for assessing resilience of SCIs. (#2) By identifying new smart resilience indicators including those from Big Data. (#3) By developing a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix. (#4) By developing the interactive SCI Dashboard tool. (#5) By 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 summarizes the results from the work in Task 1.3 of the SmartResilience project. Within the Work Package "Establishing the project baseline and the common framework", Task 1.3 contributes to a better understanding of the indicators for resilience assessment by examining the actual needs from the ones responsible for such an assessment.

This deliverable establishes, at an early stage in the project, a baseline for understanding end users' current and foreseen challenges, needs and requirements for assessing resilience of critical infrastructures and using resilience indicators (RIs) for doing so. This is a necessary step to ensure that the resilience assessment methodology and smart RIs will be designed in ways that are useful and therefore adopted, thus delivering increased resilience for critical infrastructures, beyond the project.

The identification of end users' challenges, needs and requirements in assessing resilience within Task 1.3 has been guided by an actor analysis approach and is predominantly based on qualitative methods, consisting of semi-structured individual or group interviews with key end users connected to critical infrastructures, desktop studies and literature reviews. The task has covered eight critical infrastructures in the SmartResilience case studies (ALPHA-HOTEL) as well as an additional case study covering interconnected critical infrastructures (DSB). Furthermore, in order to take into account end users beyond these nine case studies, a literature review has been carried out as well as a survey among the Members of the Community of Users of Safe, Secure and Resilient Societies (CoU).

The key findings from Task 1.3 are summarized below:

- Designing useful indicators requires extensive end user involvement in order to be able to integrate the indicators into existing organizational processes. There is a need to define the "work" that the indicators are supposed to do and make sure they meet the challenges of interconnected infrastructures.
- End users in the case studies confirmed and provided further insight into the following key challenges, which are illustrated by examples: the concept of resilience; external threats (climate change, cyber-attacks, terrorist attacks, flooding); the complexity of critical infrastructures; and data management.
- End users in the case studies expressed specific needs and requirements, which has been analyzed in terms of five dimensions of resilience and illustrated by examples: system/physical; information/data; organizational/business: societal/political and cognitive/decision-making.
- The survey to the CoU indicated that some actors do not see a need to develop RIs because they think current practices are sufficient. Although the low response rate calls for caution in interpreting the results, the responses suggests a number of challenges for the SmartResilience project. First, the need for the project to create assessments and RIs that

are clearly regarded as providing added value in relation to end users' current and foreseen needs. Second, the challenge to design assessments and RIs that can be widely disseminated, while at the same time taking different contexts into account.

- Three implications for indicator development are suggested. Firstly, indicators should be developed with an appropriate end user in mind. This means posing questions such as: What organization, and what function or user group, will use it? What is their interest in using indicators? What is their legitimacy to spread the indicator in the critical infrastructure? Secondly, indicators should be developed in dialogue with end users, in order to increase the likelihood that they cover areas that are relevant and currently not sufficiently covered; are relevant, understandable and legitimate; and are designed according to end users' own motives for assessing resilience and perceptions of usefulness. Thirdly, indicators should be developed in alignment with end users' organizational processes. This suggests that the project should develop indicators which are easy to understand in order to decrease the dependency of individual expertise and misunderstandings across different organizations; meet the level of capacity of resources that the organization(s) are willing to spend on assessments of resilience; and allow end users to collect, process and share (big) data, taking data security into account.

Table of Contents

1.1 Background 3
1.2 About Task 1.3 and relationship to other tasks and WPs in SmartResilience 3
1.3 Introduction of terminology 4
1.4 Outline of report and responsibilities 5
2.1 Interviews with end users and desktop studies 7
2.1.1 Selection of end users for interviews 7
2.1.2 Individual or group interviews 7
2.1.3 Analysis of results and validation 8
2.2 Literature Review 9
2.3 Survey to Community of Users 9
3.1 Introduction 10
3.2 Contextualizing for what purpose? 10
3.3 Contextualizing indicators to end users 10
3.4 Contextualizing indicator development through end user participation 11
3.5 Contextualizing indicators through integrating with existing organizational processes 12
3.6 Contextualizing indicators to interconnected infrastructures 12
3.7 Summary and conclusions 13
4.1 ALPHA: The City of London – a critical financial hot-spot of the world 15
4.1.1 Introduction 15
4.1.2 Current status working with resilience and assessing resilience 16
4.1.3 Main threats, current challenges, needs and requirements for assessing resilience 18
4.1.4 Foreseen challenges, needs and requirements for assessing resilience 18
4.1.5 Discussion and conclusion 19
4.2 BRAVO: The future-oriented and sustainable community of Bahnstadt, Heidelberg 20
4.2.1 Introduction 20
4.2.2 Current status working with resilience and assessing resilience 22
4.2.3 Main threats, current challenges, needs and requirements for assessing resilience 26
4.2.4 Foreseen challenges, needs and requirements for assessing resilience 27
4.2.5 Discussion and conclusion 28
4.3 CHARLIE: The Austrian health care system 29
4.3.1 Introduction 29
4.3.2 Current status working with resilience and assessing resilience 31

4.3.3 Main threats, current challenges, needs and requirements for assessing resilience 31
4.3.4 Foreseen challenges, needs and requirements for assessing resilience 32
4.3.5 Discussion and conclusion 33
4.4 DELTA: The transportation infrastructure of Budapest airport 34
4.4.1 Introduction 34
4.4.2 Current status working with resilience and assessing resilience 37
4.4.3 Main threats, current challenges, needs and requirements for assessing resilience 37
4.4.4 Foreseen challenges, needs and requirements for assessing resilience 38
4.4.5 Discussion and conclusion 41
4.5 ECHO: An urban large industrial zone in Pančevo 41
4.5.1 Introduction 41
4.5.2 Current status working with resilience and assessing resilience 45
4.5.3 Main threats, current challenges, needs and requirements for assessing resilience 45
4.5.4 Foreseen challenges, needs and requirements for assessing resilience 46
4.5.5 Discussion and conclusion 47
4.6 FOXTROT: Drinking water supply in Sweden 49
4.6.1 Introduction 49
4.6.2 Current status working with resilience and assessing resilience 51
4.6.3 Main threats, current challenges, needs and requirements for assessing resilience 53
4.6.4 Foreseen challenges, needs and requirements for assessing resilience 53
4.6.5 Discussion and conclusion 54
4.7 GOLF: Flooding events in the City of Cork 55
4.7.1 Introduction 55
4.7.2 Current status working with resilience and assessing resilience 58
4.7.3 Main threats, current challenges, needs and requirements for assessing resilience 58
4.7.4 Foreseen challenges, needs and requirements for assessing resilience 58
4.7.5 Discussion and conclusion 59
4.8 HOTEL: Energy supply infrastructure in Helsinki 60
4.8.1 Introduction 60
4.8.2 Current status working with resilience and assessing resilience 62
4.8.3 Main threats, current challenges, needs and requirements for assessing resilience 64
4.8.4 Foreseen challenges, needs and requirements for assessing resilience 65
4.8.5 Discussion and conclusion 66

4.9 DSB: Assessing resilience in interconnected critical infrastructures in Oslo 67
4.9.1 Introduction 67
4.9.2 Current status working with resilience and assessing resilience 68
4.9.3 Main threats, current challenges, needs and requirements for assessing resilience 70
4.9.4 Foreseen challenges, needs and requirements for assessing resilience 71
4.9.5 Discussion and conclusion 72
5.1 Results 73
5.2 Implications of results for usefulness 74
6.1 Introduction 75
6.2 Analysis of current and foreseen challenges 75
6.3 Analysis of current and foreseen needs and requirements 77
6.4 Actor analyses and stakeholder management 78
7.1 Overall conclusions 80
7.2 Results in relation to other tasks in SmartResilience 81
7.2.1 Task 1.3 in relation to previous studies 81
7.2.2 Input from Task 1.3 to forthcoming studies 82
7.3 Implications for resilience assessment methodology and indicator development 82

List of Figures

Figure 1: Example of U-curve: System functionality curve for smart critical infrastructure [79]. 5
Figure 2: London "City" 15
Figure 3: City of Bahnstadt 21
Figure 4: Classification of Critical Infrastructures [17] 21
Figure 5: Bow-Tie Diagram 23
Figure 6: Stadtwerke Heidelberg's Stakeholder Diagram 26
Figure 7: The distribution network today and tomorrow [19] 27
Figure 8: Overview of the Austrian e-card Infrastructure that enables a shared electronic health record system (ELGA) that is currently being implemented throughout Austria. 33
Figure 9: IBCDRP framework for Complete Operation Loss 39
Figure 10: Geographic location of the city Pančevo 42
Figure 11: Southern Industrial Zone of City of Pančevo and nearby settlements 43
Figure 12: The drinking water supply cycle. 49
Figure 13: Aerial view of flooded riverside area in Cork City (CCC) 56
Figure 14: Concept of incident preparedness and continuity management as defined by NESA [45]. 63
Figure 15: Overview of the Sydhavna area and the nearby critical infrastructures. Adapted from [53]. 68
Figure 16: Hierarchy of critical societal functions and capabilities (For illustration). 70
Figure 17: Do you have professional experience of working with any of the following concepts? 73
Figure 18: In your opinion, how does resilience compare to the following approaches in terms of usefulness? Resilience models are.....than.... 73

List of Tables

Table 1: Responsible partners related to the study on end users' challenges, needs and requirements in the different case studies....6
Table 2. . Currrent vs foreseen challenges and current vs foreseen needs and requirements for the critical infrastructure. 8
Table 3. Summarizing challenges, needs and requirements according to the five dimensions of resilience. 9
Table 4. Summarizing the literature review of contextualizing indicator development as a means to making them useful for end-users....13
Table 5: Actor analysis ALPHA 16
Table 6. Challenges, needs and requirements for the ALPHA case. 19
Table 7. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the ALPHA case....20
Table 8: Actor Analyis BRAVO....22
Table 9: 10 Steps to Understand Risks, Threats and Opportunities (Terrorist Attack), adapted from [1] 23
Table 10: 10 Steps to Understand Risks, Threats and Opportunities (Flash Flood), adapted from [1]....24
Table 11: 10 Steps to Understand Risks, Threats and Opportunities (Cyber Security Breach), adapted from [1] 25
Table 12. Challenges, needs and requirements for the BRAVO case. 28
Table 13. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the BRAVO case. 29
Table 14: Actor Analysis CHARLIE....30
Table 15. Challenges, needs and requirements for the CHARLIE case....32
Table 16. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the CHARLIE case. 34
Table 17: Actor Analysis DELTA 36
Table 18. Challenges, needs and requirements for the DELTA case. 40
Table 19. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the DELTA case. 41
Table 20: Actor Analysis ECHO 44
Table 21. Challenges, needs and requirements for the ECHO case. 47
Table 22. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the ECHO case. 48
Table 23: Actor Analysis FOXTROT 50
Table 24. Challenges, needs and requirements for the FOXTROT case. 54

Table 25. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, visualizing and assessing resilience for the FOXTROT case. 55
Table 26: Actor Analysis GOLF 56
Table 27. Challenges, needs and requirements for the GOLF case. 59
Table 28. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the GOLF case. 60
Table 29: Actor Analysis HOTEL 62
Table 30. Challenges, needs and requirements for the HOTEL case. 66
Table 31. Summarizing the most important issues for which the Smart Resilience methodology can be used for identifying, vizualizing and assessing resilience for the HOTEL case study. 67
Table 32. Challenges, needs and requirements for the DSB case. 71
Table 33. Summarizing the most important issues for which the Smart Resilience methodology can be used for identifying, visualizing and assessing resilience in the DSB case study. 72
Table 34: Current and foreseen challenges among end users 75
Table 35: Current and foreseen needs and requirements among end users, in relation to five dimensions of resilience 77

List of abbreviations

Acronym	Definition
BCP	Business Continuity Planning
BLFNR	The Budapest Liszt Ferenc International Airport Budapest
BUW	University of Wuppertal
BZN	Bay Zoltan nonprofit Ltd. For Applied Research Hungary
CAISO	the California Independent System Operator
CCC	Cork City Council
CCP	Central Counterparties
CHP	Combined Heat and Power generation
CoL	City of London
CoU	Community of Users of Safe, Secure and Resilient Societies
DSB	Norwegian Directorate for Civil Protection
EU	European Union
EUCP	EU Civil Protection team
FCA	Financial Conduct Authority
HNP	Hungarian National Police
IBCDRP	Integrated Business Continuity and Disaster Recovery Planning
IVL	IVL Swedish Environmental Research Institute
KBI	Key Business Indicators
KPI	Key Performance Indicator
MSB	Swedish Civil Contingencies Agency
MUW	Medical University of Vienna
NESA	Finnish National Emergency Supply Agency
NESO	Finnish National Emergency Supply Organization
NIS	NIS j.s.c. Novi Sad (Petroleum Industry of Serbia)
RI	Resilience Indicator
SCI	Smart Critical Infrastructure
SINTEF	Stiftelsen SINTEF
SLV	Swedish National Food Agency
SRH	Heidelberg University of Applied Sciences
SWH	Stadswerke Heidelberg
SWWA	Swedish Water and Wastewater Association
UK	United Kingdom

Acronym	Definition
USTUTT	University of Stuttgart
VAKA	Swedish National Water Disaster Group
WP	Work Package

1 Introduction

1.1 Background

Modern critical infrastructures are becoming increasingly smarter. 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 and respond/recover?

Box 1. ***Current and foreseen challenges:***
It is salient also to include foreseen challenges as the project deliverables needs to account for them in order to be useful also in the future.

These are the main questions tackled by the 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 RIs, including those from Big Data
- Developing a new advanced resilience assessment methodology based on smart RIs and a resilience indicators cube, including a resilience matrix
- Developing an interactive SCI Dashboard tool and a practical guideline for resilience assessment based on developed methodology
- Applying the methodology and tools in eight case studies (ALPHA-HOTEL), integrated under one virtual, smart-city-like, European case study

The SmartResilience project is structured around seven work packages (WP). The first WP focuses on establishing the project baseline and a common framework while WP2 further analyses the challenges and interdependencies of Smart City Infrastructures. In WP 3, the SmartResilience indicators based methodology and an integrated tool (SCI Dashboard) for assessing, predicting and monitoring resilience of SCIs are developed. WP 4 is devoted to identifying and defining the "classic" existing RIs and deriving "new" smart RIs. In WP5, the SmartResilience indicators-based resilience assessment methodology and its RIs are applied and validated against the project case studies (ALPHA-HOTEL), including a combined cascading and ripple effect scenario (INDIA). Dissemination and exploitation, in order to increase impact of project results, is covered in WP6. WP7 (Project management and Coordination) supports all other work by coordinating and monitoring project progress.

With the new indicator-based methodology and its tools, the project seeks to enable and support end users (authorities, operators and owners of critical infrastructure) to better assess the resilience of their respective critical infrastructures and, as a result, significantly improve the resilience of the same. To ensure that the resilience assessment methodology and (smart) RIs will be usable and attractive to the end users, the SmartResilience project involves its end users throughout the project.

1.2 About Task 1.3 and relationship to other tasks and WPs in SmartResilience

SmartResilience is highly integrated in its project design, where individual tasks feed into others. Task 1.3 is part of WP1 (Establishing the project baseline and a common framework) and aims to, already at an early stage in the project, increase the understanding of end users' current and foreseen challenges, needs and requirements in assessing resilience of critical infrastructures and using RIs in doing so. It is salient also to

include foreseen challenges as the project deliverables needs to account for them in order to be useful also in the future.

It is important to establish this baseline in order to ground the development of the resilience assessment methodology and smart RIs on the end users' perspectives to ensure that they will be useful. While this report will argue for the need to contextualize the SCIs, and each case study will illustrate case-specific details that are important when formulating indicators and adapting methodologies developed in the project, the report also contains a concluding discussion in which a generic summary of challenges, needs and requirements are synthesized as generic lessons learned to be addressed in that process.

The identification of end users' challenges, needs and requirements in assessing resilience within Task 1.3 has been guided by an actor analysis approach and is predominantly based on qualitative methods, consisting of semi-structured individual or group interviews with key end users connected to critical infrastructures, as well as desktop studies and literature reviews. These qualitative methods were complemented with a brief online survey.

The task has covered the key end users of the eight critical infrastructures within the SmartResilience case studies (ALPHA-HOTEL) as well as an additional case study covering specifically interconnected critical infrastructures (DSB). Furthermore, in order to take into account end users beyond these nine case studies, a literature review of research to date related to end user's challenges, needs and requirements has been carried out as well as a survey among the Members of the Community of Users of Safe, Secure and Resilient Societies (CoU). All together the methodologies bring complementary perspectives on how the project can take end users into account in order to increase the chances that assessment methodology and RIs are made useful.

This report presents the main results from the literature review, the survey to the CoU and the case study interviews and desktop studies, and puts forward overall conclusions together with an outlook of the conclusions impact on the SmartResilience project ahead.

Task 1.3 has taken its point of departure in the SmartResilience initial framework for resilience assessment derived in Task 1.1, where common definitions and concepts of resilience were reviewed and an initial SmartResilience framework agreed on. Task 1.3 also discusses its results with respect to usability and limitations of resilience assessment put forward based on the analysis of existing approaches, indicators and data sources carried out in Task 1.2. The results from this study will in turn inform WP3 in the development of an indicator-based resilience assessment methodology (including practical guidelines and SCI Dashboard tool) as well as WP4 in the development of smart RIs. Furthermore, the case studies provide a developed baseline for the continued work with the eight case studies (ALPHA-HOTEL) in WP2 and WP5, including an increased understanding of the key end users connected to each SCI. The latter information is also helpful in order to further develop the projects dissemination strategies in WP6. As the SmartResilience project evolve, end users challenges, needs and requirements will be updated throughout, primarily in WP5.

1.3 *Introduction of terminology*

Many different terms are used in this report. This section outlines the most important terms used in this report and their definition in order to increase the readability of the report.

As a point of departure, Task 1.3 has used the initial **resilience** definition of the SmartResilience project, as revised in Task 1.1 and put forward in Deliverable 1.1 "Initial Framework for Resilience Assessment" [79]. According to this definition, "*resilience of critical infrastructures is the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond and respond/recover rapidly from disruption*" [79][1]. Resilience management goes beyond risk management to address the complexities of large integrated systems and the uncertainty of future threats, building on risk analysis and risk management as important input [79].

[1] Note that this definition has been revised further after work in Task 1.2, however, this latest updated definition was not yet available during the main work in task 1.3. The new revised definition of resilience in the SmartResilience project is: "*Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, respond/recover optimally from disruptions caused by them and adapt to the changing conditions"* [37]. The new definition was accepted by all project partners.

The understanding of resilience within SmartResilience is also supported by visualization of a V-or U-curve in a time versus system functionality axis (see Figure 1). The time axis shows the different phases of the resilience cycle. The figure shows that SCIs increase the system functionality, from conventional to smart functionality. However, smart technology may also increase the vulnerability of the infrastructure system. SmartResilience does not focus on the curve itself (the steepness of the absorption curve or the slope of the respond/respond/recovery curve) as a measure of resilience. Instead, resilience is measured using RIs.

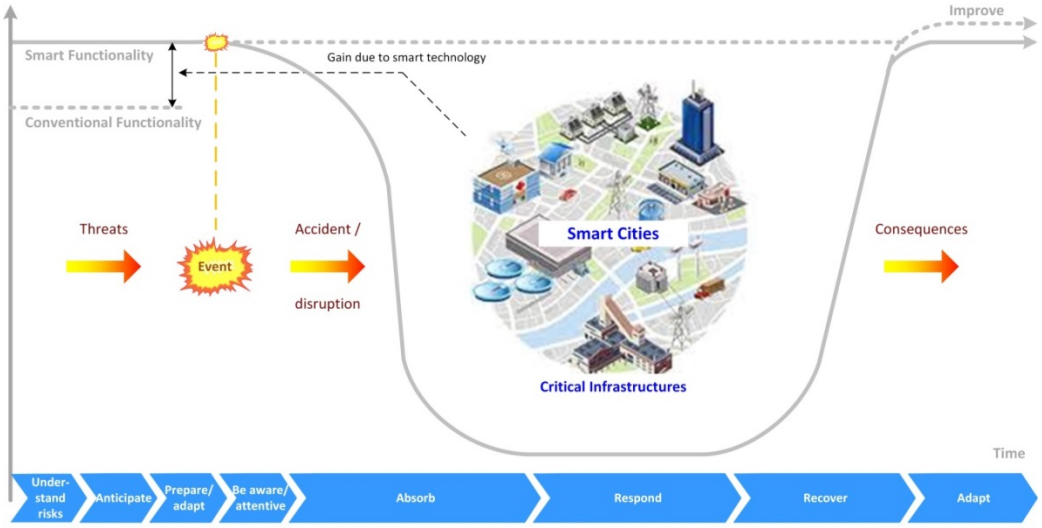

Figure 1: Example of U-curve: System functionality curve for smart critical infrastructure [79].

As many end users do not use the term resilience in their work, related concepts and terms such as **risk management**, **business continuity**, **vulnerability assessments** etc. are used in the empirical chapters of this report. The definition and meanings of these related concepts and terms depends on the end user using them.

The report distinguishes between **current** and **foreseen** challenges, needs and requirements for assessing resilience. This distinction promotes capturing both short-term and long-term resilience perspectives. Many organizations have identified new threats in the horizon that may not be satisfactory addressed today. If the SmartResilience project would not take into account both current and foreseen challenges, it would constitute a risk that the tools developed in the project will be short-lived.

In this report both the terms end users and stakeholders are used. They can refer to the same organizations but the use of them varies depending on the perspective. The definition of **end user** in this report refers to the variety of organizations that the project targets to use the (smart) RIs and indicator-based assessment methodology developed by the SmartResilience project. **Stakeholder** is any organization that has a stake, or interest, in the SCI in focus, either because they are affected by the SCI or because they affect it. End users are most likely found among stakeholders, but not all stakeholders will be end users.

1.4 *Outline of report and responsibilities*

This report is the main deliverable which puts forward the results from Task 1.3 on end user's challenges, needs and requirements in assessing resilience. In the next chapter (2) of the report, the process and methodology of data collection and analysis for the nine case studies, the literature review and survey is described. This is followed by the summary of the literature review in chapter 3, which describes existing studies and projects of particular relevance for this task and relates them to the work that has been carried out here. In chapter 4, the results from each case study, based on interviews with end users and desktop studies, is presented. Chapter 5 brings together the main findings from all empirical data in an overall analysis of end users' main challenges, needs and requirement in assessing resilience and using RIs. Finally, chapter 6 draws conclusions, relates the results to other tasks of the SmartResilience project and presents a number of implications from these results for further development of the indicator-based assessment methodology and smart RIs within SmartResilience.

IVL has been the task leader with overall responsibility of the task and is the main author of the report, with the responsibilities of carrying out the literature review, the survey to CoU and putting forward the analysis

and conclusions. However, several project partners have been involved in carrying out the nine different case studies and making valuable contributions to the report. Main authors and contributing partners regarding the case studies are presented in Table 1.

Table 1: Responsible partners related to the study on end users' challenges, needs and requirements in the different case studies

Short name	Main focus	City/Country	Responsible partner	Assisting partner
ALPHA	Finances	London/UK	IVL	CoL
BRAVO	Smart city	Heidelberg/Germany	UTSTUTT	SRH/EU-Vri/SWH/BUW
CHARLIE	Health care	Vienna/Austria	MUW	
DELTA	Transport	Budapest/Hungary	HNP/BZN	HNP/BZN
ECHO	Supply	Pančevo/Serbia	NIS	
FOXTROT	Water	Stockholm/Sweden	IVL	
GOLF	Government (flood)	Cork/Ireland	HNP/BZN	CCC
HOTEL	Energy	Helsinki/Finland	IVL	
DSB	Interconnected SCI	Oslo/Norway	SINTEF	

2 Methodology

2.1 Interviews with end users and desktop studies

2.1.1 Selection of end users for interviews

The selection of respondents for interviews within each of the nine case studies was carried out with help of a two-step actor analysis approach. In the first step of the actor analysis, key stakeholders with regard to resilience work and assessment were identified in connection to the critical infrastructure of each case study by the responsible project partner(s) (See Table 1 above). Key stakeholders identified included both end users (private and public) that are already project partners of SmartResilience (e.g. City of London (CoL), Cork City Council (CCC), Stadtswerke Heidelberg (SWH), Hungarian National Police (HNP)) but also end users that are vital for respective critical infrastructure beyond project partners.

Each identified key stakeholder was then described in terms of their role or responsibility in relation to the critical infrastructure and resilience (or related concepts). The level (national, regional, local, other) and type (public, private, civil society, other) was also outlined for each stakeholder. Between 1 to 10 key stakeholders were identified per case study, including owners and operators of the critical infrastructure, regulators of the critical infrastructure and governmental representative with responsibility for the country's overall emergency management, disaster reduction or resilience. In Annex 1, the actor analysis template is provided and the actor analysis for each case study is presented in their respective chapter.

Based on the analysis of key stakeholders and their roles/responsibilities, a selection of the most relevant organizations to study more in-depth was made, together with an identification of relevant individuals to interview within the organization. The selection of organizations and individuals within those organizations was carried out in dialogue with the end users themselves.

2.1.2 Individual or group interviews

While the first step of the actor analysis aimed to identify the key stakeholders and their characteristics, the second step of the actor analysis aimed to understand their challenges, needs and requirements for assessing resilience through semi-structured interviews and desktop studies. The interviews took place either individually with each respondent or as group interview with several respondents being present at once. Depending on the availability and geographical distance between key individuals in each case study, the interviews were carried out either over telephone or face-to-face. Desktop studies based on literature, publicly available reports, and websites regarding key stakeholders and respective critical infrastructure were furthermore reviewed as a complement to the interviews.

In total, interviews with 48 end users connected to the nine case studies took place August –September 2016. Annex 2 provides a summary of all interviewed end users and information on the mode and type of interview. The number of respondents differs between the case studies due to number of identified key stakeholders in the critical infrastructure and access to and availability of respondents. The length of interviews varied depending on end user and type of interview (individual or group), but was estimated to 1 hour for individual interviews and 1-3 hours for group interviews.

To enable comparability of the results as well as to simplify the reporting of the findings by different interviewers, common guidelines and an interview protocol were developed and used for the interviews (see Annex 3 Interview Protocol and Annex 4 Interview Guideline). The questions in the interview protocol focused on four main areas: current work with resilience, work with resilience in other organizations, current work with assessing resilience including use of indicators, and current and foreseen challenges, needs and requirements. The questions within these areas took its point of departure from the revised definition of

resilience put forward in Task 1.1 (see chapter 1) and its different phases (understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond/respond/recover rapidly from disruption). Since resilience is not a ubiquitous term, this raised a reminder throughout the interview what the project means by resilience. The interview protocol was adapted to the context of the specific SCI and, when necessary, translated into the domestic language of the respondents by the responsible project partner(s).

All respondents were asked to sign an Informed Consent and Information Sheet (see Annex 5) before the interview, in order to obtain the respondents informed consent to participate in this particular study within SmartResilience and inform them about what their participation entailed. The informed consent form includes information about the aim of the study and issues of confidentiality. It was made clear that any information provided could be published in a public report, which is why no sensitive, confidential or classified information resulting from interviews could be included in report. Moreover, the Informed Consent agreement includes a possibility for each interviewee to modify/withdraw participation or sharing of data at any time during the process. In one of the case studies, one interviewee withdraw but we compensated for the missing information with publicly available material such as websites and reports.

2.1.3 Analysis of results and validation

The interviews, based on the interview protocol and guidelines, have been performed in English or the respective domestic language of preference to each end user. The interviewer(s) were project partners with appointed responsibilities for the cases included in this report. In order not to lose important information during the semi-structured interviews, the interviews were recorded and/or detailed minutes were taken. The results from the interviews for each case study were then summarized together with the information from the desktop study, and the results were presented per case study (in English

The task leader (IVL) put together a table of preliminary observations from each case study, which was then discussed at a Telecon and through e-mail dialogue between the involved project partners. The results from the case studies were furthermore presented during a Task 1.3 Consolidation Validation workshop in Trondheim on October 12, 2016, where project partners discussed the preliminary results and their implications for the project. These discussions have been taken into consideration in the analysis and conclusions of this report.

The case study reports are presented in chapter 4. For each report the data was summarized in two tables. First, the case studies summarized the current vs foreseen challenges and the current vs foreseen needs and requirements for the critical infrastructure.

Table 2. . Currrent vs foreseen challenges and current vs foreseen needs and requirements for the critical infrastructure.

Current challenges	Foreseen challenges
Current needs and requirements	Foreseen needs and requirements

Secondly, the data was summarized according to the five dimensions, as a means to specify what is needed for the development of the Smart Resilience methodology and data base for the specific case study.

Table 3. Summarizing challenges, needs and requirements according to the five dimensions of resilience.

Dimensions of resilience
System/physical: Technical aspects, physical/technical networks, interconnectedness
Information/data: Technical systems dealing with information/data
Organizational/business: Business-related, financial and HR aspects and organizational networks
Societal/political: The broader societal/social context, indirect stakeholders
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)

In chapter 6, these various findings are summarized and abstracted as an input for further work with the methodology and data base. Compare to figures 2 and 5 in D1.2 (section 2.2.3), where the dimensions are juxtaposed to the different phases of the resilience curve, constituting a matrix.

2.2 Literature Review

A literature review/desktop study on previously collected end user needs and requirements not linked to particular case studies was made. The literature review was conducted through collecting materials from related EU projects around protection of critical infrastructures and the like, with a focus on those projects that engaged end users in order to create tools, models, guidelines and the like that those end users would benefit from (see Annex 6). Moreover, guidelines and framework material from governmental agencies were analyzed. A literature survey on research articles was made through Scopus, using search criteria that combined terms such as “critical infrastructures”, “indicators”, “experience”, “stakeholder engagement”. More than 300 articles that addressed indicator development were found, but only around 20 of those concerned end user engagement in indicator development. Most of them concerned indicator development for research or policy use. Of those, only a very small number concerned indicator development for end users’ own use.

2.3 Survey to Community of Users

The survey aimed to increase the project’s understanding of how potential end users, i.e. a broad group of stakeholders not involved in the project, assess the usefulness of current assessments of resilience and what can be done to improve these.

The survey was conducted among the Members of the Community of Users of Safe, Secure and Resilient Societies (CoU)[2]. The survey, which entailed four questions, was conducted during the period September 26 – October 7, 2016, as a mean to assess the respondents’ valuation of the current resilience assessments in relation to other related approaches (e.g. risk assessment and business continuity) and their view on resilience assessment improvement. See Annex 6 for the full survey.

All in all only 12 out of 1,050 members responded to the survey, which is why the survey results should not be considered as representative for all members of the CoU but rather as examples of views of some members with experience of working with resilience. A majority of the respondents (10 out of 12 respondents) have professional experience, substantial or limited, of working with resilience. Members with little or no experience of working with resilience possibly considered the survey too advanced. It is also possible that an extended survey period would have enabled more members of the CoU to answer the survey. SmartResilience will consider the possibility to carry out a survey to the CoU again later in the project.

[2] EC is supporting the development of a “Community of Users of Safe, Secure and Resilient Societies” to facilitate information exchanges among and between policy-makers, research, industry, practitioners, and the general public. CoU should inter alia ensure that research programming takes practitioners needs into account.

3 Literature review: Existing knowledge on end users' needs and requirements for assessing resilience

3.1 Introduction

"*One of the most important goals of developing tools for measuring vulnerability is to help bridge the gaps between the theoretical concepts of vulnerability and day-to-day decision making*"([12], p. 30).

Most assessments of resilience are not intended to serve stakeholders' practical work with understanding and managing risks or disturbances. Either they are designed for research use [3] or for policy use [7], but not for end users' direct use. Thus, it is not possible to tell how well these assessments correspond to the organizations' resources, skills, assignments and current processes. On the other hand, publications by governments, offering guidance to various local governments or companies (see e.g. [8]), or publications offering guidance to resilience in certain domains, most often do not specify the means or models to be used. This is because the regulatory approach: the regulator specifies the goals to be reached by the regulated organizations but leave to them how to achieve them.

To be useful to end users in day-to-day decision-making, indicators need further contextualization [12]. This literature review covers a number of studies that are particularly relevant to consider when focusing on the usefulness of assessments and indicators for resilience in critical infrastructures. It consists of three main parts. Firstly, the fundamental question why one seeks to assess resilience is reviewed: what should the assessments and indicators be useful for? Secondly, studies that have focused on how to design useful indicators and methods for doing so are presented. Thirdly, the specific challenges raised when assessing resilience in interconnected infrastructures are highlighted.

3.2 Contextualizing for what purpose?

Prior and Hagmann [61] suggest five different reasons to measure resilience in terms of security of critical infrastructures:

- Characterize or model resilience
- Raise awareness or share information about critical risks
- Allocate resources among various competing areas or issues
- Build resilience
- Monitor policy performance

They review three different resilience models and suggest a number of overall considerations. For example, if an indicator is aimed at reducing complexity in assessing the resilience of a complex system: "*how can you simplify a complex process or concept so that it is understandable and measurable without losing the very complexity and deepness of meaning you are trying to capture*?" ([61], p. 293).

3.3 Contextualizing indicators to end users

Birkmann [12] investigated the usefulness of three different indicator models for natural hazards. Usefulness here refers to both reliability (whether the models accurately represent actual vulnerability and resilience) and guidance to decision-making. He stresses the need to contextualize indicators to local contexts, uses and users. First, there is a need to operationalize and translate vulnerabilities into quantitative and qualitative measures. Secondly, there is a need to design and adjust the indicators for specific functions (e.g. risk identification or evaluation or risk management performance) and for specific user groups (e.g. disaster manager or urban planners).

Moreover, most indicators are designed in relative terms, allowing a comparison of places, entities or over time. This is useful as long as indicators will be used for a relational understanding of resilience, for example as a tool to allocate development funding. However, "*it will not tell you if the river-side community you are concerned about can be resilient to a major flooding event, only whether it will be better off than the neighboring community*" ([61], p. 294).

Further, Prior and Hagmann [61] warn against the unreflective use of proxies as a means to assess resilience, such that using only easily available data. An example of that is the use of redundant resources (e.g. various back-ups) as a proxy for respond/respond/recovery potential. Redundant resources are not by themselves providing respond/recovery – they need to be properly deployed when needed. Moreover, the lack of redundant resources does not preclude response/respond/recovery: there might be other means to that end. Finally, Prior and Hagmann urge analysts and policy-makers to consider carefully on the ways in which the choice of measures themselves affects the way in which resilience is being understood. One could add: and on the way this choice affects how resilience could be improved.

Lee et al. [41] argued that there is a need to demonstrate the "business case" for assessment of organizational resilience through its ability to quantify improvements in their resilience and tracking changes in that measurement over time. To that end they argue, there is a need for leading indicators that proactively assess resilience towards future challenges, rather than simply relying on lagging indicators, that is relying on data from past performance.

In a study designed to develop leading indicators for safety performance for helicopter offshore operations, Herrera et al. [32] tested an initial set of indicators through workshops, interviews with operational staff and observations of simulated helicopter landings. Based on the literature review, they argued that indicators should be designed according to the following criteria:

- Meaningful: values should correlate to accident frequency or consequence.
- Available and affordable
- Reliable beyond subjective assessment
- Operational: be able to be used in operational context
- Ownership: the indicators should be "owned" by the personnel which performance is measured

The suggested indicators were analyzed using a model (Functional Resonance Analysis Model) which allowed the researchers to consider the influence of context on actual performance, as well as allowing learning from not only failures but also from normal operations. This approach also helped to identify indicators beyond check-lists or those already easy to collect.

3.4 Contextualizing indicator development through end user participation

In a few cases, RIs are designed in cooperation with affected stakeholders. Only sometimes though, are the indicators designed to be used for specific users in mind that is contextualized.

There is quite a few other EU funded projects in the area of protection of critical infrastructures that involve end user participation as a means to assess needs, requirements and the value of developed measures to assess and manage vulnerabilities (see Annex 6). Often the methods used to engage end users and their specific contribution is unclear (e.g. IMPROVER, DRIVER, CRISMA). In a few cases though, there are preliminary findings that show how practitioners struggle with resilience concepts compared to concepts of business continuity and risk management (e.g. RESILENS). The requirements for specific tools to be used for resilience management guidelines were constructed in cooperation with end users in the SMR project. The PREDICT and RESILENS projects have a similar approach as SmartResilience.

In an EU research project within the Critical Infrastructures Programme, Hernantes et al. [31], based upon a literature review, designed a framework with four dimensions of resilience: technical, organizational, economic and social resilience. Domain experts within different fields (energy companies, first responders, civil protection, healthcare and organizations responsible for critical infrastructures) joined for three workshops to define relevant policies that affect resilience and how they related to each other, based upon various scenarios for power outage. Between the workshops, simulation and Delphi calculations were used to judge the various impacts of these policies. The resulting framework was subsequently used by experts to assess the resilience levels and opportunities to enhance resilience of a nuclear power plant and a water distribution company, through documents, interviews and observations. Hernantes et al. argues that the

collaborative modeling with recurring workshops provides two advantages: shared learning across experts from interdependent critical infrastructures and learning over time, from crisis to crisis. Although a very productive project, there are two important limitations from this project: a) the model has not been subject to empirical testing as a means for end users' work with assessing resilience b) there still remains work to define the quantitative metrics.

In another project, Sudmeier et al. [69] assessed resilience to earthquakes in Nepal as a means to provide stakeholders with a tool to identify and rate underlying causes to vulnerability and preparedness. They employed participatory qualitative methods, typically used in vulnerability and capacity analysis, such as semi-structured interviews with key informants, transect walks, participatory risk and social resource mapping to understand relations between different groups, coping strategies, to identify stakeholders, vulnerable households and dangerous areas. Fifty different indicators, grouped into five categories were developed. Through household survey questionnaires they obtained indicator values which were used to compare the resilience of six communities. The indicators focus mainly on outcome values though and there is a need to further validate process variables that could be used for preparedness planning.

3.5 *Contextualizing indicators through integrating with existing organizational processes*

Reflecting common principles for emergency management, the Swedish Civil Contingencies Agency (MSB) stresses that the same organizations that are responsible for a critical infrastructure in normal operations are also responsible to manage the infrastructure in crisis situations and that crisis preparedness and management needs to be integrated in existing management processes. It is rare that research addresses how this could be done though. In a recent review of more than 30 different frameworks to assess the protection of critical infrastructures, Bialas [11] argue that none of them were based a continuous improvement model such as the Deming Cycle (PDCA).

However, there is one study of the usefulness of indicators designed by the end user for their own purposes. Roe and Schulman [62], have for many years conducted ethnographic fieldwork at the California Independent System Operator (CAISO), an organization that manages California's high-voltage transmission grid in real-time. Their research has enabled them to understand resilience as an organizational process in response to smaller scale shocks. It is the successful management of these shocks, they argue, that prevents many larger crises from happening through learning processes, either directly when control room operators correct and adjust operations in real-time as needed to keep, or indirectly when managers identify conditions that could disorient or even degrade the skills of control operators of the infrastructures.

Resilience, they argue, is a variable that extends across multiple stages of an infrastructure's cycle of operations. Control rooms "*can signal their readiness for future resilience through measurable responses as they seek to prevent accidents to happen and back away from conditions that are precursors to full-blown system failures*" (p. 116). In the article they analyze an example of the responses in one output error as due to three different disturbances, that is in terms of the variation in one of CAISOs principal reliability standards. When calculating this indicator over time, they found that the movement towards and back from the defined limit was larger directly after disturbances but reduced over time. Observations and interviews revealed that this initial variation was a deliberate effort to learn and to improve performance over time.

3.6 *Contextualizing indicators to interconnected infrastructures*

There is an emerging discussion over an assumed incompatibility of current organizational set-ups and the potential effects of cascading failures across critical infrastructures [25]. Challenges include:

- Coordination issues: there is an increasing number of organizations, across the private and public sectors, which address critical infrastructure protection.
- Reliability across networked infrastructures: research around highly reliable organizations stress the need for trust, informal relations and a shared commitment, dimensions that become problematic with increasing market-based coordination
- Ways in which the government can provide incentives for stakeholders to address issues beyond their own organization.

- Accountability and management by objectives. This concern how can measure and value the absence of a loss.

Theoretically, there is a large number of potential connections that may cause cascading effects in numerous directions, an issue that has retrieved a lot of research attention [25]. However, Roe and Schulman [62] argue that the key to preventing cascading effects lies in either communication across critical infrastructures in precursor conditions or in the effective management of each sector. In fact, Van Eeten et al. [78] show that cascading failures are anything but "unmanaged". Using a dataset of media reports on failures in critical infrastructures, they report a pattern where the energy and telecom sectors are the main event-initiating sectors and where none of the other sectors cause disruptions in the energy or telecom sectors. At the same time, such cascading effects are both more common and more banal than the literature suggests, contrasting the usual image of low probability-high consequence events. They argue that this suggests that, rather than a vast web of interdependencies with catastrophic potential, there are a few well-known pathways that have provided opportunities to learn and to design mitigating or decoupling moments. Thus, any cascading effects due to failing electricity and telecom supply are expected, not a sign of failing risk management. This is why most other critical infrastructures have redundant capacity or continuity plans that address such events.

3.7 Summary and conclusions

This literature review has showed how indicators can be contextualized in order to fit the end users and increase usability (see table 4 below).

Table 4. Summarizing the literature review of contextualizing indicator development as a means to making them useful for end-users

Contextualizing in five dimensions	
Purpose of use	• Characterize or model resilience • Raise awareness or share information about critical risks • Allocate resources among various competing areas or issues • Build resilience • Monitor policy performance
To end-users needs	Need to demonstrate the "business case" for assessment of organizational resilience (leading indicators needed): • Meaningful: values should correlate to accident frequency or consequence. • Available and affordable • Reliable beyond subjective assessment • Operational: be able to be used in operational context • Ownership: the indicators should be "owned" by the personnel which performance is measured Need to design and adjust the indicators for: • Specific functions (e.g. risk identification or evaluation or risk management performance) • For specific user groups (e.g. disaster manager or urban planners).
Indicator development in dialogue with end-users	Collaborative modeling with recurring workshops provides two advantages: • Shared learning across experts from interdependent critical infrastructures • Learning over time, from crisis to crisis
Through integrating with existing organizational processes	Resilience as an organizational process in response to smaller scale shocks Resilience defined as a variable that extends across multiple stages of an infrastructure's cycle of operations

To interconnected infrastructures	Coordination issues Reliability across networked infrastructures Incentives for stakeholders to address issues beyond their own organization. Accountability and management by objectives

Three important conclusions can be drawn.

- Designing useful indicators requires definition of the "work" that the indicators are supposed to do, or support.
- Involving end users extensively in the process of designing indicators, in an iterative manner, allows for integrating them into existing organizational processes.
- In interconnected infrastructures, there is a need identify how to support coordination, information sharing and constructing incentives, but also to identify the most pressing problems to address, for example through a risk-based approach.

4 Case studies: End users' challenges, needs and requirements for assessing resilience

4.1 ALPHA: The City of London – a critical financial hot-spot of the world

4.1.1 Introduction

London has been the financial hub of the United Kingdom (UK) and a major trade and business center since the Middle Ages [43]. Today the city competes with New York City for the status of the world's major financial center.

Much of London's finance industry is located at the "Square Mile" or the "City," the long standing business hub of London. The other major financial district is the Canary Wharf area, about four kilometers east of the City. It is estimated that the financial services sector employs about 315,200 people within the City. Apart from traditional banking activities and insurance, London also thrives as a center for foreign exchange and bond trading. The foreign exchange market has a daily global turnover of about 2.5 trillion GBP. London accounts for about 0.73 trillion or 36.5 percent of the pie. The Bank for International Settlements estimates that London generates 0.88 trillion or 46 percent of daily global revenue in the interest-rate derivative market.

Figure 2: London "City"

London has always been the seat of many multinational financial organizations. The Bank of England is the UK's central bank. Established in 1694, this is the second oldest central bank in the world and the model on which central banks of other countries base themselves on. Other than banks and insurance entities, the Bank of England oversees also financial market infrastructures (FMIs) that play a key role in the smooth functioning of the economy and can enhance the stability of markets and promote wider financial stability [9]. There are three main types of FMIs overseen by the Bank of England: a) recognized payment systems, b) securities settlement systems and c) central counterparties (CCP). Market functioning relies on ensuring the continuity of the services that these infrastructures provide. Payment systems enable the lending and repayment of money, allow businesses to receive payments for goods and services, and facilitate the

payment of salaries and benefits to the general public. Securities settlement systems enable the purchase and sale of equities and bonds. Central counterparties offer their guarantee to their participants that transactions in a range of financial and commodity markets will be honored even if the original counterparty defaults. In its supervision of financial market infrastructure the Bank of England will work closely with the HM Treasury and the Financial Conduct Authority (FCA) reflecting the FCA's responsibilities for the trading infrastructure and market conduct. See also Table 5.

Lloyd's (also known as Lloyd's of London) begun in 1688 and is the largest specialist insurance and reinsurance market in the world with premium of approximately £43.5 billion per annum. The Corporation of Lloyd's is the body that oversees the market to ensure it operates in a way that does not jeopardize the brand or impact the licenses held in over 200 territories globally. The aim of the market is to enable companies and people to offset risk through an insurance policy and covers marine, aviation, catastrophe and other forms of underwriting. Worldpay is a fintech (that is, financial technology) company and a global leader in payments processing technology and solutions for merchant customers. This section builds on interviews with representatives from Worldpay and Lloyds (two persons). The data from Bank of England is provided by publicly available data.

Table 5: Actor analysis ALPHA

Name of organization (original language)	Level	Type	Role/responsibility in case study
Bank of England	National	Public	Regulator
Worldpay	Multinational	Private	Payment provider
Lloyds	Multinational	Private	Reinsurance company
HM Treasury	National	Public	Regulator
Financial Conduct Authority	National	Public	Regulator
City of London Corporation	Local	Public	Infrastructure provider

4.1.2 Current status working with resilience and assessing resilience

The Bank of England oversees and support financial stability [9]. Market functioning, and therefore financial stability, can be dependent on the continuity and orderly operation of services provided by FMIs. Monitoring, managing and mitigating risk, including risks to the financial system at large, is a primary responsibility for the operators of financial market infrastructure. Supervision of banks, insurance companies and FMIs is therefore closely linked to preserving financial stability. Consistent with that, the Bank of England will undertake its supervision of the operators with a view to protecting and enhancing the stability of the financial system. In the event of major operational disruption to the financial system, the three authorities' (The Bank of England, HM Treasury and the FCA) main objectives are:

- To keep retail and wholesale markets open and functioning. Specifically, aiming to keep payment and settlement systems open to complete today's business, and 'getting money and securities in the right hands'.
- In the event that markets do not remain open, to ensure an orderly and early return to trading, e.g. by providing an information clearing house, effective channels of communication, and formulating an effective and coordinated response.
- To involve relevant infrastructure providers and market participants, when making decisions affecting markets. To be ready to facilitate market initiatives.

The Bank of England performs regular exercises to assess resilience of the industry. Among these, there is the overall resilience benchmarking [73] and cyber and technology benchmarking [74]. In 2005 the UK Financial Authorities launched an ambitious Resilience Benchmarking project to assess how the financial sector would

cope in the event of major operational disruption and how quickly it would be able to respond/respond/recover afterwards. The project was constructed to answer the following questions [73]:

- How resilient is the UK financial sector?
- How quickly can the sector respond/recover from major operational disruption?
- Do firms plan and prepare effectively?
- Are there any concentrations or dependencies that could be potential areas of vulnerability?
- What action is needed to improve the resilience and respond/recovery capability of the sector?

In 2012 the financial authorities surveyed financial firms' technology and cyber resilience to address the following objectives [74]:

- Capture and share technology and cyber resilience practice across the sector with the aim of strengthening its resilience;
- Increase understanding of the sector's capabilities in relation to technology and cyber resilience;
- Assess the technology and cyber resilience practices of selected organizations and highlight inconsistencies which they should review; and
- Identify technology and cyber resilience topics for inclusion in future sector exercises.

The interviewee from Worldpay leads a team that addresses business continuity and respond/recovery and corporate security across the whole organization. The interviewee is familiar with resilience concepts and parts of the role are to insure governance to comply with various standards in the area: ISO22301 – Business Continuity Management; ISO27031 - Guidelines for information and communication technology readiness for business continuity; and ISO27001 – Information security management. These standards, the interviewee stressed, are much more stringent than governmental regulation. The organization is audited against these standards by an internal auditor, independent from the team, on a continual basis and every year there is external audit by the British Standards Institute.

The team monitors all external threats on a daily basis through mass media and other channels. The team maps new triggers that may cause disruptions but also closes down irrelevant ones in collaboration with various internal departments, e.g. the legal department, "*to get their view as well to get sure we got the right triggers, what actions we need to take*". They also coordinate the mapping of triggers with key partners and suppliers as well as industry forums. Moreover, Worldpay participate in the finance industry exercises organized by the regulatory organizations. The interviewee stressed that all the major companies in the financial industry "*do exactly what we do*": participate in the same forums, share the same information. He also stated that the other companies and regulatory agencies have a similar approach, even if the models and their degree of "maturity" might differ somewhat.

There are four kinds of risks that the team monitors on a daily basis through mass media and through specifically assigned processes. First, that their employees cannot access the premises due to various disruptions such as terrorist attacks, environmental impact such as fire, flood or utility failure (electricity, water, telecom etc). Second, telecom disturbances also impact on customers' access to services. Third, there might be intrusions into Worldpay's network. The company repeatedly tests its defenses against such intrusions. Forth, pandemics might influence the workforce or the infrastructure such that employees cannot reach their offices. New technology and new processes are tested internally and with select customers in pilot phases, in a controlled manner, before released "out in the wild".

The major tool for Worldpay's work with resilience seems to be "The Scenario Playbook". The playbook is the basis for the local departments resilience planning and for their response to various disruptions. The playbook is continually updated when the team learns from experience and after testing new potential triggers such as new software. It is based upon identified triggers such as if key suppliers would go into administration (taken over by government) or liquidation, or in case of denial of access to premises etc. Testing items include people's abilities to perform their tasks, alternative sites, the ability to work from home etc. Testing criteria includes respond/recovery time and up and running times as well as appropriateness: does the function test do what it should test? Changes in the playbook or weaknesses identified from events or from testing is the basis for mitigating action, usually in terms of a project to change processes, technology etc. The major means for resilience seems to be to have back-ups in terms of communication channels, power supply, servers etc.

The team also works with the local departments as a means to learn about vulnerabilities and capabilities. Local departments carry out exercises, in collaboration with the resilience team, as a means to check their preparedness. The local departments have people assigned to address resilience who report back to the team and who participate in an annual conference on security and safety. Smaller incidents happen on a daily basis for various reasons, some of an effect of attempted fraud. These are either contained or the local departments are capable to manage them. Thus, there is only a limited learning potential from these smaller incidents. The major learning potential lies in Worldpay's deliberate testing of its own capacity to withstand disruptions and to a lesser extent from a small number of major incidents.

At Lloyd's, everybody is responsible for managing risks, as risk is at the heart of what they are doing: "transferring risks from clients to us". The interviewees from Lloyd's have different responsibilities. One of them is in charge minimizing the impact of operational incidents for the Corporation and market, to ensure they can continue working in case of a disruption and that companies in the market have correct procedures in place of similar quality to the Corporation, i.e. business continuity management. The other heads the internal risk management function at Lloyd's identifying and addressing various risks across the Lloyd's market and Corporation: financial risks, operational risks, regulatory change and issues of legal compliance. Instead of resilience, Lloyd's talk about risk appetite – as this is how insurance companies make money. Moreover, as Lloyds is specialized into reinsurance of high risk operations they accept high levels of risk as a means to high results.

The biggest risks to Lloyd's are financial and in particular that the insurance companies in their market do not sufficiently prepare or capitalize for their exposure to major events such as catastrophes. Lloyds define "a risk appetite" as a clearly defined tolerance level to various events around the world: what is the amount of money they are willing to pay for a defined catastrophe such as a hurricane. They monitor their exposure to various events, run scenarios and manage the market to stay within those thresholds. There are two major means to control those risks. First, they have a financial reserve such as bonds or equity funds to cover losses. Second, they oversee that clients have a conservative approach to managing risks – an effective board structure as well as an effective governance and effective business continuity process.

The Corporation's operational risks stem from anything that would deny access to or the use of its premises such as terrorism, earthquakes, supply of electricity and power. The interviewees are working with various other departments and processes to develop business continuity plans for these: "to try get ahead of the game" – mapping threats out and developing a process to respond/recover etc.

The interviewees argued that all financial institutions deal with risks and that all insurance companies work within a similar regime, including business continuity planning that address respond/recovery and to avoid damaging the UK financial infrastructure. This also includes complying with relevant standards. The regulatory regime, they argued, has become a lot more stringent after the financial crisis in 2008, with tight cooperation between operators and the agency. The interviewees argued that "*we have a much more robust regulatory regime than perhaps other sectors*". Lloyd's have taken part in industry exercises organized by the regulatory agencies, for example around the effects of terrorism or pandemic. They chair the insurance market business continuity forum. Lloyd's also organize internal management exercises with various departments as around various scenarios as well as workshops for companies within the market.

4.1.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: that employees cannot access the premises due to various disruptions such as terrorism, earthquakes, supply of electricity and power, telecom disturbances also impact on customers' access to services; intrusions into corporate networks; financial and in particular that the insurance companies in their market do not sufficiently prepare or capitalize for their exposure to major events such as catastrophes. Worldpay: Challenges to assessment include getting time and window to schedule testing.

4.1.4 Foreseen challenges, needs and requirements for assessing resilience

Worldpay argue that Brexit and increasing reliance upon digital payment are the major challenges for the future. When people stop using cash, there is an increasing expectation of a 24/7 availability of digital payments.

Lloyd's identifies some new emerging risks as those to stemming from technology and climate change. For example, one cyber risk could be that people hack into aircraft controls and cause crashes. Lloyd's argues

that emerging risks pose a challenge to assessing resilience and also if their insured companies go into new markets. In terms of climate risks they use external expertise through sitting on panels and risk management forums, discussing with colleagues, as well as using external specialist modeling companies to constantly update quantitative estimates of probability and impact. For example, they need to reassure that their insured companies think about the risks due to hacking. When asked about the potential use of big data, they argued that social media could be a source. For example the magnitude of a shipwrecked ship can be calculated through collecting data from transponders attached to floating life boats. However, there is a long way from harvesting such data. In table 6 below, the challenges, needs and requirements for the London financial sector are summarized.

Table 6. Challenges, needs and requirements for the ALPHA case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* that employees cannot access the premises due to various disruptions such as terrorism, earthquakes, supply of electricity and power, telecom disturbances also impact on customers' access to services; intrusions into corporate networks; financial and in particular that the insurance companies in their market do not sufficiently prepare or capitalize for their exposure to major events such as catastrophes. 2. Main challenges: Challenges to assessment include getting time and window to schedule testing.	1. Brexit 2. Increasing reliance upon digital payment are the major challenges for the future. When people stop using cash, there is an increasing expectation of a 24/7 availability of digital payments. 3. Lloyd's identifies some new emerging risks as those to stemming from technology and climate change.
Current needs and requirements	**Foreseen needs and requirements**
1. To keep retail and wholesale markets open and functioning. 2. In the event that markets do not remain open, to ensure an orderly and early return to trading 3. To involve relevant infrastructure providers and market participants, when making decisions affecting markets. 4. To be ready to facilitate market initiatives. 5. They need to monitor their exposure to various events, run scenarios and manage the market to stay within those thresholds. 6. In terms of climate risks they need to use external expertise through sitting on panels and risk management forums, discussing with colleagues, as well as using external specialist modeling companies to constantly update quantitative estimates of probability and impact.	1. Capture and share technology and cyber resilience practice across the sector with the aim of strengthening its resilience. 2. Increase understanding of the sector's capabilities in relation to technology and cyber resilience. 3. Assess the technology and cyber resilience practices of selected organizations and highlight inconsistencies which they should review. 4. Identify technology and cyber resilience topics for inclusion in future sector exercises. 5. Need to reassure that their insured companies think about the risks due to hacking. 6. Social media could be a source for collecting needed data, e.g the magnitude of a shipwreck can be calculated through collecting data from transponders attached to floating life boats.

4.1.5 Discussion and conclusion

The data collected (including desktop data) indicates that the finance industry has a shared and quite elaborated perspective on resilience and on means to provide that. Operators and agencies collaborate intensively to share information and to assess common risks and means to address them.

Diverse kinds of threats were mentioned although a lot of them were concerned with shared outcomes that seem to be critical to the industry. For example, terrorism, natural hazards and loss of supply of power or telecom could all interfere with employees' access to or use of their premises. Emerging risks are also shared

such as e.g. those related to cyber technology, although the impact of events might differ – from intrusions to internal networks to those caused to insured assets.

The organizations in case also seem to have elaborated programs for monitoring and evaluating risks, how they should be measured and criteria for their impact as well as how to manage them in order to reach defined targets, such as time to respond/recovery (Worldpay) and accepted losses (Lloyd's). Major tools include standards, a scenario playbook and exercises. The current regulatory regime is not only risk-based but also informed by recent experiences from the last financial crisis in 2008. Resilience as a concept seems to provide added value to understanding sources and means to address various risks. However, resilience concepts are also mixed up with risk management and business continuity concepts.

In terms of challenges to measure resilience, it seems as if the issue of using big data to measure risk or impact is not yet a widely discussed issue. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the ALPHA case can be summarized in table 7 below.

Table 7. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the ALPHA case.

Dimensions of resilience	Examples from ALPHA
System/physical: Technical aspects, physical/technical networks, interconnectedness	Increased dependency on digital payments in the financial industry. Employees cannot access the premises due to various disruptions such as terrorism, earthquakes, supply of electricity and power.
Information/data: Technical systems dealing with information/data	Developing big data is of interest through e.g. the use of social media.
Organizational/business: Business-related, financial and HR aspects and organizational networks	Challenges to assessment include getting time and window to schedule testing.
Societal/political: The broader societal/social context, indirect stakeholders	Brexit. To involve relevant infrastructure providers and market participants, when making decisions affecting markets.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Need to reassure that their insured companies think about the risks due to hacking. Assess the technology and cyber resilience practices of selected organizations and highlight inconsistencies which they should review.

For this case study, the concept of resilience is a useful device, and issues of complexity and sensitive data management are all major issues to be considered.

4.2 BRAVO: The future-oriented and sustainable community of Bahnstadt, Heidelberg

4.2.1 Introduction

Bahnstadt in Heidelberg is one of Germany's largest urban development projects. It is designed to be Heidelberg's first smart neighborhood. Bahnstadt is located in the southwestern part of Heidelberg's city center, and it shares a border with the main station. The energy concept consists of passive house standards as a universal construction method, district heating supply to be covered in the medium term by renewable energies, and intelligent control of power consumption using smart metering. Bahnstadt being the first smart neighborhood is dependent on the critical infrastructure: Stadtwerke Heidelberg (SWH) [28].

Figure 3: City of Bahnstadt

SWH provides its customers in Heidelberg and the region with reliable electricity, gas and heat, and offers many services related to energy saving and climate protection. On behalf of the city of Heidelberg and other communities, they are also responsible for water supply. In addition, SWH operates the swimming pools, the cable cars, garages, and also controls the city coordination tasks and are a part of the funding for public transportation. With a turnover of over 200 million euros and more than 1,000 employees, of which around 350 are on loan to the regional transport company, it is a major employer in Heidelberg. As one of the largest public energy suppliers, SWH along with the City of Heidelberg and other partners is leading the way into providing electricity without any nuclear power. The energy concept 2020 shows the way to this goal: with a clear plan of action along the entire value chain of an energy supplier – this includes measures for greater energy efficiency and expanding renewable energies - from generation and storage through offering products [68]. According to [17] "Definition of Critical Infrastructures" SWH belongs to the Critical Infrastructure Sectors "Energy" and "Water" and the subsectors "Electricity" and "Public Water Supply" (see Figure 4).

Definition of Critical Infrastructures

Organizations and institutions of special importance for the country and its people where failure or functional impairment would lead to severe supply bottlenecks, significant disturbance of public order or other dramatic consequences.

Critical Infrastructures divided by sectors and subsectors

Sectors	Subsectors
Energy	• Electricity • Gas • Oil
Water	• Public water supply • Public sewage disposal

Figure 4: Classification of Critical Infrastructures [17]

The key organizations identified, besides SWH, are the Federal Office of Civil Protection and Disaster Assistance, City of Heidelberg, Regional Council of Karlsruhe and electricity consumers. Each of these actors have a specific role in this critical infrastructure. For example, the Federal Office of Civil Protection and Disaster Assistance is the governmental representative with an overall responsibility for Germany in terms of emergency management and relief [24]. The City of Heidelberg is another governmental representative with the responsibility for Heidelberg's overall emergency management including disaster reduction and resilience. Regional Council of Karlsruhe regulates this critical infrastructure in terms of policy development and supervision. See also Actor Analysis in Table 8 below. The electricity consumers rely daily on the service

provided by this critical infrastructure. These organizations rely on one another to provide a safe and reliable energy every day of the year.

Table 8: Actor Analyis BRAVO

Name of organization	Name of organization (English)	Level	Type	Role/responsibility in case study*
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	Federal Office of Civil Protection and Disaster Assistance	National	Public	Superior civil protection authority
Stadt Heidelberg	Heidelberg City	Local	Public	Municipal civil protection authority
Stadtwerke Heidelberg Netze	Stadtwerke Heidelberg Netze	Local	Private	Local utility company and distribution service operator (DSO)
Regierungspräsidium Karlsruhe	Regierungspräsidium Karlsruhe	Regional	Public	Federal civil protection authority

4.2.2 Current status working with resilience and assessing resilience

The key organizations identified (Federal Office of Civil Protection and Disaster Assistance, City of Heidelberg, Regional Council of Karlsruhe and electricity consumers) are following a guideline for companies and agencies [18] which was published by the Federal Office of the Interior in 2011.

A main part of this guideline is a checklist which is based on the following literature:

- American Water Works Association 2001 [6]
- British Standard 2006 [13]
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2005 [15]
- Bundesministerium des Innern 2005 [16]
- Egli 1999 [22]
- Federal Emergency Management Agency 2003 [16]
- Gustin 2004 [27]
- Innenministerium Baden-Württemberg und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2010 [33]
- Jungbluth 2005 [38]
- National Fire Protection Association 2004 [51]
- Umweltbundesamt 2001 [75]
- Umweltbundesamt 2001 [76]
- Zentrum für Alpine Umweltforschung 2000 [80]

In addition, the guideline includes a list of hazards. Following the guideline helps the companies and the agencies to identify threats, consequences as well as preventive and respond/recovery measures (Figure 5). Recovery measures are only part of resilience. The guideline does not include measurable key risk indicators.

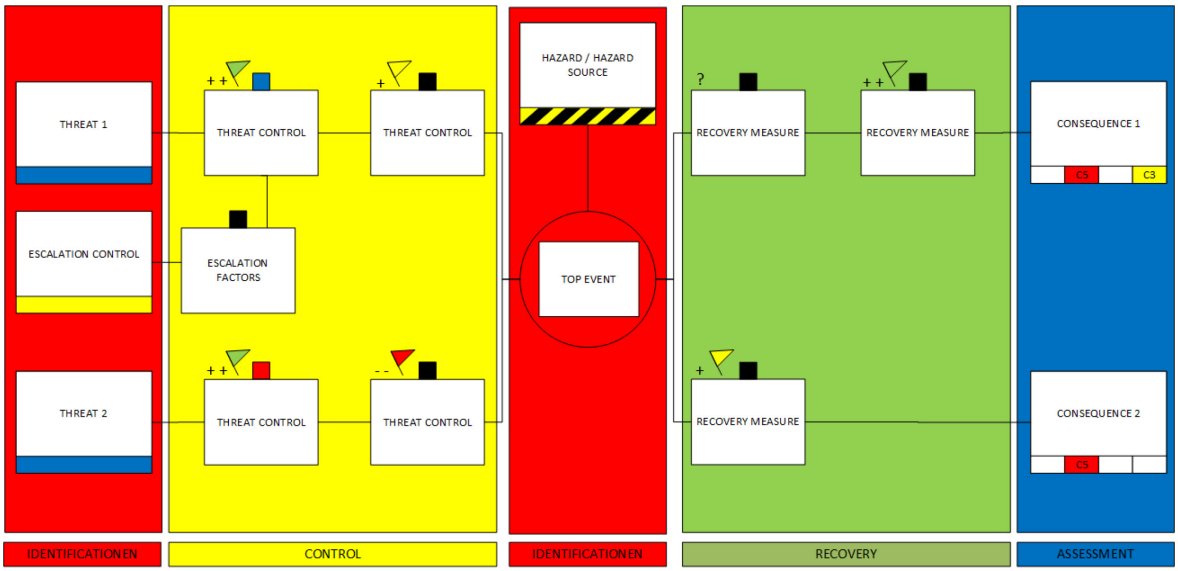

Figure 5: Bow-Tie Diagram

SWH follows the risk management framework given by the ISO 31000 [34] and the ISO 27001 [35] with tailored adaptations for the power and utility business. Additionally, SWH follows the recommendations given by the inter-trade organizations. Using charts, SWH tries to identify and continually understand new risks, threats, and opportunities. This method of understanding risks to this critical infrastructure is a continual process whenever a new development is considered. For each risk scenario, there are 10 key categories identified by the ISO 31000 as important for risk understanding. They are: name or title of risk, scope of risk, nature of risk, stakeholders, risk evaluation, loss experience, risk tolerance, appetite or attitude, risk response, treatment and controls, potential for risk improvement, strategy and policy developments. With these defined categories it is not only possible to understand risks and threats but also decides preventative and mitigation measures. For example, once a risk is identified answering the following questions on the chart, the next step of the process is to develop ways on how to respond and treat risks. At the end of the chart the potential to improve on the previously used techniques are identified.

SWH have identified three mains risks that are important to be considered and have developed the risk management framework for each as illustrated in Table 9, Table 10, and Table 11 according to [1].

The three risk tables are in the following order:

- Terrorist attacks
- Flash floods
- Cyber security breach

Table 9: 10 Steps to Understand Risks, Threats and Opportunities (Terrorist Attack), adapted from [1]

Nr.	Criteria	Description
1	**Name or title of risk**	Terrorist attack
2	**Scope of risk**	Large, loss of infrastructure, city devastation including company stakeholders, stolen data, loss of revenue
3	**Nature of risk**	Current business risk with high uncertainty of when and where this could occur with potentially high negative impact
4	**Stakeholders**	See Company's Stakeholder diagram in Figure 6
5	**Risk evaluation**	Not likely occurrence, with high magnitude of business interruption and other invaluable losses
6	**Loss experience**	Heidelberg has not yet experienced any terrorist attacks; Loss of water, heating, gas and ultimately monetary losses

Nr.	Criteria	Description
7	Risk tolerance, appetite or attitude	Tolerance – zero tolerance Risk attitude – taken very seriously and all precautions to avert the crisis as soon as possible
8	Risk response, treatment and controls	Good communication with the city police Object protection in the substations (bullet proof windows and roof windows, fencing around the building) Good communication with the control room in case of cut of power supply from any of the substations
9	Potential for risk improvement	Installations of security cameras, electronic keys to substations to allow entry to only some personnel SWH has decided to initiate a crisis management training program for employees beginning next year
10	Strategy and policy developments	Crisis Management squad related to the risk

Table 10: 10 Steps to Understand Risks, Threats and Opportunities (Flash Flood), adapted from [1]

Nr.	Criteria	Description
1	Name or title of risk	Flash flood
2	Scope of risk	Medium, loss of infrastructure, loss of distribution, harm to key stakeholders, loss of revenue
3	Nature of risk	A business hazard with moderate negative impact
4	Stakeholders	See Company's Stakeholder diagram in Figure 6
5	Risk evaluation	Likely occurrence, with medium magnitude of business interruption including infrastructure loss
6	Loss experience	Occasional flooding of the substation in the Old City, potentially power supply is cut off
7	Risk tolerance, appetite or attitude	Tolerance – medium tolerance (natural disaster) Risk attitude – taken very seriously and all precautions to assure customers are provided with basic amenities
8	Risk response, treatment and controls	Target for control of risk and desired level of performance Interconnections via a meshed system to provide power to the affected region Has worked efficiently till date Grid restoration procedures defined
9	Potential for risk improvement	Good city infrastructure Better water drainage systems
10	Strategy and policy developments	Modernization of systems

Table 11: 10 Steps to Understand Risks, Threats and Opportunities (Cyber Security Breach), adapted from [1]

Nr.	Criteria	Description
1	Name or title of risk	Cyber Security Breach
2	Scope of risk	Medium to extremely large, loss of data, loss function ability, complete system shutdown or failure, loss in reputation, loss in revenue
3	Nature of risk	Current operational risk and long-term hazard with potentially high negative impact
4	Stakeholders	See Company's Stakeholder diagram in Figure 6
5	Risk evaluation	Somewhat likely occurrence, with high magnitude of business interruption and/or reputation loss
6	Loss experience	Security systems resisted well so far. The IT-Systems are protected by state-of-the art firewalls, while the control room for the infrastructure is under special security surveillance.
7	Risk tolerance, appetite or attitude	Data is stored decentralized, in case of a data loss within from smart metering there are routines to create replacement values. The control room has a full redundancy in a remote place.
8	Risk response, treatment and controls	Certified security and risk management due to ISO:27001 and German "Energiewirtschaftsgesetz §11" Herein: Collection and documentation of all known risks including monitoring and routines.
9	Potential for risk improvement	Daily task
10	Strategy and policy developments	New administrative body to work on known and new risks together with departments and the managing board SWH is accredited according to a technical security management (TSM) program.

Additionally, SWH refers to their specific stakeholder diagram in order to consider, react, and communicate based on the affected stakeholders. Their specific stakeholder diagram is as follows:

Figure 6: Stadtwerke Heidelberg's Stakeholder Diagram

Although SWH does not currently operate under the term resilience, their risk assessment techniques are found in the definition of resilience defined in D 1.2 Report of this project i.e. the "*Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, respond/recover from disruptions caused by them and adapt to the changing conditions*." [37]. As described in Table 9, Table 10, Table 11 , for specific risk, measures are undertaken in different dimensions and phases. For example, for a cyber-attack scenario (see Table 11), measures are taken to understand risk considering the physical and social dimensions i.e. - at first they define the potential impact of an attack on the functionality of the critical infrastructure like loss of data to complete loss system shutdown causing the business interruptions, and/or loss of reputation. In addition, they assess their preparedness to deal with it such as the status of security systems, firewalls for IT systems, security surveillance. Furthermore, the redundancy measure such as decentralized data storage in remote location allows preparing for absorbing the shock in case of a terrorist attack event, or respond to an event by following the business continuity standard ISO 27001. Also, organizationally, preparing a strategy and policy development plan through an administrative body to work on known and new risks across the company and external stakeholders.

They also stress continually upon the importance of staying sustainable and reliable in the future for all of their stakeholders and they are currently looking for ways to evolve their risk assessment into a resilience assessment.

4.2.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: terrorist attacks, flash floods, Cyber security breach . To identify and continually understand new risks is a main challenge for the SWH. This creates a challenge to assess how resilient the system would be when encountered with an unknown event and prepare for the unknown.

Especially for the new town district "Bahnstadt" those risks are not finally identified as this part of the town only exists since 2011.

The district features its own energy concept which is partly self-sustaining with:

- Passive house standard as a universal construction method
- District heating supply which will be covered in the medium term by way of renewable energies
- Intelligent control of power consumption via smart metering

Nevertheless, the district continues to be a part of the whole supply grid of the SWH. Consequently, the Bahnstadt's energy, transportation and water infrastructure is designed to operate both as part of a large system but mainly to serve a more localized community independently of the wider network.

To fulfil this purpose, the SWH relies on multiple connected micro grids that can either operate together or individually. During a major hazard event those micro grids can buffer local service users from impacts elsewhere. Whereas IT is a key enabler allowing service providers to switch operations from micro grids to integrated networks and vice versa, it is also a major threat as it gives room for cyber-attacks and other kinds of terrorism.

Hence, the main challenges for SWH are identifying the most threatening hazards, getting reliable grid data to evaluate those hazards and measuring the impact of cyber-attacks on the IT system of the SWH.

Furthermore, the major needs and requirements are establishing key risks indicators, restoration of the grid system and installation of a better water drainage.

This is getting more important as SWH relies more and more on smart grid solutions (see Figure 7). The installation of sensor systems to identify the network situation becomes a "must" for smart network use and control. This involves appropriate IT infrastructures for information processing.

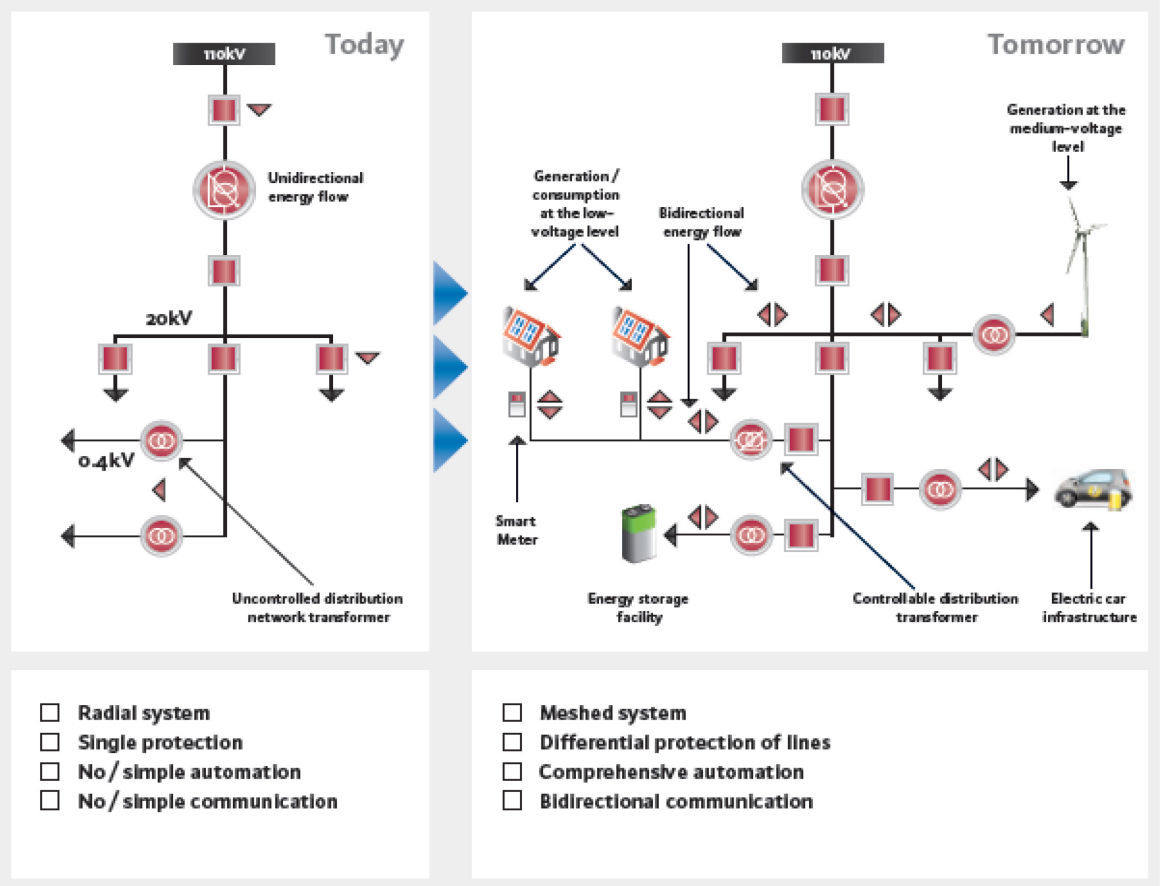

Figure 7: The distribution network today and tomorrow [19]

4.2.4 *Foreseen challenges, needs and requirements for assessing resilience*

The major need is to install a crisis management squad related to the risk. Furthermore, SWH intends to implement a crisis management training program for employees beginning next year. Another need is the further modernization of the existing infrastructure.

In a group interview which was held at SWH the participants were confronted with getting relevant data out of the IT-System of SWH. This is quite time-consuming and could result in negligence of acquiring the data. The factors such as manpower and complex IT systems make it a time consuming process. Acquiring enough and accurate data is essential to assess resilience of this critical infrastructure and hence, this is a challenge for SWH. In table 12 below, the challenges, needs and requirements for the BRAVO case are summarized.

Table 12. Challenges, needs and requirements for the BRAVO case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* terrorist attacks, flash floods, Cyber security breach 2. *Main challenges:* identifying the most threatening hazards, getting reliable grid data to evaluate those hazards and measuring the impact of cyber-attacks on the IT system of the SWH.	1. Further modernization of the existing infrastructure. 2. The outcome of cyber-attacks has to be considered. 3. To include the resilience concept into the current approach of the "Federal Ministry of the Interior" the existing checklist has to be extended by including thresholds for Key Risk Indicators. 4. Establishing key risk indicators.
Current needs and requirements	**Foreseen needs and requirements**
1. Need to have ood communication with the city police 2. Object protection in the substations (bullet proof windows and roof windows, fencing around the building) 3. Need for good communication with the control room in case of cut of power supply from any of the substations 4. Target for control of risk and desired level of performance 5. Need for interconnections via a meshed system to provide power to the affected region 6. Grid restoration procedures need to be defined 7. Need for a certified security and risk management due to ISO:27001 and German "Energiewirtschaftsgesetz §11" 8. Need to define the potential impact of an attack on the functionality of the critical infrastructure 9. Need to assess their preparedness to deal with it 10. Need for preparing a strategy and policy development plan	1. Installations of security cameras, electronic keys to substations to allow entry to only some personnel 2. To install a crisis management squad related to the risk. 3. Implement a crisis management training program for employees beginning next year. 4. Restoration of the grid system 5. Installation of a better water drainage.

4.2.5 Discussion and conclusion

So far it is established from the interview that the risk management system was sufficient to withhold any risks for the SWH. On the one hand this is a positive outcome, and on the other, this situation makes it even more difficult to evaluate the resilience of the existing system.

Whereas the existing risk management system was sufficient until today it has to be altered to resist new threats. Especially, the outcome of cyber-attacks has to be considered. To include the resilience concept into the current approach of the "Federal Ministry of the Interior" the existing checklist has to be extended by including thresholds for Key Risk Indicators.

Furthermore, cyber-attacks and their current outcome on the Stadtwerke Heidelberg have to be investigated. This investigation will also help to develop Key Risk Indicators for SCIs. Analyzing the current

and foreseen challenges, needs and requirements according to the five dimensions of resilience for the BRAVO case can be summarized in table 13 below. For this case study

Table 13. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the BRAVO case.

Dimensions of resilience	Examples from BRAVO
System/physical: Technical aspects, physical/technical networks, interconnectedness	Object protection in the substations (bullet proof windows and roof windows, fencing around the building) Installations of security cameras, electronic keys to substations to allow entry to only some personnel Restoration of the grid system Installation of a better water drainage.
Information/data: Technical systems dealing with information/data	Getting reliable grid data to evaluate hazards
Organizational/business: Business-related, financial and HR aspects and organizational networks	Implement a crisis management training program for employees Preparing a strategy and policy development plan Grid restoration procedures defined Certified security and risk management procedures
Societal/political: The broader societal/social context, indirect stakeholders	Good communication with the city police Interconnections via a meshed system to provide power to the affected region
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Identifying the most threatening hazards The outcome of cyber-attacks has to be considered. To include the resilience concept into the current approach of the "Federal Ministry of the Interior" the existing checklist has to be extended by including thresholds for Key Risk Indicators.

For this case study, resilience as a concept will be welcome as a tool making sense of and managing foreseen risks. Complexities mainly concerns connections to other SCIs. Data management mainly concerns the need for more reliable data.

4.3 *CHARLIE: The Austrian health care system*

4.3.1 Introduction

As a case study for the resilience of critical infrastructures in the context of health care systems the Austrian health care system is investigated. The treatment of patients in today's health care systems requires the complex coordination of several health care providers that are embedded in multiple formal and informal relationships among each other [59]. To understand the resilience of a health care system as a whole it is therefore necessary to focus not only on individual health care provider such as hospitals, but to also employ a systemic perspective [40]. Cost, quality, effectiveness, and resilience of care is also a property of the entire system of flows of patient through individual health care providers [10]. Although the main focus of the case studies in the SmartResilience project lies on individual cities, therefore it was decided to study the resilience of health care on a country-wide level.

In terms of "smartness" of critical infrastructures, health care systems world-wide have recently undergone or are currently subject to the revolution dubbed the big data age [64]. Health care systems produce abundances of observational data such as electronic health records or administrative claims data [44]. This development is catalyzed by the adoption nation-wide patient information systems and eHealth applications, which were both identified by the European Commission to be key enabling technologies, together with health technology assessments, to improve resilience, as well as accessibility and effectiveness, of health

care systems [21]. To gain a better understanding to which extent such novel technologies are known, used, or deemed relevant by the actors in the Austrian health care system, was one of the main motivations in this particular actor analysis.

Austria has a – for historical reasons – highly segmented health care system with competences split up between various regional or national organizations in different sectors of the health care system [58]. In general, one can distinguish between the outpatient sector (e.g. doctors, pharmacies, other health-related professions such as physiotherapy, etc.) and the inpatient sector (e.g. hospitals). Responsible for outpatient care in Austria are mostly more than 20 different social security institutions. Basically each of the nine federal states has its own institution, next to institutions for specific professions, such as government officials. All of these institutions are organized into single carrier organization, the Main Association of Social Security Institutions. In the inpatient sector the hospitals are again managed by regional carrier organizations, next to some exceptions of hospitals that are managed directly by the Republic of Austria. The latter most notably includes the General Hospital in Vienna, which is the largest hospital in Europe that is built in a compact structure i.e. that is not spread over several locations. For the actor analysis carried out in this task, the focus was therefore on the relevant actors on these individual levels: nation-wide or regional, and hospital-based actors. Also see Table 14.

Responsibility for response to disasters and protection from catastrophes is spread among nation-wide and regional agencies, as well as individual health care provider. In brief, on a national level general guidelines are formulated that are implemented in the context of specific individual provider and regional agencies. To investigate actors on the level of individual provider, the relevant actors were interviewed from technical direction of the General Hospital in Vienna, on a nation-wide level key actors from the Main Association of Social Security Institutions were interviewed. Furthermore, opinions of experts for formulating guidelines for crisis response plans for hospitals were analyzed.

Table 14: Actor Analysis CHARLIE

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
AKH Wien	General Hospital of Vienna	Regional (sub-national)	Public	The general hospital of the city of Vienna, Austria is the largest hospital in Europe and employs about 9,000 people and treats around 95,000 inpatients annually. It is also the city's university hospital and the site of the Medical University of Vienna.
Wiener Krankenanstaltenverbund (KAV)	The Vienna Hospital Association	Regional (sub-national)	Public	The Vienna Hospital Association includes all hospitals and geriatric centres of the City of Vienna and is one of the biggest hospital operators in Europe.
Hauptverband der österreischichen Sozialversicherungsträger	Main Association of Austrian Social Security Institutions	National	Public	Carrier organization of all social security institutions of Austria which are responsible for health and accident insurance, as well as public pension schemes.

4.3.2 Current status working with resilience and assessing resilience

On the level of individual hospitals, resilience or related concepts are understood exclusively in the context of specific scenarios. Different scenarios of disasters and man-made crises are therefore identified that might pose significant challenges that cannot be managed effectively in the normal mode of operation. These scenarios include, for instance, situations where the capacity of the emergency department is exceeded by far such as the collision of two metro trains, but also failures of other infrastructures that are critical to the functioning of the hospital such as power supply. Great attention is also paid to terrorism, which may affect both areas (failure of other critical infrastructure or mass casualty incidents). In order to face these challenges, the organizations make extensive use of checklists that are formulated in processes that involve all relevant actors and stakeholders for those particular scenarios. In the case of a mass casualty incident, for instance, a clearly defined patient guidance system is in place to ensure that patients in a critical state are given priority over less critical cases. This happens in coordination with agencies that are responsible for routing ambulance cars in the most efficient way by, both, taking the criticality of the state of the patient into account and potential obstacles in the route to the respective hospitals. In order to assess the effectiveness of the response measures, the organizations rely chiefly on simulation exercises. These exercises are subsequently evaluated to identify potential to further optimize the response measures.

On a systemic, nation-wide level, actors are primarily concerned with scenarios that might affect the quality and accessibility of care on longer terms. Therefore, the focus shifts from emergency response to planning and preparing for, as well as adapting to certain types of disruptions on a systemic level. Of particular interest here are events that lead to a change in the number of health care providers in a certain region and the long term consequences of such changes. For instance, a certain type of specialized medical services might become unavailable over an extended period of time due to a localized disaster, such as floods. Next to disasters, changes in the density of health services might also result from budgetary changes or other socio-economic developments, e.g. a region becoming unattractive for certain types of doctors. But in principle it is also feasible that the density of care providers might increase due to some external events. Both of these developments – an increase or a decrease in the density of certain types of medical services in a given region – might substantially lower the quality and effectiveness of care. Clearly, a decrease in the density of care provider bears the risk that waiting times or travel distances increase too much for the population such that effectively the services become inaccessible. A disproportional increase in medical services, on the other hand, might lead to a situation where the individual provider ceases to be economically viable since the number of patients per provider simply becomes too low. In order to plan for such events and adapt to changes in the health care provider landscape, quantitative tools are used that provide information on the regional density of each type of health care provider relative to the covered population. These numbers are compared throughout the country in order to estimate the optimal number of providers and make the corresponding adjustments.

4.3.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: situations where the capacity of the emergency department is exceeded by far, terrorism, events that lead to a change in the number of health care providers in a certain region, changes in the density of health services. On the level of individual hospitals, the current challenges for assessing resilience lie mostly in a better understanding of scenarios that might lead to severe disruptions. In particular, the formulation of effective response plans through checklists is the method of choice. It has been identified that the largest current need for assessing resilience in the face of these scenarios lies in large-scale exercises that simulate the scenarios and might give valuable insights into how the current processes can be further optimized. Thereby it has been noted that the processes are then most effective, if they stay as close to the normal mode of operation as possible. That is, any crisis response measures that require certain actions that are unfamiliar to the acting persons are typically detrimental to the overall response and resilience of the system or organization.

On the systemic level it has been recognized and even acknowledged on a legislative level that observational health care data, such as administrative claims, should be used in health planning and therefore also in planning and preparing for disruptive events. One of the major challenges in this respect results from the federalism in the Austrian health care system. That is, each federal state typically used their own patient information system with in parts widely differing data standards, e.g. with respect to the time resolution of

the data. It requires therefore extensive work to harmonize the different data sources, which is a prerequisite for getting full coverage of the status quo of the health care system. Next to data quality, a substantial challenge is the communication of complex interventions to other stakeholders in the health care system. As an organically grown and federal system, health care in Austria is in some senses extraordinary robust with respect to changes. It is therefore an absolute necessity that all actions and potential changes are also assessed along a political dimension and not only using evidence-based methods alone. However, it is also acknowledged that all actions aimed at increasing the resilience of the health care system must take into account information about the system itself. Decisions on whether there should be a (dis-)investment in specific sectors of the health care system must be based on an understanding of how interventions will impact health-related and economic parameters. A prerequisite for such an understanding is an efficient infrastructure for nation-wide patient information systems. An overview of the current infrastructure in this regard is shown in Figure 8. There a schematic overview of the Austrian health information system infrastructure is given. The aim of such an information system is to collect patient- and provider-level data from the inpatient and outpatient sectors, as well as from pharmacies and to make them available for various eHealth applications and services.

4.3.4 Foreseen challenges, needs and requirements for assessing resilience

On the individual-provider level it is anticipated that the growing interconnectedness of critical infrastructures will become increasingly challenging. On the one hand, hospitals are becoming increasingly smart themselves, for instance through inter-connected technical facilities that require a complex IT infrastructure as well. This complex infrastructure will need to be operated by highly trained technical personnel in order to function properly. The increasing interconnectedness is of course not only apparent within the hospital, but also on its reliance on other critical infrastructure. Cascading failures in interconnected infrastructures have indeed been observed in the past. For instance, in Italy a local blackout triggered failures of IT infrastructure that was critical for the functioning of other parts of the power grid, which in turn went black [14]. This led to a failure of yet other control systems that in turn shut down other nodes in the power grid as well, leading to a cascade that eventually sent more than half of the country into a blackout. Further training and exercises, as well as the formulation of detailed response plans and checklists are thought to be necessary for such kind of scenarios.

On the systems level it will become of increasing importance to make the abundances of observational data manageable. It is also recognized that these developments offer novel types of vulnerabilities that have not necessarily been on the radar in health management so far. For instance, Austria is currently introducing a nation-wide shared electronic health record system called ELGA. Such observational health data might be an attractive target for various forms of cyber-crimes or fraud. Data security will therefore be a topic that must be addressed by the relevant actors in the health care system. As this field is typically not a core competence in that particular type of agencies and organizations, a building up of a secure data infrastructure is anticipated to be one of the major challenges in the future. Also related to this, data quality assessment and harmonization will become more and more important. In table 15 below, the challenges, needs and requirements for the Austrian healthcare system are summarized.

Table 15. Challenges, needs and requirements for the CHARLIE case.

Current challenges	Foreseen challenges
1. *Most relevant threats*: situations where the capacity of the emergency department is exceeded by far, terrorism, events that lead to a change in the number of health care providers in a certain region, changes in the density of health services 2. *Main challenges:* a better understanding of scenarios that might lead to severe disruptions, harmonize the different data sources, which is a prerequisite for getting full coverage of the status quo of the health care system, the communication of complex interventions to other stakeholders in the health care system	1. Growing interconnectedness of critical infrastructures 2. Important to make the abundances of observational data manageable.

Current needs and requirements	**Foreseen needs and requirements**
1. Formulate effective response plans through checklists. 2. Large-scale exercises that simulate the scenarios and might give valuable insights into how the current processes can be further optimized 3. The communication of complex interventions to other stakeholders in the health care system.	1. Data security must be addressed by the relevant actors in the health care system. 2. Further training and exercises, as well as the formulation of detailed response plans and checklists are thought to be necessary to be able to manage cascading effects. 3. Data quality assessment and harmonization will become more and more important.

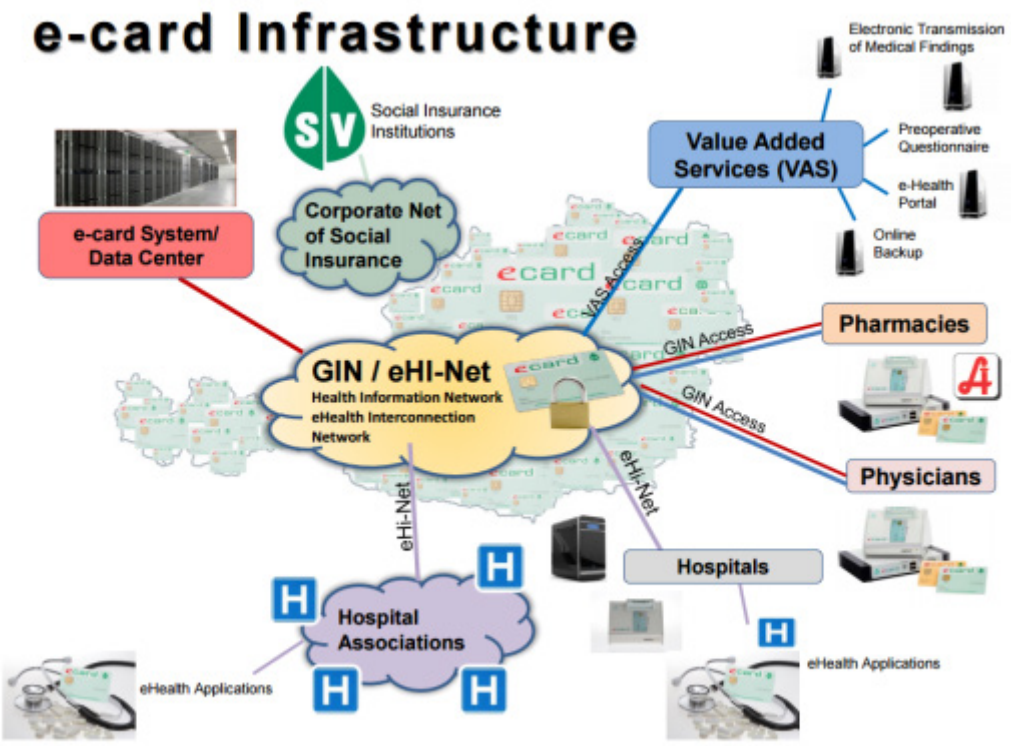

Figure 8: Overview of the Austrian e-card Infrastructure that enables a shared electronic health record system (ELGA) that is currently being implemented throughout Austria.

4.3.5 Discussion and conclusion

In the course of this analysis it has become clear that the assessment of resilience takes on very different forms depending on the organizational level. Therefore the results on an individual level – the hospital perspective – were contrasted with the corresponding results on a nation-wide level – the systems perspective.

In brief, assessment of resilience on the individual-level is almost exclusively based on concrete scenarios and focuses on immediate or short-term response measures. On the systems-level, on the other hand, assessment of resilience is typically concerned with scenarios that are formulated in a quite general way with effects that are mostly relevant on longer time horizons. Overall little relations were found between resilience efforts on the individual and on the systemic level, although the actors certainly recognized and acknowledged the importance of assessing resilience across the entire spectrum of health care.

In terms of planning, preparing, and adapting to adverse events, actors on the individual-level stressed that in their opinion in order to improve resilience of the organizations in question, crisis response measures

should always be implemented in a way such that they do not deviate more than necessary from the normal mode of operation. One of the key findings on the systems-level in terms of "smartness" of infrastructures is that the potential of health information systems has been recognized in order to design interventions such that the health care system improves in resilience in a way that is fiscally sustainable. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the CHARLIE case can be summarized in table 16 below.

Table 16. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the CHARLIE case.

Dimensions of resilience	Examples from
System/physical: Technical aspects, physical/technical networks, interconnectedness	Growing interconnectedness of critical infrastructures The communication of complex interventions to other stakeholders in the health care system.
Information/data: Technical systems dealing with information/data	Different patient information systems are used in different states. Important to make the abundances of observational data manageable.
Organizational/business: Business-related, financial and HR aspects and organizational networks	Large-scale exercises that simulate the scenarios and might give valuable insights into how the current processes can be further optimized
Societal/political: The broader societal/social context, indirect stakeholders	Data security must be addressed by the relevant actors in the health care system. Further training and exercises, as well as the formulation of detailed response plans and checklists are thought to be necessary to be able to manage cascading effects.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	A better understanding of scenarios that might lead to severe disruptions

For this case study, resilience is not yet a widely used concept (although probably useful), whereas organizational complexity due to various standards and terminologies is a widely accepted issues as well as data management (for the same reasons).

4.4 DELTA: The transportation infrastructure of Budapest airport

4.4.1 Introduction

The Budapest Liszt Ferenc International Airport (IATA: BUD, ICAO: LHBP, General: BLFNR) is the largest international airport in Hungary and is built at the easternmost limits of the Hungarian capital city, Budapest. Its construction began in 1940 and it has developed continuously since, the current phase is the project BUD 2020 with investments of over 165 million EUR, including a new passenger pier, a new passenger terminal and an airport hotel and the "Cargo City". The total land area of the facility is 15,050,000 square meters, 25% larger than London Heathrow International Airport [5]. The facility has both commercial (passenger, cargo) and general aviation traffic, but is also occasionally serving military airplanes (e.g. KC-130s in Balkan wars). In 2015, the commercial aviation served 10,298,963 passengers, 92,214 airplanes and 91,421 tons of cargo with coordinated work of approximately 12,000 people [2].

Air Control Tower, LHBP (BUD)

Crime scene of bombing. (Hetek-archív)

During its history, there has been no successful bombing or terror attacks against the airport. However, two RAF terrorists, Horst Ludwig Meyer and Andrea Klump, who were German citizens but received training in Arab countries in 1988, attempted to blow up a transfer bus with Jewis "Aliyah" emigrants travelling to the airport with the intention to emigrate to Israel. The attack commenced on 23rd of December in 1991, but was unsuccessful. Only two police officers were severely injured and four passengers suffered minor injury as the police car deflected the main force of the bomb explosion. The perpetrators were chased down in 1999, when Horst died in gunfight with the police. Andrea Klump was arrested and sentenced for 12 years in prison [26].

Currently, BLFNR is the second most protected critical infrastructure in Hungary. The level of security is provided by a well-coordinated cooperation of authorities (including first responders) and private companies, with the airport operator company in the first place. With 52 flight companies, 8 authorities, 3 ground handling companies, 27 shops and so on, there are more than one hundred of actors, all obliged to take its part in protection of the airport as a critical infrastructure. Hence, the airport is not run by one single entity but a group of stakeholders, who all carry out critical infrastructure protection on two levels: firstly, each organization or company is protecting themselves to ensure continuous operation within this critical infrastructure, secondly, each organization or company is carrying out its designated role in the protection of the airport as a critical infrastructure, contributing to the efforts of the whole. There are some stakeholders who supervise or organize the others. This can mean that one stakeholder, e.g. the Airport Police Directorate is supervising the work of another stakeholder, e.g. the Budapest Airport Armed Security Guard. However, in most cases co-operation is based on memorandums of understanding or mutual interests. At the airport level, resilience-related cooperation is coordinated by the Airport Security Committee, serving as a platform for managers of stakeholders, facilitating cooperation and understanding at top-level. Out of these there are several key stakeholders as outlined below, explaining their importance as remarks in brackets (see also Table 17):

- Airport Police Directorate (part of Hungarian National Police (HNP), general policing and first response at airport, supervising all security related activities at the airport)
- Budapest Airport Zrt. (airport operator)
- National Transport Authority (main regulator and supervisor)
- Airport Disaster Management Directorate (first responder for natural threats and accidents)
- Wizz Air (W6) flight company (has main base in the airport)
- National Security Agency (early warning on man-made threats)
- Centre for Counter-Terrorism (prevention of terrorist attacks, including cyberattacks)
- HungaroControl (national air traffic control on civil aviation)

As part of this study, the Hungarian National Police (HNP) organized a group interview at Airport Police Directorate premises where senior experts (from 10 to 30 years of airport experience) representing the key actors answered the interview protocol (see Annex 3). The rest of this case study is based on information that was received during the group interview, and consensus was reached between the participants in every question.

Table 17: Actor Analysis DELTA

Name of organization	Name of organization (English)	Level	Type	Role/responsibility in case study*
Országos Katasztrófavédelmi Főigazgatóság	General Directorate for National Disaster Management	National	Public	General responsibility for disaster management (including firefighters) in Hungary. For the airport, its main role is to operate the firefighter service, and its second role is to monitor the ADR transports.
Budapest Airport Zrt.	Budapest Airport Ltd.	Local	Private	Main operator of Budapest airport, including T1 test site, with the general responsibility of operating the airport as a critical infrastructure.
Magyar Állam	The Hungarian State	National	Public	Owner of the airport and the international aviation traffic rights. Currently operating the airport through Budapest Airport Zrt.
Nemzeti Közlekedési Hatóság	National Transport Authority	National	Public	The authority executes all administrative and supervision activities related to transport, i.e. supervises and monitors the transport market participants' activity and operation.
Repülőtéri Rendőr Igazgatóság	Airport Police Directorate	Regional (sub-national)	Public	Responsible for police duties at the airport and along the main road leading to the airport. Responsibilities include fight against crime and terrorism, border control, public order as well as aviation security.
HungaroControl Zrt.	HungaroControl Ltd.	Local	Private	Provides air navigation services in the Hungarian airspace and (on a NATO assignment) the upper airspace over Kosovo, trains air control personnel and conducts air navigation research and development.
European Aviation Safety Agency	European Aviation Safety Agency	Other	Public	Ensures the highest common level of safety protection for EU citizens as well as environmental protection, manages single regulatory and certification process among Member States, facilitates the internal aviation single market and creates a level playing field and works with other international aviation organizations and regulators as a European Agency.

4.4.2 Current status working with resilience and assessing resilience

Work with resilience starts with anticipation and preparation. Therefore, each stakeholder has first to assess threats and possible scenarios, mostly disruptive events. Regarding threats, human factors are in the main threat: terrorism, property crimes endangering or disrupting operation, malevolent use of airport systems or airplanes, attacks or incidents coming from outside of the airport (UAV fly-in, firing lasers at approaching airplanes, MANPADS firing at airplanes), accidents and disruptions caused by human negligence as well as strike. Natural disasters are second in importance [72].

In addition, many other scenarios can be recognized as posing a potential threat. The most important ones are: systems without redundancy or that are too dependent on other systems, lack of safety or security by design (from construction design to smart systems design), lack or inoperability of backup systems, inappropriate Facility Management, bad or occasional maintenance, inappropriate training, and exceeding passenger handling capacity [36].

Adaptation cannot be accomplished without timely identification. To achieve this, stakeholders continuously monitor the global security situation, the global health situation (pandemics), number and status of customers, meteorology, regulatory framework, regional air traffic (e.g. Ukraine is now a dangerous airspace), perform continuous tracking of staff working at the airport, filtering out Malicious Insiders and Smart Infiltrators as well as unreliable or undertrained staff. Surveillance of airport premises is another leg of this early warning system. Also, some of the stakeholders are using an Airport Security Management System, including Safety Performance Indicators and Security Performance Indicators. The most important source is the continuous newsfeed and flow on information between stakeholders of the airport. In a first step, the information is analyzed by human experts to identify relevant changes. Most of the stakeholders use Change Management Systems, as a standalone system or as integrated into risk assessment models. In addition, there are regular drills to prepare the staff and refine response procedures.

Airplane external fire drill

4.4.3 Main threats, current challenges, needs and requirements for assessing resilience

Naturally, the cores of current challenges are addressing the most relevant threat scenarios. These include: terrorist attack, direct terrorist threat, bomb threat, security breach or security compromise (unchecked passenger in the Security Restricted Area), airplane disaster, airplane in danger, power outage, sudden cease of operation in case of an important stakeholder (dependability), or unexpectedly dangerous objects (e.g. Samsung Note S7).

To cope with such challenges, most stakeholders have their individual Action Plans, Business Continuation Plans or Emergency Response Plans. In addition, the airport has an Airport Emergency Plan coordinating stakeholders. However, it is important to highlight that those plans cannot cover all possible scenarios, therefore it is essential to have staff with expertise in crisis management that are able to follow the plans but be flexible if current scenario is out of the scope of the plan. This creates a disaster resilience system where airport-wide and organizational emergency plans pair up with individual crisis management competences with required flexibility. For each scenario, relevant experience is analyzed and plans updated as necessary. Therefore it is important to investigate all incidents thoroughly, but not with the intention to find someone responsible or to clear all employees, but the inquiry has to focus on detecting gaps and vulnerabilities.

Improvised cover against volcanic ash in 2010

To adapt to new threats and prepare for known emergency scenarios, regular emergency drills are carried out, which are very good platforms for assessing resilience. Airport stakeholders assess resilience on continuous basis (flight companies and first responders) or on periodic basis (other stakeholders). There is a major drill with a connected resilience assessment every second year. Several examples can be highlighted: El-Al Security Drill, BCP Drill, ER Drill, Fire Drill. These are drills organized around different emergency

situations or scenarios, known ones as well as new threats. Furthermore, table-top scenarios as well as resilience audits and investigation of incidents are also carried out as assessment of resilience, however, the main foundation of the resilience assessments at the BLFNR are regular drills. Different drills require different cooperation, for example Air Traffic Control with Counter Terrorism, Disaster Management with Airport Police Directorate and Flight Companies. Periodically, drills are organized when all stakeholders are involved. During such an assessment, different indicators are used to measure performance: Time measure, human resources required, estimated fatalities (e.g. CT drill with soap bullets), cost estimation or risk assessment (RA 5x5 matrix), selecting critical business procedures, Fatal Accidents Rate (disaster per departure) as well as security and safety related key progress indicators.

The resilience definition guiding BLFNR is: "*ensuring business continuity with the ability of fast respond/recovery from disruptive events and adaptation to sudden changes*". The continuous operation of the airport is ensured by organic cooperation of stakeholders operating on the airport and others providing services related to the airport (public transportation, taxi service etc.). Almost all stakeholders use above definition of resilience and carry out joint efforts as necessary. There are two main types of resilience highlighted: planned and improvised resilience. Planned resilience is when stakeholders are prepared for a given event, as it happened already before and the critical infrastructure adapted itself already. The effectiveness of this planned resilience mostly relies on staff expertise and quality of plans. Improvised resilience can be metered when there are unexpected or previously not happened events, therefore plans are not available. The effectiveness of improvised resilience mostly relies on flexibility and sharp-mindedness of the staff. However it should here be noticed, that in case of certain first responders, resilience is handled as a basic duty element and not distinguished from standard operations (e.g. disaster management), while some other stakeholders do handle resilience as part of Enterprise Risk Management. Sometimes this means – as mentioned above - that one stakeholder, e.g. the Airport Police Directorate is supervising the work of the other stakeholder, e.g. Budapest Airport Armed Security Guard, while in most cases co-operation is based on memorandum of understanding or mutual interest. At the airport level, resilience-related cooperation is coordinated by the Airport Security Committee, serving as a platform for managers of stakeholders, facilitating cooperation and understanding at top-level.

MALÉV suddenly ceased operation, 2012 (BUD)

4.4.4 Foreseen challenges, needs and requirements for assessing resilience

It is assumed that the first half of the "u-curve" (see Figure 1) is well handled, including preparation, resistance and absorption of disrupting events, even some adoption at the other end. The second half, especially respond/recovery is much less cared about. Although stakeholders do have Business Continuity Plans and the airport has an Airport Emergency Plan, stakeholders usually hardly understand the benefit from costly redundancy and other respond/recovery-related investments [60]. It would be good to go beyond the response phase and have assessments also of the respond/recovery phase. For example, it would be good to assess robustness of business critical processes. The right side of the "u-curve" can be better understood as staircase where robustness determines steepness of stairs, as described in the Integrated Business Continuity and Disaster Recovery Planning (IBCDRP) framework (see Figure 9) which is a novel framework and first candidate as basis for the overall stress-test framework [63].

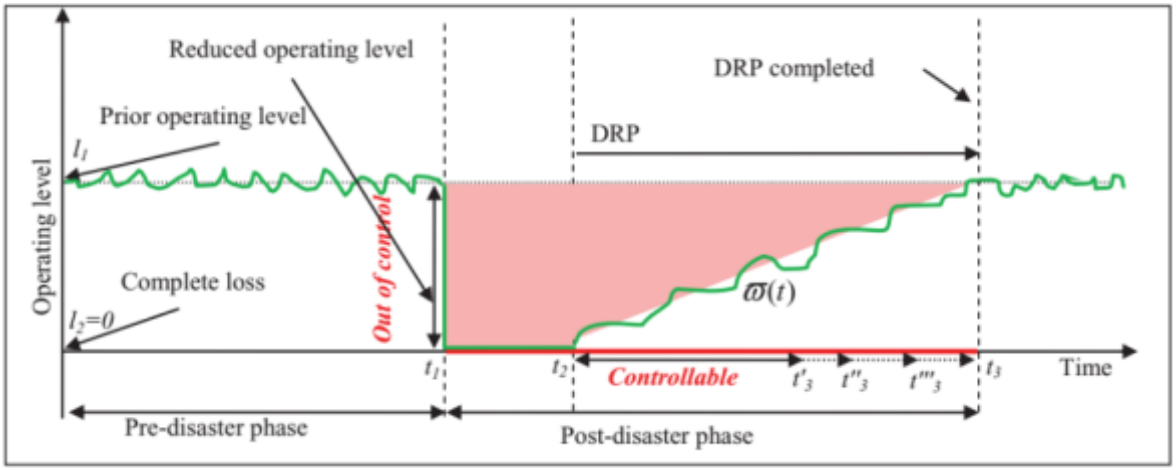

Figure 9: IBCDRP framework for Complete Operation Loss

In addition, there are some scenarios which are not possible to be modelled in a drill and hence not assessed in that manner, due to extreme cost or real disruptive effect on air traffic (e.g. explosion on runway). It is important to raise awareness that drills and resilience assessments have to be taken seriously, not just as a matter of some more paperwork. The best resilience assessments are put forward when they are connected to drills. However, sometimes it is hard to convince stakeholders to invest money into such near-real drills and resilience assessments. There is a need for something that can be objectively measured and justified within the As Low As Reasonably Practicable (ALARP) approach. Also, there is a need for increased budget expenses on resilience assessments and drills and assessment has to be carried out objectively with involvement of external, independent experts, Red Teams (hired ethical hackers and infiltrators testing vulnerabilities) etc. [42].

Regarding indicators, an extensive number of industry-related RIs are in use, both quantitative indicators (e.g. time measurement) and qualitative indicators (e.g. 3-level Priority Scale). Quantitative indicators have target value and performance is measured in percentage of this target value. Qualitative indicators are results of analysis of a given situation resulting in classification using pre-defined assessment models. However, there should be indicators developed for assessment of respond/recovery and adaptation (e.g. time spent until full respond/recovery). Other phases of resilience are covered by indicators; however their level still can be increased.

It is difficult to explain indicators to corporate decision makers e.g. why further investment into security is imminent. Indicators shall be standardized and benchmarked (supervised). The most important thing is to establish indicators working for all Critical Infrastructures. As general indicators, one ideal candidate is a qualitative indicator for cost/benefit analysis derived from multiple quantitative indicators (cost, DaLa, FAR etc.). Next step can be indicators valid for one or more industrial sector, bridging to currently existing and quite well defined array of indicators in given industries. Indicators has to be able to be presented in different resolution, from red-yellow-green bar to well detailed 3D graphs, as corporate financial decision makers need simple but convincing explanations to secure budgets, while experts need high resolution indicators to identify gaps and areas able to be developed. This requirement of same-time scalability and multi-levelness is the biggest challenge for indicators. Indicators have to be clear, realistic, measurable, tangible, standardized, harmonized and performing.

There have to be a common understanding on measurement methods, formulas for calculations and evaluation of indicators across industrial sectors. A method should be developed deriving cost/benefit analysis using indicators, weighting indicators and so on. Indicators have to be easily understandable. A constant development, supervision and benchmarking of indicators is needed. Supervised RIs indicators have to be revised from time to time as well as new indicators coming from assessments or relevant experience shall be validated to achieve supervised status.

As the airport is moving forward in becoming increasingly “smart”, participating in the “SmartAirports” project and working on adaptation of Airport 4.0 concept, this critical infrastructure will become different and it may raise new vulnerabilities, however, it is possible that it will solve other vulnerabilities. For example the traditional check-in desk is not as much important as before, as „smart” solutions as self-check-in have

made them almost obsolete [39]. In table 18 below, the challenges, needs and requirements for the Budapest airport are summarized.

Table 18. Challenges, needs and requirements for the DELTA case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* Terrorist attack, direct terrorist threat, bomb threat, security breach or security compromise (unchecked passenger in the Security Restricted Area), airplane disaster, airplane in danger, power outage, sudden cease of operation in case of an important stakeholder (dependability), or unexpectedly dangerous objects (e.g. Samsung Note S7) 2. *Main challenges:* Covering all possible threat scenarios by means of drills due to extreme costs	1. Lesser focus on respond/recovery phase in the U-curve proposed in D1.1 2. Convincing the stakeholders to invest in resilience assessment and near-real drills 3. Understanding of the stakeholders about the benefits from costly redundancy and other respond/recovery related investments 4. Difficulty in explaining the indicators to the decision makers 5. New vulnerabilities due to the use of smart and new technologies
Current needs and requirements	**Foreseen needs and requirements**
1. Thorough investigation of all the incidents, 2. Regular drills to assess the state-of-the art 3. Expertise of the staff in crises (know/unknown), flexibility & sharp mindedness of staff 4. Detection of all gaps and vulnerabilities 5. Need to have planned and improvised resilience 6. Ensure quality of plans 7. Cooperation, memorandum of undertaking, mutual interests with all stakeholders involved e.g. Air Traffic Control with Counter Terrorism, Disaster Management with Airport Police Directorate and Flight Companies 8. Measuring success of drills based on indicators from risk assessment, safety, security domains 9. Understanding at top-level	1. Properly and adequately combine drills and resilience assessment This implies the indicators to measure resilience should be derived and checked during the drills[3]. The user should be able to objectively assess resilience and justify within the As low As reasonably practicable approach and including cost benefit analysis of the improvement measures based on indicators. The assessment should Go beyond the response phase and focus on the assessment of respond/recovery plans, adaptation by means of indicators, assess robustness of critical business processes as it determines the steepness of the curve 2. Resilience assessed in a given scenario should be as quantifiable as possible In each phase of the resilience cycle it should be possible to determine which values are providing the "composite resilience indicator" (e.g. resilience level proposed in D1.2. 3. Establish agreed check list of indicators in cooperation with stakeholder The agreed checklist of indicators for assessing resilience should be established in cooperation with all important stakeholders from. Airport, National bodies, International associations (IATA), external, independent experts, Red teams 4. Ensuring the quality of Indicators Indicators need to be simple, realistic, measurable,

[3] Drills: Coordinated, supervised activity usually employed to validate a specific function or capability in a single agency or organization. Drills are commonly used to provide training on new equipment, validate procedures, or practice and maintain current skills. For example, drills may be appropriate for establishing a community-designated disaster receiving center or shelter. Drills can also be used to determine if plans can be executed as designed, to assess whether more training is required, or to reinforce best practices. A drill is useful as a stand-alone tool, but a series of drills can be used to prepare several organizations to collaborate in an FSE. For every drill, clearly defined plans, procedures, and protocols need to be in place. Personnel need to be familiar with those plans and trained in the processes and procedures to be drilled.

	standardized, benchmarked and performing. The need to be revised of indicators from time to time. The indicators that work for all Critical Infrastructures i.e. recommended should be identified. 5. Increase the cooperation awareness of the stakeholders Raise awareness in general about resilience assessment and drills, Involvement of external, independent experts, Red teams

4.4.5 Discussion and conclusion

The BLFNR resilience definition is: "ensuring business continuity with the ability of fast respond/recovery from disruptive events and adaptation to sudden changes". There is a distinction between two main types of resilience: planned resilience and improvised resilience, depending of existence of anticipation and preparation phase. In the civil aviation, all stakeholders use the concept of resilience but are focused on the anticipation, preparation, absorb and respond phases of resilience, while respond/recovery and adaptation is inadequately addressed. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the DELTA case can be summarized in table 19. below.

Table 19. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the DELTA case.

Dimensions of resilience	Examples from DELTA
System/physical: Technical aspects, physical/technical networks, interconnectedness	Various intrusions into the physical and informational systems
Information/data: Technical systems dealing with information/data	New vulnerabilities due to the use of smart and new technologies
Organizational/business: Business-related, financial and HR aspects and organizational networks	Convincing the stakeholders to invest in resilience assessment and near-real drills Properly and adequately combine drills and resilience assessment
Societal/political: The broader societal/social context, indirect stakeholders	Understanding of the stakeholders about the benefits from costly redundancy and other respond/recovery related investments Establish agreed check list of indicators in cooperation with stakeholder Increase the cooperation awareness of the stakeholders
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	The ability to make flexible responses in case of events beyond scenario-planning (improvised resilience) Resilience assessed in a given scenario should be as quantifiable as possible Ensuring the quality of Indicators

For this case study, resilience is a useful concept because it can wide the understanding of challenges to address and the vulnerabilities in the current means of managing them.

4.5 ECHO: An urban large industrial zone in Pančevo

4.5.1 Introduction

City of Pančevo with its Southern Industrial Zone is chosen to represent a case study for the resilience of critical infrastructures as a representative of industry sector, with many recognized threats in the

neighborhood, in a smart city. In order to perceive and understand the influence of industry in the sense of resilience it is necessary to cover the impact of each individual risk factor in this industrial zone as well as the impact of this zone on other systems of smart city. Therefore, not only representatives of industry were included, but all the complex relationships between the industry zone, representatives of the City and the Ministries that regulate the zone.

Figure 10: Geographic location of the city Pančevo

Pančevo is a city located in the southern part of Autonomous Province of Vojvodina, in Republic of Serbia (see Figure 10: Geographic location of the city Pančevo). The city is located on the banks of the Danube and Tamiš, in the southern part of Banat, and it is the administrative headquarters of the South Banat District. Pančevo is the fourth largest city in Vojvodina by population. According to the official census of the year 2011, the city of Pančevo has 123,414 inhabitants.

City of Pančevo has the so called Southern Industrial Zone located at the southeast edge of town, right next to the residential area of the city, app. 4 km away from the city center (see Figure 11). In addition to the compound of the HIP-Petrohemija a.d. Pančevo, this zone includes the HIP Azotara Pančevo a.d. and NIS Oil Refinery Pančevo. The area is connected to road, rail and river circulation by means of the port on the Danube River. In this industrial zone there is a production of petroleum products, basic chemical products, polyethylenes, mineral fertilizers, calcium ammonium nitrate, carbamide and NPK fertilizers.

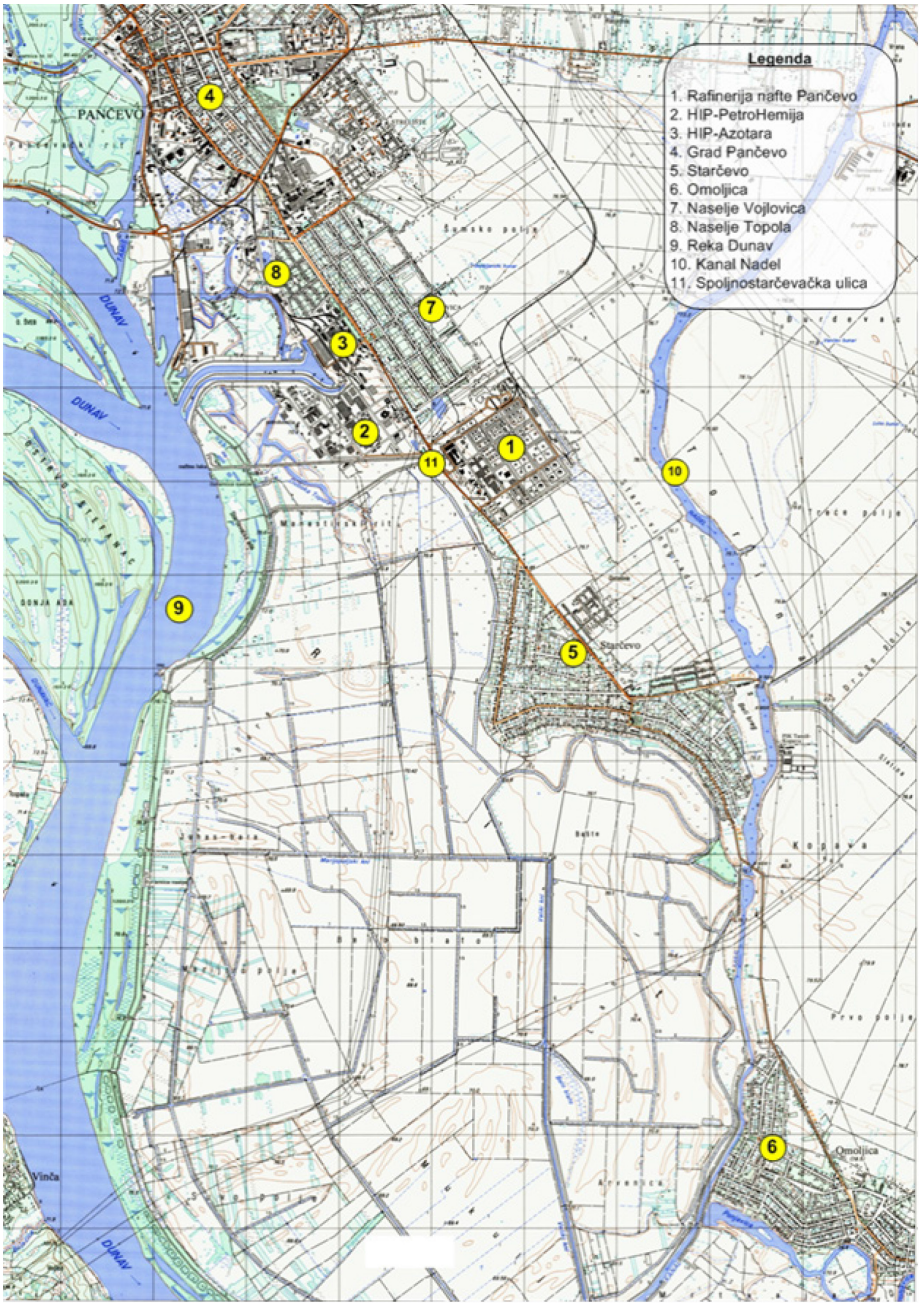

Figure 11: Southern Industrial Zone of City of Pančevo and nearby settlements

The key organizations identified in terms of resilience work besides the NIS Oil Refinery Pančevo and HIP Petrohemija, which are part of the industrial zone, are also the Sector for Emergency Situations of the city of Pančevo (municipal level), the Section for Preventive Protection of the Department for Emergency Situations in the City of Pančevo, within the Ministry of Interior (national level), as well as the Department for Accidents and Chemicals of the Ministry of Agriculture and Environmental Protection (national level).

Although each of the organizations, which were interviewed, has their own activities, their roles in terms of the critical infrastructure are interlinked; they are complementing and yet contrasting. On the one hand some of them are responsible for identifying risks, controlling and monitoring the identified risks, using all available and familiar tools, techniques, methods, best global practices for the prevention of accidents, organizing and securing readiness to accident response and accident situations, such as NIS Oil Refinery Pančevo and HIP Petrohemija.

Other organizations actively affect the critical infrastructure through the respective control in terms of compliance with legal provisions and thus contributing to the security such as Ministry of Agriculture and Environmental Protection and Ministry of Interior. The Ministry of Agriculture and Environmental Protection

grant the Decisions on the Documents Safety and Accident Protection Report and the Accident Protection Plan for Critical Infrastructure Companies and control them through inspection. Ministry of Interior also controls Critical Infrastructure Companies thought its own inspection. City of Pančevo, through its Headquarters for Emergency Situations, monitors security throughout the city and in the southern industrial zone where there is critical infrastructure.

The links among these organizations are conditioned by their roles: NIS Oil Refinery Pančevo and HIP Petrohemija belong to the southern industrial zone, City Administration of Pančevo is connected with above mentioned industrial entities and monitors and participates in the response to technical and technological accidents, together with the Department for Emergency Situations in the city of Pančevo, within the Ministry of Interior. Moreover, the abovementioned ministries through their bodies, i.e. the inspection, control the companies with critical infrastructure and get involved in the work of technical committees when approving the Safety and Accident Protection Report and the Accident Protection Plan for Critical Infrastructure Companies. Also see Table 20.

Table 20: Actor Analysis ECHO

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
Ministarstvo unutrašnjih poslova Republike Srbije, Uprava za vanredne situacije	Ministry for internal affairs of the Republic of Serbia, Directorate for emergency	National	Public	Operates protection and rescue activities in the area of civil defense, as well provides firefighter units.
Blok Prerada (NIS a.d. Novi Sad)	Block Refining (NIS j.s.c. Novi Sad)	Local	Private	Owner of refinery and responsible for emergency response activities for whole refinery.
NIS a.d. Novi Sad	NIS j.s.c. Novi Sad	National	Private	Owner of 5 blocks where one of the blocks is Block Refining. Providing all kinds of support in the event of emergency or crisis.
Ministarstvo zaštite životne sredine Republike Srbije	Ministry of environmental protection	National	Public	Defines legal requirements in the area of SEVESO. Provides approval on SEVESO documents and periodically control the implementation.
HIP Petrohemija	Petrochemical industry	Regional (sub-national)	Public	In the close vicinity located petrochemical facilities, as well SEVESO facility and can affect the safety of refinery in the event of accident. Cooperates from a business aspect and as well in the event of emergency situation.

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
				Have periodic joint drills.
Gradska uprava Grada Pančeva	Municipality of the City Pančevo	Local	Public	City Administration of Pančevo is connected with above mentioned industrial entities and monitors and participates in the response to technical and technological accidents.

4.5.2 Current status working with resilience and assessing resilience

In order to produce a comprehensive Vulnerability Assessments, the City of Pančevo has made an analysis of all natural disasters in the past 20 years, which was then used for the definition of preventive/corrective measures to prevent similar events in the future. Relevant departments of the City Administration regularly carry out analysis of the defined environmental pollution parameters – indicators (SO2, CO, NO2, H2S, and NOx). The obligation of a Seveso company is to deliver its Safety Report and Accident Protection Plan to the City Authorities who will do their own elaborations thereof and include those in the City's Vulnerability Assessment. City of Pančevo has the City Emergency Task Force which meets and negotiates accident response procedures in a case of an accident. Communication with critical infrastructure companies is daily because they submit to the city information on the activities conducted during the previous day, the daily reports of operations, overhaul plans, information about starting/stopping of a plant.

This suggests that state authorities operate strictly within frameworks of legislation - law, bylaw and legislation requirements enforcement and the industries such as NIS Oil refinery Pančevo and HIP Petrohemija should comply with these legal requirements, such as having Vulnerability Assessments, Safety Reports, Emergency Plans in place. Often in order to develop required Risk Assessment Study, organizations such as NIS Oil Refinery Pančevo and HIP Petrohemija engage consultants due to a lack of competency in the area.

Ministries who were involved in this research constantly work on improving the competences of their employees; they control the critical infrastructure companies, give approval to their documents, i.e. the Safety Report and Accident Protection Plan, regularly monitor the hazardous waste, correct their checklists used in inspection, as required, revise the inspection supervision risks, all in accordance with the estimated and observed situation at the location of a critical infrastructure company, whereby they also indirectly modify the desired and sustainable level of safety at the location through supervision and control mechanisms.

The critical infrastructure companies (NIS and HIP Petrohemija) apply the tools, techniques and methods for understanding of all the risks, analyzing the risks identified at similar facilities around the world, taking action to define accident prevention measures, prevent accidents, plan and implement measures for the rehabilitation after accidents, also bringing the infrastructure into the state before the accident.

4.5.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: terrorist threats, accidents. End users (NIS Oil Refinery and HIP Petrohemija) from industrial zone explained that their challenges, needs and requirements in assessing resilience today are the following:

- Employees avoiding to use existing risk assessment tools during preparation activities
- Developing the area specific risk register summarizing the results of all hazard identification and Risk Assessment studies
- Lack of an Comprehensive Emergency Plan on municipality level

Since continuous improvement of technology process and increasing the efficiency of the processes, these companies purchase safer and more modern equipment. Thus new risks appear because, in some cases, this new equipment has been mounted on the old one. That means there is a need to reassess risks and in

particular cases there is a have lack of adequate competencies of employees to do such assessments, otherwise it is not done in a comprehensive manner.

For that very reason, the challenge ahead recognized by the City of Pančevo is the continuous trend of urban settlements expansion towards areas with an estimated increased risk. Regardless of the fact that the risk assessment is done by NIS Oil Refinery Pančevo and HIP Petrohemija and submitted to the City of Pančevo, there is a trend approaching of the building new houses closer to the industrial zone i.e. Critical Infrastructure.

Additionally, possible terrorist threats are also an issue together with the necessary understanding that resilience assessment requires expertise, updated training, and acquisition of the latest know-how and the development of new Key Performance Indicators (KPI).

In terms of using indicators in assessing resilience end users explained, especially from industrial zone, that current indicators are not sufficient to give the overall and real picture about reliability of the production units, and do not cover all processes safety aspects. There are a lot of process safety indicators that are tracked without subsequent actions and some of them are not interconnected. All existing indicators should be evaluated and it should be decided which indicators need modification and which new indicators need to be further developed.

One of the permanent needs is the constant work to improve awareness of workers about the risks that surround them. Fast improvement in technological process requires constant improvement of their skills and knowledge. But the problem occurs within the older population of workers who adopt these changes slower than needed. Hence, there is a constant need for workshops with these workers to improve their understanding of hazards and risks surrounding their work and tools which are used for risk assessment. Human factor is an important resilience issue and should not be ignored. In that sense, the biggest challenge is to increase the awareness of the employees and change their behavior and attitude, especially when conducting high risky activities such as: work at highs, hot works, work in confided space, excavation, lifting operations and even the way of observation during normal operation in order to identify unsafe act and prevent undesired event.

Ministry of Agriculture and Environmental protection and Ministry of Interiors, on the other hand, recognize that an unfavorable staff age structure (older employees) may also have a negative impact when it comes to understanding the concept resilience and to do proper evaluation of all the risks concerning Critical Infrastructure Companies.

In addition, common activities aimed at the optimization of these public institutions result in the staff sizing down, as well as frequent reorganizations, have too been recognized as negative ongoing trends. This brings the public institutions into a position where they might not have enough skilled personnel required in order to adequately respond to the challenges inherent to such industrial zone in the city as is the southern industrial zone in the City of Pančevo.

4.5.4 Foreseen challenges, needs and requirements for assessing resilience

Although the risks have been recognized and evaluated at the level of the critical infrastructure, there is room for their development when it comes to resilience. Further work is needed to develop new, more comprehensive KPIs and Key Business Indicators (KBI), which would cover all aspects of resilience. Based on this, there is a need to develop Guidelines for the identification of appropriate smart resilience KPIs which are missing. These KPIs and KBIs should focus on asset integrity, process safety, environmental impact of production units and emergency response.

Furthermore, it is necessary to work on the education of employees (NIS Oil Refinery Pančevo and HIP Petrohemija) and to apply knowledge through team work of all stakeholders in the critical infrastructure organisations, including the competent city and state authorities, and improve their communication. Additional education of employees is needed in terms of improving their understanding of processes, risks, preparedness for reaction in case of emergency and impact and consequences of new technologies. Also, the introduction of user friendly tools for risk assessment needs to be easily operated at all organizational levels and easily manageable by all involved parties.

Likewise, the size of the critical infrastructure and the scope and severity of possible accidents require a broader awareness among urban inhabitants and the activation of civil protection. Lack of adequate

awareness and knowledge among the wider population, especially those residing close to the critical infrastructure or in its immediate vicinity, has been recognized by the City of Pančevo as potentially great risk in case of an accident. It was identified that awareness and improved training on the KPI system should be provided to all involved parties.

Linkage and exchange of experience with similar industrial zones in the world, motivating employees to accept changes in the way they work and adopt the latest know-how are also requirements which demand additional engagement. In table 21 below, the challenges, needs and requirements for the Pancevo industrial zone airport are summarized.

Table 21. Challenges, needs and requirements for the ECHO case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* terrorist threats, accidents 2. *Main challenges:* employees avoiding to use existing risk assessment tools during preparation activities, developing the area specific risk register, summarizing the results of all hazard identification and risk assessment studies, lack of a comprehensive emergency plan on municipality level	1. The continuous trend of urban settlements expansion towards areas with an estimated increased risk. 2. The size of the critical infrastructure and the scope and severity of possible accidents require a broader awareness among urban inhabitants and the activation of civil protection. 3. Public institutions might not have enough skilled personnel required in order to adequately respond to the challenges inherent to such industrial zone
Current needs and requirements	**Foreseen needs and requirements**
1. To improve awareness of workers about the risks that surrounds them. 2. Current indicators are not sufficient to give the overall and real picture about reliability of the production units, and do not cover all processes safety aspects. 3. There are a lot of process safety indicators that are tracked without subsequent actions and some of them are not interconnected.	1. To work on the education of employees improving their understanding of processes, risks, preparedness for reaction in case of emergency and impact and consequences of new technologies. 2. Knowledge through teamwork of all stakeholders in the critical infrastructure organisations, including the competent city and state authorities, and improve their communication. 3. User friendly tools for risk assessment need to be easily operated at all organizational levels and easily manageable by all involved parties. 4. Develop new, more comprehensive KPIs and Key Business Indicators (KBI), which would cover all aspects of resilience. 5. Develop Guidelines for the identification of appropriate smart resilience KPIs which are missing.

4.5.5 Discussion and conclusion

All participants in the study were aware of the existence of major risks recognized in the legal requirements - Vulnerability assessment, Safety Report and Emergency Plan such as leakage of flammable gases and their subsequent burning and explosion, as well as dangers that could cause poisoning people due to the exposure of chemicals. Significant efforts were made for those to be recognized, controlled and reduced to a minimum level. These processes involved a lot of people working on them constantly, analyzing how to improve the business to be safer, to be more reliable. Many workshops have been developed to present to workers threats and risks of their jobs. A lot of financial resources have been invested to improve safety in the Critical Infrastructure Companies as well.

However, the communication and coordination seems to be insufficient among all stakeholders that contribute to ensure resilience, where the level of understanding of resilience also varies between organizations. On one hand, there are critical infrastructure companies that are constantly working on increasing their awareness and reduce their risks to ensure that their systems are as resilient as possible, even though they themselves recognize that there is room for improvement. On the other hand, during interviews it was concluded that municipal and state officials (municipality of the City of Pančevo and interviewed Ministries) do not monitor the resilience enough which raises the question if they actually have the capacity to respond to the challenges of critical infrastructures, as they act strictly within the framework of legislation.

To sum all above mentioned up, the most important findings in terms of assessing resilience are:

- Public entities have much more understanding about risks and hazards related to natural disasters rather than on risks related to production in the industrial zone
- A municipal Emergency Plan for the Industrial zone do not exist
- Employees do not regularly use existing risk assessment tools during preparatory activities
- The risk registries for the production sites do not summarize the results of all hazard identification and risk assessment studies
- There is a pile of miscellaneous indicators which are not interconnected

Development of new indicators, simple and understandable would be of great importance for improving the resilience of the southern industrial zone in the City of Pančevo. Besides of increasing awareness, this will help to better understand threats and risks that are identified through existing required safety documents such as Vulnerability assessment, Safety Report and Emergency Plan, subsequently this will lead to improving of current approach to resilience practice. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the ECHO case can be summarized in table 22 below. In this case study, the concept of resilience can perhaps be used as a means to highlight the need for a comprehensive approach to the risks in the whole industrial district, addressing the interconnectedness of the various industries and the need for a comprehensive data management approach.

Table 22. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the ECHO case.

Dimensions of resilience	Examples from ECHO
System/physical: Technical aspects, physical/technical networks, interconnectedness	The continuous trend of urban settlements expansion towards areas with an estimated increased risk.
Information/data: Technical systems dealing with information/data	Current indicators are not sufficient to give the overall and real picture about reliability of the production units, and do not cover all processes safety aspects. developing the area specific risk register,
Organizational/business: Business-related, financial and HR aspects and organizational networks	To work on the education of employees improving their understanding of processes, risks, preparedness for reaction in case of emergency and impact and consequences of new technologies. User friendly tools for risk assessment need to be easily operated at all organizational levels and easily manageable by all involved parties.
Societal/political: The broader societal/social context, indirect stakeholders	Public institutions might not have enough skilled personnel required in order to adequately respond to the challenges inherent to such industrial zone The size of the critical infrastructure and the scope and severity of possible accidents require a broader awareness among urban inhabitants and the activation of civil protection.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Need to train and motivate personnel, both workers (which generally have low risk awareness) and personnel in the ministries (which may be inadequately trained). Develop new, more comprehensive KPIs and Key Business Indicators (KBI), which would cover all aspects of resilience.

4.6 FOXTROT: Drinking water supply in Sweden

4.6.1 Introduction

Drinking water is often called our most important food. Sweden has for long enjoyed top quality drinking water straight from the tap. With an average daily household consumption of 160 L/person, drinking water is used for plenty of other purposes than just drinking, and the water quality is taken for granted by the majority of the Swedish population. There is an overall good state of the art relative to other critical infrastructure and other European countries:

- Overall plenty of supply
- Overall good quality
- Good knowledge of risks
- Robust system for monitoring vulnerabilities and risks

In recent years, however, a number of threats towards the Swedish drinking water, now and in the future, have appeared on the horizon. These threats include an increasing water shortage in some areas, climate change, which can increase the risks of pathogens in the water, and unexpected events such as heavy rainfall that contaminate the sources for drinking water.

A picture of the drinking water supply cycle is presented in Figure 12. The water is distributed to the consumers from pressurized pipes either from a water tower or from low level water reservoirs. Water is produced in ground water or surface water plants. Half of the Swedish drinking water is produced from large surface water plants, while the majority of the 1,750 waterworks in Sweden are smaller ground water plants. Among the ground water plants, there are also plants using artificial ground water for its production, where surface water is pumped into for example an esker to increase the capacity of the aquifer.

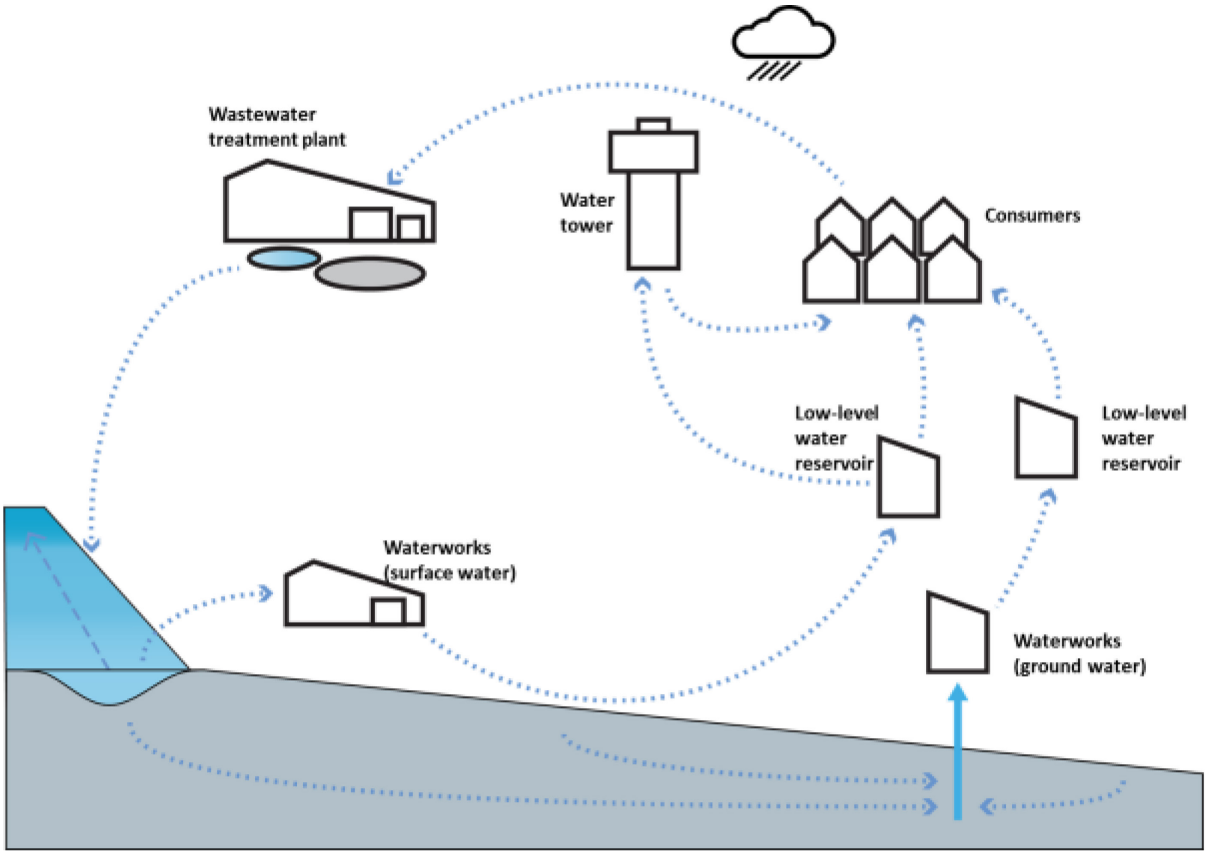

Figure 12: The drinking water supply cycle.

The increasing threats towards the Swedish drinking water have been increasingly acknowledged, and resilience of drinking water production are already on the agendas of the Swedish National Food Agency (SLV), The Swedish Civil Contingencies Agency (MSB), the Swedish Water and Wastewater Association

(SWWA), the municipalities responsible for supervision of the water works as well as the separate utilities, i.e. the drinking water producers. SLV is responsible for the national coordination regarding drinking water in Sweden. MSB is responsible for supporting and overseeing municipal and regional government activities with respect to crisis and emergency management. SWWA represents the interests of the municipalities in the whole field of municipal water and wastewater. More information on this can be found in project report D.1.2 "Analysis of existing assessment resilience approaches, indicators and data sources" [79]. Also see Table 23.

This chapter builds on a summary of interviews made with experts at MSB, SLV, Norrvatten and Stockholm Vatten combined with material from [79] and literature on the topic. Norrvatten and Stockholm Vatten own and operate drinking water plants and drinking water networks in the Stockholm region. Stockholm Vatten is also responsible for wastewater networks, wastewater treatment and waste management.

Table 23: Actor Analysis FOXTROT

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
Myndigheten för samhällsskydd och beredskap	Swedish Civil Contingencies Agency	National	Public	Responsible for issues concerning civil protection, public safety, emergency management and civil defense. Responsibility refers to measures taken before, during and after an emergency or crisis.
Livsmedelsverket	National Food Agency	National	Public	Responsible for the national coordination of drinking water issues in Sweden, with special focus on adaptation to climate change and crisis and emergency planning regarding drinking water supply. Have set up special a support function (VAKA) for serious crises/disturbances in the supply of drinking water.
Länsstyrelsen (e.g. Stockholms läns länstyrelse)	County Administrative Board (e.g. of Stockholm)	Regional (sub-national)	Public	Responsible authority on regional level, coordinating local (e.g municipalities) and national levels. Supports municipalities and other actors, responsible for emergency preparedness, with planning, risk and vulnerability assessments as well as education and training. Supervisor of crisis management and emergency response work of the municipalities.
Kommuner (e.g. Stockholm stad)	Municipalities (e.g. City of Stockholm)	Local	Public	The municipalities hold the main responsibility for securing drinking water supply to their citizens, including risk management and emergency preparedness. The municipalities are responsible, as far as possible,

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
				to manage their own risks. In case of more extreme events, regional and national support is provided.
Drickvattenproducenter och distrubutörer (e.g. Stockholm Vatten, Norrvatten)	Drinking water producers and distributors (e.g. Stockholm Water, Northern Water Board)	Local	Public/ Private	The drinking water producers and distributors, always under the responsibility of the municipality, do not have any designated responsibility for emergency preparedness in legislation, but are assigned to take necessary measures if outgoing drinking water do not meet health and safety requirements as well as maintain a reasonable level of security. Drinking water producers and distributors can be either under municipality management, management of municipality associations or municipality companies, or by private operators (delegated by the municipality).
Svenskt Vatten	The Swedish Water & Wastewater Association	National	Other	Assist drinking water producers in technical, economic and administrative issues and to represent the interests of the municipalities in the whole field of municipal water and wastewater in negotiations with authorities and other organizations on regulations.

4.6.2 Current status working with resilience and assessing resilience

On a national level, SLV is working with several types of educational activities in relation to crisis management. SLV has produced several handbooks on crisis and emergency management as well as risk and vulnerability analysis. Other examples of initiatives include a web service for management of accidents at water source as well as coordination of a working group around crisis management within the National Drinking Water Network hosted by SLV.

During a crisis or disaster, support and assistance can be provided from VAKA, the National Water Disaster Group. VAKA provides support to municipalities and regions affected or likely to be affected by problems with the drinking water supply and is organized by SLV. The group constitutes of professionals from drinking water distribution, environmental protection and emergency services nationwide with previous experiences of crises and disasters. VAKA can be contracted by drinking water producers, environmental and health departments, emergency services, and municipal governments and their services are free of charge. County administrations and national authorities can also ask for assistance. VAKA has access to storage of emergency water supply.

MSB requests that operators of drinking water plants produce risk and vulnerability analyses. The municipalities are responsible for those, and the County administration summarizes the local situation to MSB. The only requirement are that an analysis is made, there is no follow-up on the quality of the analysis.

With regard to cyber security, MSB provides knowledge and support to operators, for instance via a simulator for cyber safety in industrial control systems.

The municipal company Norrvatten has created a safety handbook for water works together with SLV, which they also follow in their continuous work with risk and vulnerability assessments. Norrvatten has long term development goals related to resilience: (1) Sustainable capacity – to be able to produce a definite amount of water, no matter what happens with the water source, (2) Redundancy – to be able to provide for water from different water sources and (3) To be able to cope with future changes in raw water quality. To reduce the risk of cyber-attacks, the office network and the control network are not interconnected to avoid Internet access to the control system. Swedish Defense Research Agency (FOI) has performed real attacks against their system in order for Norrvatten to be able to improve their IT security against external threats. They have also improved the physical protection at the plants to reduce the risk of un-wanted visitors at the facilities.

Stockholm Vatten is working towards eliminating all delivery interruptions causing delivery failure. Stockholm Vatten is working proactively with sustainability of the drinking water supply by engaging early on in the City's planning process to include water issues in an early stage. In certain areas, risk analyses are made. Similar to Norrvatten, redundancy is a key factor in Stockholm Vatten's strategy both in drinking water production and distribution. With regard to microbial risks, microbial risk assessments are made in order to not only detect but also assess risks both proactively to reduce risks but also as a support in decision making during for example contamination of the water source, Lake Mälaren. Stockholm Vatten also performs long-term trend analyses to learn more about risks related to climate change. Risk analyses are also made related to sabotage at plants or in reservoirs. Similar to Norrvatten, the office and control networks are separated and the IT systems are tested to see how secure they are.

The concept of resilience is not widely used within the Swedish drinking water sector. The interviewees agree that the concept is highly relevant for drinking water supply, but the concept is not well established. Other related concepts that were mentioned during the interviews were risk management, sustainability, robustness, reduced vulnerability and availability. Several of the actors mentioned that they do work with resilience, even though they do not use that exact word. Resilience was also referred to as a "buzzword" and a concept that people are not always comfortable using.

MSB was the actor with the most in-depth knowledge of the concept of resilience. The interviewee described resilience as being about reducing disturbances and being able to come back to the same position after a disturbance. Compared to striving for robustness where the key is to withstand a disturbance, resilience is, according to MSB, a wider concept where one realizes that it is not possible to plan for all possible risks. MSB also uses continuity management in conjunction with resilience.

SWWA has developed the VASS Sustainability Index and the VASS Drinking water performance indicators which are a form of self-assessments where there are several questions related to resilience (see further Table 17 in [79]). The VASS Sustainability Index is most relevant for the long term work with sustainability of the water and wastewater sector on a municipal level, both for the municipal administration and for local politicians. Distributors and suppliers, such as Norrvatten and Stockholm Vatten, should comply with the requirements in the VASS Sustainability Index, but are less likely to use it as a tool for improvement. This emerged during a discussion at a seminar about VASS Sustainability Index in 2016.

Norrvatten works to a limited degree with the VASS indicators mentioned above. According to them, the VASS statistics is better suited for working with the distribution network than with the production facility. Norrvatten has together with its counterpart in southern Sweden, Sydvatten, developed their own Sustainability index presented in rose diagrams.

Stockholm Vatten is not working with specific indicators related to resilience. Classical risk matrices are used, but not single indicators. Centrally, Stockholm Vatten is working to calculate their VASS Sustainability Index for the whole organization. When asked if this is a useful method for them, the answer was that there is a risk when using very broad indicators that certain risks are not well covered. For such a large organization as Stockholm Vatten, it is also challenging to report data in a consistent way to form the Index. Stockholm Vatten has participated with data to VASS Drinking water, but is not using the performance indicators in their own work with sustainability.

4.6.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: cyber-attacks, accidents in raw water supply, microbial contamination. The drinking water sector has not been assessed for its resilience in a unified framework. The reason why no such assessment has been made on the whole infrastructure could – according to the interviewees – be that the concept is abstract, that it is a very challenging task to undertake, and that there is a lack of relevant indicators and metrics. The challenges come from the very broad area of knowledge that an assessment of resilience of the drinking water sector would have to encompass. An assessment need to cover both where to place the water source or emergency water supply, the quality of the water source, drinking water production and distribution. If the question is brought up to a regional level, it becomes even more complex. Another possible explanation is that citizens have grown to take safe drinking water supply for granted in Sweden. Since the citizens do not push for an assessment of resilience, the politicians in the municipalities are not challenged to take such an initiative.

Probably the best assessment made in relation to resilience of the whole sector was the final report by the Drinking Water Inquiry, published in 2016 [67] with the objective to identify current and potential challenges for a safe drinking water supply in the country, in the short and long term, and, if necessary, propose appropriate measures. There is also the Climate and Sustainability Inquiry [66]. Some key suggestions from [67] related to resilience are that (1) regional water supply plans should be compulsory for all Counties in the future, (2) the County administration should decide on Water Protection Areas, and that Water Protection Areas should be compulsory for municipalities, (3) monitoring of water sources should be improved, (4) the water treatment processes should be improved, (5) the public control should be adapted to the needs of the water supply sector and (6) the emergency contingency should be strengthened.

MSB is regularly performing Risk and Capability Assessments. In the assessment published 2016 [71], they conclude that the municipalities lack the ability to maintain the drinking water supply through for example emergency water supply. The assessment also noted the age of the infrastructure and that economic resources are not always available to secure the renewal rate and maintenance of the infrastructure, which is a growing problem.

According to SLV as well as the Drinking Water Inquiry there is a lack of monitoring of threats to the drinking water supply. There is also a lack of objective data about assessment of resilience in the sector as well as of continuous monitoring.

It appears that the sector has struggled for some time to produce indicators for assessment of sustainability in the drinking water sector. One reason to this, suggested by Norrvatten, is that the sector is fragmented with both large and small municipalities. Hence there is a challenge to create a common ground since there are many different opinions and there is also the challenge of producing data and statistics of good quality.

4.6.4 Foreseen challenges, needs and requirements for assessing resilience

The main future challenges for the drinking water sector foreseen by the interviewees in the long term are (1) Quality and availability of water (affected by climate change), (2) larger demand on the infrastructure (due to urbanization together and an increasing population) and (3) risk of microbial outbreaks (lack of barriers in the drinking water plants). Short term disturbances mentioned are leaks on the distribution network and break downs and unexpected events, such as fires, at the water works.

When asked about risk of terror attacks or cyber-attacks, the interviewees agree there are such risks. Stockholm Vatten mentions an increased risk of sabotage.

The interviewees agree that the production facilities are becoming “smarter” in terms of more advanced treatment steps and more monitoring and control. This may increase the vulnerability of the sector, since more technically advanced plants may lead to (1) a risk of lack of competence since operation will be dependent on a few numbers of people who know the “smart” systems and (2) a risk that the engineering expertise that took us to where we are today is forgotten. There is a large potential to increase automation at water works in Sweden, but with more automation there is an increased exposure if there is not expertise to handle an event caused by system failure. There is also a risk that information will be abundant about the situation at the plants, but with little gain if there is “information over-load”, i.e. too much information to handle.

Norrvatten argues that perhaps new indicators are not needed in the future. The overall risk may be the same, but the cause of the risk is gradually changed. If water works become smarter, the plants will operate better but more technology is also a risk, as described above.

Stockholm Vatten believes that assessment of resilience will become more important in the future to be able to make wise decisions, given that drinking water production faces many challenges.

Introducing new concepts related to risk and vulnerability – such as resilience – can be confusing for many people working in the sector. People ask "what good comes out of this?" and there is a need to communicate new concepts in a good way.

Another need, brought up by SLV, is about widening the definition of drinking water supply-related risks. Drinking water is not only about providing safe drinking water to the public. Disturbances in the supply of drinking water may have severe impacts on local communities. There are many companies who depend on safe drinking water, e.g. farmers.

SLV also mentioned the need to work with resilience of the drinking water supply to citizens not connected to the municipal distribution system. About 10 % of the population (1.2 million people) receive their drinking water from a local well or source where the property owners are responsible for the quality of the drinking water. It is not clear at the moment who works with resilience in these smaller distribution systems. In table 24 below, the challenges, needs and requirements for the Swedish drinking water system are summarized.

Table 24. Challenges, needs and requirements for the FOXTROT case.

Current challenges	**Foreseen challenges**
1. *Most relevant threats:* cyber-attacks, accidents in raw water supply, microbial contamination 2. *Main challenges:* Risk of microbial outbreaks (lack of barriers in the drinking water plants), leaks on the distribution network and break downs and unexpected events, such as fires, at the water works.	1. Quality and availability of water (affected by climate change). 2. Larger demand on the infrastructure (due to urbanization together and an increasing population). 3. Production facilities are becoming "smarter" in terms of more advanced treatment steps and more monitoring and control. This may increase the vulnerability of the sector, since more technically advanced plants may lead to (1) a risk of lack of competence since operation will be dependent on a few numbers of people who know the "smart" systems and (2) a risk that the engineering expertise that took us to where we are today is forgotten.
Current needs and requirements	**Foreseen needs and requirements**
1. Engaging early on in the City's planning process to include water issues in an early stage. 2. Microbial risk assessments to be made in order to detect and assess risks both proactively to reduce risks but also as a support in decision making during for example contamination of the water source. 3. Risk analyses need to be made related to sabotage at plants or in reservoirs. 4. The office and control networks need to be separated and the IT systems are tested to see how secure they are.	1. Regional water supply plans should be compulsory for all Counties in the future 2. County administrations should decide on Water Protection Areas, and Water Protection Areas should be compulsory for municipalities. 3. Monitoring of water sources should be improved. 4. Water treatment processes should be improved. 5. Public control should be adapted to the needs of the water supply sector. 6. Emergency contingency should be strengthened.

4.6.5 Discussion and conclusion

There is a common understanding of what the challenges for drinking water supply is in Sweden. Availability and quality of the drinking water together with microbial risks are threats that the sector works with today and that will be even more important in the future.

Resilience is not a well-established concept among most of the interviewees, and several of the interviewees refer to resilience as a "buzz-word". Nevertheless, the concept is highly relevant and encompasses a wider perspective than many of the other concepts that are related to resilience, such as robustness and risk management.

The drinking water supply in Sweden has not been assessed for its resilience; the closest work on the topic is the Drinking Water Inquiry from 2016 which, among many other things, relate to issues associated with resilience.

It seems that indicators – though mentioned as important – do not play a key role in assessing resilience of drinking water supply in Sweden today. Classical risk management is more common. There is a challenge to agree on what metrics to use in the sector. Different actors have different needs with regard to indicators, and indices that are a combination of many different metrics may not be precise enough for each specific requirement. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the FOXTROT case can be summarized in table 25 below.

Table 25. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, visualizing and assessing resilience for the FOXTROT case.

Dimensions of resilience	Examples from FOXTROT
System/physical: Technical aspects, physical/technical networks, interconnectedness	Larger demand on the infrastructure (due to urbanization together with an increasing population). Quality and availability of water (affected by climate change).
Information/data: Technical systems dealing with information/data	Production facilities are becoming "smarter" in terms of more advanced treatment steps and more monitoring and control. This may increase the vulnerability of the sector, since more technically advanced plants may lead to (1) a risk of lack of competence since operation will be dependent on a few numbers of people who know the "smart" systems and (2) a risk that the engineering expertise that took us to where we are today is forgotten. The office and control networks are separated and the IT systems are tested to see how secure they are.
Organizational/business: Business-related, financial and HR aspects and organizational networks	Engaging early on in the City's planning process to include water issues in an early stage. Emergency contingency should be strengthened.
Societal/political: The broader societal/social context, indirect stakeholders	Examine the impact of threats on different stakeholders, for example how farmers would be affected by disturbances in the supply of drinking water.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Risk analyses are also made related to sabotage at plants or in reservoirs. Microbial risk assessments are made in order to detect and assess risks both proactively to reduce risks but also as a support in decision making during for example contamination of the water source.

For this case study, the concept of resilience was not necessarily useful, according to the interviewees, although it might be in the future. Data security was considered a major issue, whereas organizational complexity was considered an issue of regulation and variation among end-users with very different realities and resources.

4.7 GOLF: Flooding events in the City of Cork

4.7.1 Introduction

Cork City, located at the head of a tidal estuary and at the downstream end of a large river catchment is prone to both tidal and fluvial flooding. Cork City is the second largest city of the Irish Republic with a population of 125,622 as per the 2016 census. Flood risk is assessed on the likely probability of varying degrees of severity occurring. This probability is designated as the % probability of the event in any one year i.e. % annual exceedance (% AEP). In the recent past, notable flood events have occurred in August 1986, November 2000, November 2002, October 2004 and December 2006 and most recently November 2009 and October 2014. Tidal flooding is more common than fluvial, but fluvial flooding can often be more serious and costly. A serious flood such as in November 2009 can affect the water supply to over 50,000 households and

businesses. Disruption to public transport, hospitals, energy supply and local government services can also occur.

Figure 13: Aerial view of flooded riverside area in Cork City (CCC)

Cork City Council will be the lead flood response agency for any flood emergency within Cork City. Assistance will be provided by other response organizations including the Irish Police Force, Health Services Executive, Civil Defense, Fire & Defense Services, Voluntary Emergency Services, Cork County Council, and Electricity Supply Board. See also Table 26.

Table 26: Actor Analysis GOLF

Name of organization (original language)	Level	Type	Role/responsibility in case study*
National Directorate for Fire and Emergency Planning / Office of Emergency Planning	National	Public	General responsibility for disaster management (including firefighters) in the country. In case of a flood, carries out national emergency coordination.
The Office of Public Works	National	Public	The OPW is the leading agency for flood risk management in Ireland, coordinating and implementing Government policy on the management of flood risk in Ireland, in order to minimize the impacts of flooding through sustainable planning.
Cork City Council	Local	Public	Cork City Council is the lead flood response agency for any flood emergency within Cork City. Cork City Council is also owner and/or operator of critical infrastructure (e.g. drainage infrastructure, Water and waste water infrastructure) as well as regulator of critical infrastructures. Furthermore Cork City Council will operate future planned flood defenses (owned by OPW).
Inter-Agency Emergency Management Office - Region South	Regional	Public	Provides support on a full time basis to the participating agencies in the consideration and implementation of their responsibilities in planning and preparing for their response to Major Emergencies in the Cork & Kerry Area.

Name of organization (original language)	Level	Type	Role/responsibility in case study*
An Garda Síochána – Irish Police Force	National	Public	The national police force, in case of flooding responsible for e.g. coordinate arrangements for the evacuation of persons from affected areas, issue of public warnings in the initial phases of the emergency, management of traffic access and egress from affected areas, identification and management of emergency transportation routes, documentation of displaced persons, facilitating requests for assistance from the Defense Force and provision of air support to undertake aerial reconnaissance of the flood affected areas.
Health Services Executive	National	Public	Responsible for providing health care in general and in case of flooding, including e.g. provision of First Aid & Medical Facilities to affected persons and responders, coordinating arrangements for the evacuation of vulnerable persons from affected areas, advise on public health warning/ advisory notice as well as provision of Psychosocial support to affected persons where requested.
Civil Defense	National/ Local	Public	A volunteer-based emergency response organization, supporting frontline emergency services in case of flooding. This includes e.g. assisting in evacuation, supporting the Local Authority with the provision of short term welfare services to members of the public and supporting the Health Services Executive in providing first aid personnel and patient transport.
Fire & Defense Services	National	Public	In case of flooding its responsibility includes to provide Aid to the Civil Authorities upon request, assist in evacuation, and assist in transport from affected areas, assist local authorities in flood defense operations by providing manpower and equipment and distribute essential aid and staff to key areas.
Cork County Council	Regional	Public	IN case of flooding, liaise with Cork City Council on flood issue and advice on potential upstream threats in a fluvial event.
Electricity Supply Board, Irish Water, Irish Rail, Bus Eireann, Transport Infrastructure Ireland,	National/ Local	Public/ private	Owners or operators of critical infrastructure in Cork that can potentially be affected by flooding (Water and Waste water infrastructure, public transport, energy supply infrastructure, drainage infrastructure). Responsible for ensuring security of supply and service to the citizens in case of flooding. The Electricity Supply Board is further advisory organization on discharge rates from the Inniscarra Dam and issue with electricity supply and broken supply lines.

4.7.2 Current status working with resilience and assessing resilience

Cork City Council has identified the "risk of flooding, both fluvial and tidal, of the river Lee or of waterways due to blockages etc." as one of its Corporate Risks. The Council strives to ensure the resilience of the City to flood events is maintained by:

- Implementing a Flood Protection Strategy based on Office of Public Works (OPW) Lee Catchment Flood Risk and Management Study.
- Developing Flood forecasting and warning system with the OPW and others as appropriate.
- Implementing a Flood Defense Strategy.
- Regularly reviewing the Emergency Response Plans.
- Maintaining the Main Drainage Scheme to ensure no pollution and an acceptable river water quality.

4.7.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: flooding due to climate change which cause rising sea levels and more frequent and more severe rainfall events and will significantly increase the risk of flooding and coastal erosion. Under the Flood Risk Directive 2007/60/EC, Cork City Council has a responsibility to assess and manage flood risks through the development of flood risk management plans. In response, The Lee Catchment Flood Risk Assessment and Management Study, (Lee CFRAMS) was undertaken by the Office of Public Works, Cork City Council and Cork County Council. Lee CFRAMS was incorporated into the City Development Plan process as it informed the Strategic Environmental Assessment and Strategic Flood Risk Assessment (the draft plan).

National policy in respect of flood risk areas is set out in The Planning System and Flood Risk Management: Guidelines for Planning Authorities (2009). The Guidelines advocate the Sequential approach, namely, to avoid development in areas at risk of flooding; and if this is not possible, to consider substituting the land-use to one less vulnerable to flooding; and only where avoidance and substitution is not possible to consider mitigation measures and management of the flood risks.

Proposals for vulnerable types of development in areas of moderate and high flood risk are examined against criteria set out in the Justification Test, to demonstrate overriding strategic planning need, and that the flood risk can be adequately managed without causing adverse impacts elsewhere.

Early identification of a potential flooding event is critical and Cork City Council currently achieves this by:

- Monitoring Met Eireann weather alerts and reports received from other sources on current weather conditions.
- Analyzing any reports received from staff monitoring Flood Early Warning Systems.
- Determining the potential effect of spilling notifications from the ESB Inniscarra Dam on Cork City as the rate of discharge directly affects the height of the river Lee.
- Analyzing data on storm surge forecasts from the OPW.
- Activating the Flood Emergency Plan and alert other response organizations as required.
- Notifying the Crisis Management Team if the Flood Emergency Response Plan is activated.

This process is largely manual and subjective and relies on the knowledge and experience of staff.

Communications is a challenge and the City Council has improved its ability to communicate with the public via a color coded (Red/Orange/Yellow/Green) system for flood threat. Cork City also encourages the public to register on an alert system www.corkcitynow.ie . This allows the public and business to prepare their own flood defenses in a timely manner.

4.7.4 Foreseen challenges, needs and requirements for assessing resilience

A €50 Million project to improve flood protection in the River Lee catchment area is in place from the Office of Public Works (OPW). The project will concentrate on engineering works from the Inniscarra dam and along the 10 miles of river leading into the city. Extensive repair and rising of the city key walls will greatly reduce the risk of flooding. This project will require extensive engineering works, road closures and public consultation and communications, but will greatly increase the city's resilience to flooding.

The council has identified the need for more sophisticated modelling and prediction analytics to assist in determining the likelihood and effect of floods within the city. A Tidal Flood Event Advisory System is highly desirable and the council is working with EMC² to develop a system that will receive inputs from sensors in

the harbor and weather and surge data sources to predict flood events. This would then interact with a communication system to notify key stakeholders and the public of the potential threats.

Previous flooding events have highlighted the need for systems to manage incident report and service requests. Applications with mapping front ends are currently being developed which can be leveraged to manage these needs in a future flood event.

To minimize flood risk, the City Council has adopted a two track approach in the City Development Plan;

(i) to avoid development in floodplains, wetlands and coastal areas prone to flooding and rezoned 12 hectares of suburban 'Greenfield' development land to 'water compatible' uses such as public open space and landscape preservation zones; and

(ii) to invest in infrastructural works such as flood protection and storm water attenuation. The city's historic core will be protected from flood risk by new and improved defense structures, as part of the OPW's Draft Lower Lee Relief Scheme. In table 27 below, the challenges, needs and requirements for the Cork City flooding case are summarized.

Table 27. Challenges, needs and requirements for the GOLF case.

Current challenges	**Foreseen challenges**
1. *Most relevant threats:* flooding due to climate change which cause rising sea levels and more frequent and more severe rainfall events and will significantly increase the risk of flooding and coastal erosion. 2. *Main challenges:* Implementing a flood protection strategy, developing flood forecasting and warning system, implementing a flood defense strategy, regularly reviewing the emergency response plans, maintaining the main drainage scheme to ensure no pollution and an acceptable river water quality.	1. More sophisticated modelling and prediction analytics to assist in determining the likelihood and effect of floods within the city. 2. The need for systems to manage incident report and service requests.
Current needs and requirements	**Foreseen needs and requirements**
1. Monitor Met Eireann weather alerts and reports received from other sources on current weather conditions. 2. Analyze any reports received from staff monitoring Flood Early Warning Systems. 3. Determining the potential effect of spilling notifications from the ESB Inniscarra Dam on Cork City as the rate of discharge directly affects the height of the river Lee. 4. Analyze data on storm surge forecasts from the OPW. 5. Activating the Flood Emergency Plan and alert other response organizations as required. 6. Notifying the Crisis Management Team if the Flood Emergency Response Plan is activated.	1. To avoid development in floodplains, wetlands and coastal areas prone to flooding and rezoned 12 hectares of suburban 'Greenfield' development land to 'water compatible' uses such as public open space and landscape preservation zones 2. To invest in infrastructural works such as flood protection and storm water attenuation. The city's historic core will be protected from flood risk by new and improved defense structures, as part of the OPW's Draft Lower Lee Relief Scheme.

4.7.5 Discussion and conclusion

Climate change will result in rising sea levels and more frequent and more severe rainfall events and will significantly increase the risk of flooding and coastal erosion. Flooding is a real and regular threat in Cork City and changing weather patterns mean they are more likely in the future [4] The gathering of indicators and assessing them is currently largely a manual process and relies on knowledge built up through past experience. The use of data analytics and modelling from an increased number of data sources will enhance the ability of the City to identify flood event, their severity and areas of impact. The flood defense plans for

the river Lee will mitigate the effect of floods in the city. A major emergency plan exists within the city and determines the lead and key stakeholders depending on the type of emergency. Should a serious flood occur Cork City Council will be the lead agency and operations to increase the resilience and respond/recovery of the City will be put into action in conjunction with other key stakeholders. Improved and integrated system around transportation and foot fall within the city would help in managing the evacuation of areas in risk of flooding.

Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the GOLF case can be summarized in table 28 below.

Table 28. Summarizing the most important issues for which the Smart Resilience methodology and database can be used for identifying, vizualizing and assessing resilience for the GOLF case.

Dimensions of resilience	Examples from GOLF
System/physical: Technical aspects, physical/technical networks, interconnectedness	To avoid development in floodplains, wetlands and coastal areas prone to flooding, the City has rezoned 12 hectares of suburban 'Greenfield' development land to 'water compatible' uses such as public open space and landscape preservation zones. To invest in infrastructural works such as flood protection and storm water attenuation.
Information/data: Technical systems dealing with information/data	More sophisticated modelling and prediction analytics to assist in determining the likelihood and effect of floods within the city.
Organizational/business: Business-related, financial and HR aspects and organizational networks	The need for systems to manage incident report and service requests. Implementing a flood protection strategy. Analyzing any reports received from staff monitoring Flood Early Warning Systems. Activating the Flood Emergency Plan and alert other response organizations as required.
Societal/political: The broader societal/social context, indirect stakeholders	The public needs to be educated in terms of flooding. An effective cooperation with other actors such as the county council, the Office of Public Works and the police
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Determining the potential effect of spilling notifications from the ESB Inniscarra Dam on Cork City as the rate of discharge directly affects the height of the river Lee.

The major concerns in this case study seems to stem from the need for improved modeling (data management) and coordination of various stakeholders and the public (organizational complexity), whereas the concept of resilience is not a major issue.

4.8 HOTEL: Energy supply infrastructure in Helsinki

4.8.1 Introduction

Energy generation and consumption ideally take place in the same area, i.e. generation within the city or in the vicinity, next to the consumers in households and peri-urban industry. However, concentrating the energy supply infrastructure in the same area puts more emphasis on managing risks and responding to disruptions as risks for ripple and cascading effects are higher when critical infrastructures are closer together.

The Energy supply infrastructure in Helsinki, the capital of Finland, includes the production and distribution of three main products within the same area: district heating, district cooling and electricity.

The district heating production in Helsinki covers the vast majority of city's heating needs and the district heating distribution network is, with its 1350 km of pipelines, the largest one in the world. The district heating is mainly produced in three locations within Helsinki city (Vuosaari, Hanasaari and Salmisaari) by combined heat and power (CHP) generation. The heat produced with CHP generation serves 90% of the

needs for heating the city and its domestic hot water in the spring, summer and autumn. When the consumption of heat and domestic hot water is high or, in practice, during very cold weather, eleven heating plants in different parts the city provide the additional heating needed. The heating plants also safeguard local heat supply in exceptional situations, for example, when the CHP plants are experiencing problems or the district heating pipes in some part of Helsinki are broken. As heat consumption in the city of Helsinki is not steady throughout the day, heat produced during the night is stored in large underground water tank accumulators at two of the CHP power plants (Vuosaari and Salmisaari). When more heat is needed (e.g. in the mornings), the heat is discharged from the accumulators [29].

District cooling is a relatively new product in the Energy supply infrastructure in Helsinki and is produced with trigeneration, i.e. in the same process for heating, cooling and and electricity. The production of district cooling takes place at the Salmisaari power plant and almost 80 % of district cooling production is based on energy that would otherwise be unutilized. The district cooling production and distribution is however still small, with around 100 customers and 70km of distribution network. Cooling energy is also stored at night in underground energy storage facilities and, correspondingly, can be utilized during the day. The first underground cooling storage facility was commissioned in 2012 with a second, larger, underground storage facility under development [29].

Electricity is produced partly in the CHP power plants and solar power plants within Helsinki but also includes production from power plants, including nuclear, hydro and wind power outside of Helsinki. Electricity is also imported from other countries, e.g. Sweden. The distribution network consists of many kilometers of cables above- and underground [29].

The majority of the energy produced and distributed in Helsinki comes from natural gas and coal. As the main fuel, natural gas accounts for over half of the energy production in Helsinki while coal accounts for about one-third. The highlighted benefits of coal as a fuel include its good availability, stable price and easy storing for exceptional situations [29]. To that end, the first-of-a-kind underground coal storage facility was finalized in the city of Helsinki 2004 in connection to Salmisaari CHP power plant, replacing outdoor coal storage. The underground storage has a total capacity of 250, 000 tons, which corresponds to about half of the yearly fuel consumption of the plant. The advantages of a closed underground storage in comparison to an above-ground storage include automated operation, greatly reduced dust, noise and loss of heat content and improved aesthetics. The new storage facility also provided an opportunity for the City of Helsinki to free up approx. 100,000 m^2 of urban real estate close to the city center [65]. However, it also put focus on resilience of underground coal storage. Due to its favorable bedrock, the city of Helsinki has around 10,000,000 m^3 of underground space, including storages for energy purposes and technical tunnels for pipelines and cables [77].

The main organizations related to the energy supply infrastructure in Helsinki, also with regard to risk and resilience, are Helen Ltd. and the National Emergency Supply Agency (NESA). Helen is the producer and distributor of district heating and district cooling in Helsinki, owner of the CHP power plants, heating plants and distribution networks, and one of city's electricity distributors. In terms of resilience, Helen is responsible for ensuring energy supply to its customers without major disturbances, including working with risk management and business continuity management [29][30]. NESA, working under the Ministry of Employment and the Economy, is responsible for planning and measures related to developing and maintaining security of supply and emergency preparedness, including for the energy supply sector [46]. Other important organizations with respect to risk and resilience include the City of Helsinki, the Finnish Safety and Chemicals Agency (TUKES), the association of Energy Industry (Energiateollisuus) and insurance companies. See also Table 29.

For this study, relevant material publicly available has been reviewed and interviews have been carried out with representatives from Helen and from NESA to discuss end user's needs, challenges and requirements in assessing resilience in the energy supply infrastructure.

Table 29: Actor Analysis HOTEL

Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*
Huoltovarmuus-keskus	National Emergency Supply Authority (NESA)	National	Public	Responsible for planning and measures related to developing and maintaining security of supply and emergency preparedness for all critical infrastructures, including those in the energy supply sector.
Helen Oy	Helen Ltd	National/ Local	Private	Producer and distributor of district heating and district cooling in Helsinki, owner of the CHP power plants, heating plants and distribution networks, and one of city's electricity distributors. Responsible for ensuring energy supply to its customers without major disturbances. There are also other energy companies in Finland providing electricity to the public in Helsinki.
Helsingin kaupunki	City of Helsinki	Local	Public	Helsinki's role as the nation's capital and the City's role as the main local government in Finland set requirements on the City to ensure that its key services function in all circumstances. Works with continuity management and other crisis containment measures on city level, with prepared operation models for emergencies caused by extreme weather and other circumstances. Cooperates with NESA and Helen on emergency preparedness issues.
Turvallisuus- ja kemikaalivirasto (Tukes)	Finnish Safety and Chemicals Agency (TUKES)			A licensing and supervisory authority, which promotes the safety and reliability of products, services and industrial activities in Finland. Tukes is tasked with the surveillance of production systems within its fields of operation, and enforces the relevant legislation.

4.8.2 Current status working with resilience and assessing resilience

On a national level, NESA is responsible for planning and measures related to developing and maintaining security of supply and emergency preparedness, including for the energy supply sector. One major task for NESA is to support and help companies, such as Helen, with improving their emergency preparedness and security of supply. This is done by, for example, developing and providing tools, guidelines and methods for continuity management. NESA also provides trainings and organizes shared drills, or simulated exercises, in order to test and improve emergency preparedness in e.g. the energy sector. For its work, NESA has

developed a Private-Public Partnership (PPP) model where public and private companies and organizations actively are involved and collaborate through 20 different "pools" or sectors in the National Emergency Supply Organization (NESO). The energy sector is involved mainly through the Power and District Heating Pool [48].

In practical terms, NESA uses the terms "preparedness" and "continuity" instead of "resilience", and uses the governance concept "Continuity management" in order to promote increased preparedness of the companies and organizations involved in NESO. Continuity management is seen by NESA as "*an integrated process driven from the top of the organization aiming, first, to prevent disruptions and, second, to reduce the impacts of a disruption to operation and secure the response/recovery of the organization's critical activities as quickly as possible after the disruption*" ([45] , p. 3). Figure 14 presents the continuity management concept as defined by NESA. Note that the continuity management concept and definition to large extent follows concepts and definitions of resilience (compare e.g. Figure 1).

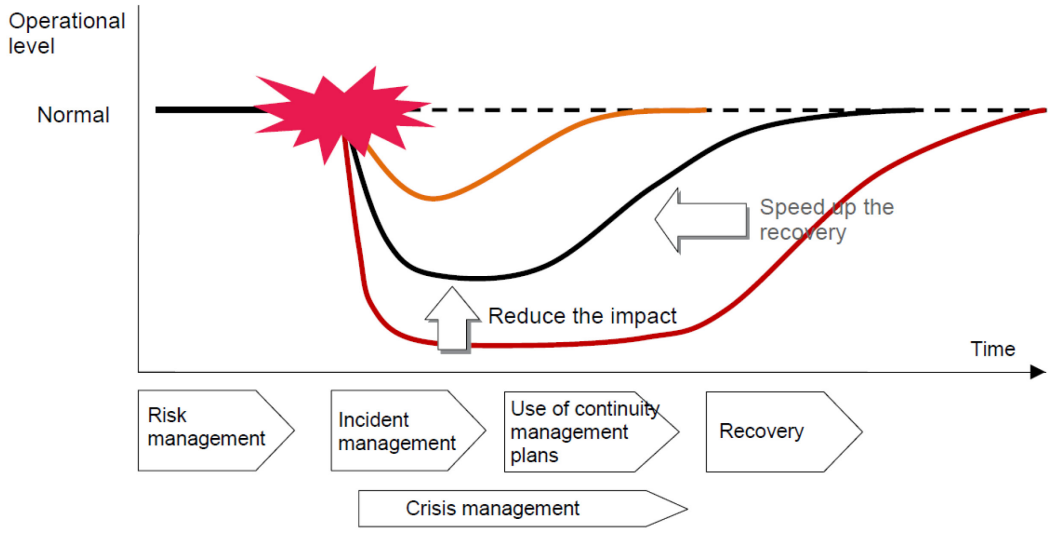

Figure 14: Concept of incident preparedness and continuity management as defined by NESA [45].

The HUOVI portal [47] and the SOPIVA project [49] managed by NESA are continuity-management tools designed to support companies and organizations in their continuity management efforts.

Although many energy related companies undertake preparedness measures, e.g. by business continuity management, on a voluntary basis with help of the tools provided by NESA, some energy companies are obliged by law to ensure continuity of their critical processes amid disruptions. For example, all electricity distribution companies in Finland under the Electricity Market Act have to have preparedness plans. NESA is responsible for monitoring and controlling these mandatory preparedness plans which the electricity distribution companies have to submit every two years. In the preparedness plans, the main risks of each company are outlined together with a plan how to manage those risks. Risks or threats particularly relevant for the energy supply infrastructure as a whole in Finland includes extreme weather events (such as storms), cyber-attacks and external and internal man-made risks, both intentional or accidental [50].

Helen, the owner of the main energy supply infrastructure in Helsinki, is working both with traditional risk management and with continuity management in order to become more resilient. Risks are identified and assessed at different levels in the organization; operational level risks, asset management risks and corporate level risks. Main risks include more frequent disruptions such as fires from fuels used in energy production, occupational accidents and leakages in district heating network system. However, more extreme risks are also discussed, such as extreme weather events, cyber-attacks and terrorism. In case of disruptions, Helen has plans and processes in place to manage them, including checklists, fire- and safety groups, stand-by personnel and communication channels with supporting organizations such the fire department and police. In order to increase preparedness, Helen also works with drills and simulated exercises, both internally organized together with e.g. the fire department or police, and those organized by regional or national organizations, such as NESA. Risks and preparedness are also discussed in different stakeholder groups, e.g.

the Association of Energy Industry, and during regular meetings with e.g. the City of Helsinki and other Energy companies [30].

Beyond risk management, Helen works with business continuity management in order to achieve a higher level of "maturity". This work includes increased awareness and discussion on risk- and preparedness issues, training for staff and improved cooperation with other organizations [30].

In terms of assessing resilience, assessments of continuity management "maturity" and organization preparedness are made both on company level by the respective energy companies and related to the energy sector as a whole by NESA [30][50].

On a company level, the assessments are made using one of the tools developed and provided by NESA, the HUOVI-portal, which includes a maturity analysis, or assessment, application. This application allows a critical infrastructure company or organization to assess its levels of preparedness and areas in which improvements are needed. The assessment application contains about 200 – 300 items (statements or descriptions) and for each item, the companies assess or reflect on their current status on a scale from 1-5 as well as desired status on a scale from 1-5. From the assessment it is then possible for the companies to identify the gap in preparedness or continuity between current state and desired state [50].

This self-assessment at company level is for most voluntary, offered to all critical infrastructure companies, but has according to the representative at NESA not been used excessively to date (the assessment application was introduced in 2010). However, within the energy sector, the Electricity Market Act requires all electricity distribution companies to make an assessment based on 70 items, specifically developed for these companies, within the maturity assessment tool. These assessments are submitted to NESA together with the mandatory preparedness plans every two years. Due to this mandatory assessment, the electricity distribution companies have to a larger extent than other companies used HUOVI-portal to make a self-assessment of their preparedness. Furthermore, NESA has also developed a specific set of items within the assessment application for the district heating companies; however, this assessment is voluntary [50].

Helen is one of the energy companies who is using the assessment application in the HUOVI-portal to measure its maturity in terms of preparedness and continuity management, both as the mandatory assessment outlined in the Energy Market Act (for their electricity distribution) and voluntary (as a district heating producer and distributer). The representative from Helen expressed that the maturity analysis application in the HUOVI-portal is a good tool to assess Helen's preparedness and maturity.

On a national level, a general assessment on the energy sector as a whole is made every two years using the mandatory self-assessments from the electricity distribution companies and voluntary self-assessment from other energy companies. The representative from NESA highlighted that this is not a very reflective assessment, but it is used to determine where the largest gaps are in the energy sector between current state and desired state in preparedness. This general assessment is discussed in the Power and District Heating Pool within NESO and used by NESA to decide where to focus their support and help towards the energy companies in order to promote further continuity management, or resilience.

In general, the representatives from Helen and NESA underlined that indicators are not used for the assessment of resilience in the energy supply infrastructure, either on company level or national level in Finland or Helsinki (to their knowledge). The overall assessment made on national level could, according to interviewee from NESA, be seen as an indicator in itself. However, this overall assessment is not widely used or official but mainly guides NESA's internal work ahead. There are some indicators used by Helen in terms of anticipating and avoiding frequent risks (e.g. temperature in coal storage to avoid fire) or indicators measuring the preparedness and need for improvement during shared drills and simulation exercises .

4.8.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: fires from fuels used in energy production, occupational accidents and leakages in district heating network system. However, more extreme risks are also discussed, such as extreme weather events, cyber-attacks and terrorism. As the assessment application in HUOVI-portal has been developed by NESA together with the targeted companies and organizations in order to find the most relevant points, the representative from NESA described the assessment application as it is today as usable and relevant for its purpose. The NESA interviewee highlighted that the assessment application is mainly a tool for companies' self-assessment in order to "force" the companies to consider preparedness and continuity management to a larger extent in their organizations and work on improving their preparedness.

However, one current need is to develop the assessment application to better include new and imminent threats, such as cyber and data security issues that have become more common and frequent in the last years. The interviewee from NESA underlined that it is important for any resilience assessment tool to adapt to changes in society.

In terms of the possibility of using indicators to a wider extent to assess resilience, the representative from NESA was positive towards a more indicator-based assessment of resilience that could give reliable numbers and figures on resilience development over time. However, there is currently a lack of tools to support such assessments and it would also require that more resources were allocated to NESA in order to work with these indicators. As it is now, the resources of NESA are limited and if too much focus would be spent on assessing resilience through indicators and by looking at figures, then less time would be spend "out in the field supporting companies and organizations in making themselves more resilient". For NESA, helping and supporting companies and organizations becoming more resilient in practice is more important than to follow up on indicators, the interviewee underlined. However, if NESA had more resources, a more indicator based assessment could be developed and used.

For Helen, working with risk and resilience and assessing them is challenging in terms of making it an integrated part of company processes and daily work, especially as resources are limited and work plentiful. The Helen representative highlighted, for example, that although the process of risk management has become more integrated in their daily work today it is challenging to measure and follow-up that the process is working or "*that we are doing as we say we do*". This is also true for business continuity management, which is still a novel way of working in Helen and not as integrated yet in the daily work or processes.

Another current challenge underlined by the representative from Helen in working with resilience in general, but also related to assessing resilience, was that different organizations are using different tools and terminology for, more or less, the same type of work. This makes communication and cooperation on risk and resilience issues more complicated. For example, the respondent from Helen puts forward that, although energy companies are to large extent speaking with the same language, they experience that many authorities have different terms for the same requests, resulting in confusion. In general, the term "resilience" is not used. This lack of common general terminology between organizations was confirmed by the representative from NESA, further highlighting the fact that Finland having two official languages (Finnish and Swedish) makes common terminology even more challenging as there are always at least two terms for the same concept. However, the interviewee from NESA underlined that they are making an effort in using terms related to resilience (e.g. "preparedness" and "continuity management") consistently towards the companies and organizations in order to promote and spread a "common language".

4.8.4 Foreseen challenges, needs and requirements for assessing resilience

Increased smartness of the energy infrastructure is highlighted as an aspect that will put more emphasis on monitoring and assessment in the future in order to follow the status of the energy infrastructure in terms of e.g. resilience and to ensure companies' capability of steady energy supply.

The increased energy generation from "non-predictable" renewable energy sources, such as wind and solar power, will require more smart distribution network and infrastructure as it is not as reliable as other energy sources and also further de-centralizes energy production. This requires more smart devices within the distribution networks that can handle de-centralized distributed and non-predictable energy production with many energy generation sources. To increase the share of renewable energy in energy production is seen as something valuable for society and the environment, but also for pricing reasons, but the challenges it poses regarding resilience and security of supply in the critical energy infrastructure is not yet widely discussed [50]. Hence, here there might be potential conflict between maintaining and improving security of supply and resilience and reaching environmental and societal objectives, at least short-term.

The issue of smarter infrastructures in terms of resilience is discussed to some extent by e.g. NESA and Helen, but is underlined by the interviewee from NESA as something that needs to be discussed more in the future. In Table 30 below, the challenges, needs and requirements for the HOTEL case are summarized.

Table 30. Challenges, needs and requirements for the HOTEL case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* fires from fuels used in energy production, occupational accidents and leakages in district heating network system. However, more extreme risks are also discussed, such as extreme weather events, cyber-attacks and terrorism. 2. *Main challenges*: (a) to develop the assessment application to better include new and imminent threats, such as cyber and data security issues that have become more common and frequent in the last years; (b) different organizations are using different tools and terminology for, more or less, the same type of work, making communication and cooperation on risk and resilience issues more complicated.	1. The current lack of indicators, tools and systems for such as assessment and a lack of resources today within companies and organizations to handle and work with such assessments. 2. For an energy company, as with most new management systems, it is also challenging making resilience work (e.g. continuity management) and its assessments an integrated part of company processes and daily work, especially as resources are limited and main work is focused on production and distribution of energy products.
Current needs and requirements	**Foreseen needs and requirements**
1. Maturity analysis, or assessment, application. This application allows a critical infrastructure company or organization to assess its levels of preparedness and areas in which improvements are needed. 2. Plans and processes in place to manage risks, including checklists, fire- and safety groups, stand-by personnel and communication channels with supporting organizations such the fire department and police. 3. Drills and simulated exercises, both internally organized together with e.g. the fire department or police, and those organized by regional or national organizations, such as NESA. 4. Risks and preparedness are also discussed in different stakeholder groups	1. The increased energy generation from "non-predictable" renewable energy sources will require more smart distribution network and infrastructure as it is not as reliable as other energy sources and also further de-centralizes energy production. 2. Here there might be potential conflict between maintaining and improving security of supply and resilience and reaching environmental and societal objectives, at least short-term.

4.8.5 Discussion and conclusion

In Helsinki and Finland, organizations and companies critical for the security of supply, e.g. energy supply, are working actively on becoming more resilient through tools and models such as risk management and continuity management. Assessments of resilience are made regularly on organizational level (by some companies) and on sector level for the infrastructure as a whole (by NESA).

The main purpose of these self-assessments made by energy companies and organizations is to encourage or "force" these actors to consider preparedness and continuity to a higher degree within their organizations, and to guide them on where to put their efforts in improving their preparedness (i.e. where the main gaps are). On a sector level, the overall assessment of preparedness, or resilience, is mainly used as a basis for discussion within NESO and to guide NESA's work ahead to address main needs in improving resilience. Hence, the assessments are not aimed at monitoring resilience development over time but rather to point out areas of improvement.

Indicators are not widely used for resilience assessment to date related to the energy supply infrastructure in Helsinki, but the current assessment tool is viewed as usable and good tool for its purposes. The representatives from NESA and Helen, however, saw a value a more indicator-based assessment or other types of assessments than current of their resilience work. Especially so when the energy supply infrastructure will need to become smarter to manage "new" sources of energy.

At the same time, a number of challenges to this end are outlined, including the current lack of indicators, tools and systems for such as assessment and a lack of resources today within companies and organizations to handle and work with such assessments. For an energy company, as with most new management systems,

it is also challenging making resilience work (e.g. continuity management) and its assessments an integrated part of company processes and daily work, especially as resources are limited and main work is focused on production and distribution of energy products. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the HOTEL case can be summarized in Table 31 below. The stakeholders in this case study seem to use quite elaborated concepts of resilience, but lack the tools and the resources to use them for assessing resilience at least for issues of complex interdependencies between SCIs. Issues of secure data management are becoming more imminent.

Table 31. Summarizing the most important issues for which the Smart Resilience methodology can be used for identifying, vizualizing and assessing resilience for the HOTEL case study.

Dimensions of resilience	Examples from HOTEL
System/physical: Technical aspects, physical/technical networks, interconnectedness	External triggers: Fires from fuels used in energy production, leakages in district heating network system. However, more extreme risks are also discussed, such as extreme weather events, cyber-attacks and terrorism.
Information/data: Technical systems dealing with information/data	The current lack of indicators, tools and systems for such an assessment
Organizational/business: Business-related, financial and HR aspects and organizational networks	A lack of resources today within companies and organizations to handle and work with assessments. For an energy company, as with most new management systems, it is also challenging making resilience work (e.g. continuity management) and its assessments an integrated part of company processes and daily work.
Societal/political: The broader societal/social context, indirect stakeholders	Here there might be a conflict between maintaining and improving security of supply and resilience and reaching environmental and societal objectives. Different organizations are using different tools and terminology for, more or less, the same type of work, making communication and cooperation on risk and resilience issues more complicated.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	To develop the assessment application to better include new and imminent threats, such as cyber and data security issues that have become more common and frequent in the last years.

4.9 DSB: Assessing resilience in interconnected critical infrastructures in Oslo

4.9.1 Introduction

In addition to strengthening the resilience of single critical infrastructures, SmartResilience aims at shedding light on the interconnectivity between infrastructures. In the project's description of resilience [37], the term "integrative resilience" emphasizes the complex interconnections between infrastructures and their environment. Interconnectivity creates a need for collaboration and coordination. The emphasis in this study is on the role of the Norwegian Directorate for Civil Protection (DSB) in dealing with interconnectivity.

DSB is responsible for civil protection, covering national, regional and local preparedness and emergency planning, fire and electrical safety, safety in handling and transport of hazardous substances. It is DSB's overall responsibility to keep oversight of risk and vulnerability in Norway. Their mandate is to prevent accidents, crises and other unwanted events, and to ensure sufficient level of emergency preparedness and crisis management. As part of the Ministry of Justice and Public Security, DSB has a special responsibility for facilitating coordination across sectoral boundaries. Although DSB may play a direct role in the management of national crises, their main relation to societal resilience is indirect, through assessing and facilitating the resilience of industrial actors and public sector entities. The latter role is the main emphasis in this study.

DSB has performed several studies of what may be labelled concentrated industrial areas, i.e. areas with several enterprises with major accident potential concentrated within one site. The emphasis in this study is on the role of DSB in ensuring that risk governance and coordination activities take place, and their need for new indicators in this respect. The emphasis is on DSB's role in creating oversight and coordination between different stakeholders in Oslo Harbour (Sydhavna). See Figure 15.

The Sydhavna area is critical for several important critical infrastructures and societal functions. According to the DSB report [2], 40 % of Norway's total fuel consumption, as well as all fuel consumption to Oslo Airport's aviation passes through this area. A large fuel depot in Ekebergåsen is also closely connected to the Harbor. This comes in addition to Sydhavna being a large port, with a correspondingly large volume of bulk and cargo logistics. The city center of Oslo is only three kilometers away, and there are roads, railway lines and large sewerage systems in very close vicinity of the harbor.

Sydhavna contains several enterprises with major accident potential. This introduces the potential for domino effects within the area, as well as potentially serious consequences for other critical infrastructures and societal functions. The area's overall risk may thus be greater than the risks of each individual enterprise. Several industrial actors, different societal sectors and different regulators will be involved in a complex process of governing the individual and accumulated risks. Indicators for both risk and resilience within such an area will therefore require collaboration and exchange of information between several organizations.

Figure 15: Overview of the Sydhavna area and the nearby critical infrastructures. Adapted from [53].

4.9.2 Current status working with resilience and assessing resilience

While the concept of resilience is part of DSB's general vocabulary, they have not performed dedicated assessments of resilience. However, they regularly perform supervisions of risk management and emergency preparedness which provide important information about resilience. Their assessments of interconnectivity concentrated industrial areas are examples of this. Two major assessments on this topic have been on Sydhavna [55] and Risavika [54]. The main conclusion of the Sydhavna assessment was that while there was a large number of risk assessments from the individual risk owners perspective, there were serious shortcomings in the overall risk assessment of the area:

There is a lack of analyses with comprehensive assessments of all relevant conditions, and which also evaluate the organizational and management-related prerequisites for proper safety in the area. It also appears unclear how the responsibility for conducting comprehensive risk assessments has been understood and followed up by key actors [55].

This was interpreted as a shortcoming in the knowledge of the risk situation of the area, as well as pointing to weaknesses in the collaboration and coordination among the companies in the area and the public organizations and supervisory authorities involved.

Three activities of relevance for resilience assessment were discussed during the interviews:

- The HarbourEx exercise
- A joint supervisory action
- A report on safety in critical infrastructures and societal functions

HarbourEx15

HarbourEx15 was s a full-scale rescue and cooperation exercise in April 27th – 29th 2015 with scenarios connected to operations in Oslo's main harbor, Sydhavna [53]. The national goals for HarbourEx15 were to evaluate the mobilization of the emergency organization and in particular the communication between involved agencies and stakeholders, including communications to the public. The exercise involved also personnel from the European Emergency Response Coordination Centre sending a team of experts from Sweden and Austria. More than 3,000 participants were mobilized from more than 30 organizations.

HarbourEx15 addressed the critical question; would the required resources find each other in dealing with an unexpected and demanding scenario? The evaluation emphasized that there was significant room for improvement in the communication between the actors involved. A main observation was that relevant information about the incident was communicated too late to the public, e.g. how the public should respond to toxic smoke and how people should prepare for possible evacuation. Another observation was the need for strengthening communication lines between governmental agencies, and for the preparation of procedures and agreements that ensure effective communication and coordination between authorities. The EU Civil Protection team (EUCP) should improve their understanding of their own role and at what level their contribution is of benefit. When the affected country's crisis management structures works well, the most beneficial contribution from the EUCP team will be on strategic and administrative level. HarbourEx is a case of resilience demonstration in an area with interconnected and complex risk. Evaluations of such exercises can provide direction to the development of indicators by pointing to areas where the system is currently working resiliently, and areas where there is need for improvement.

Photo: Espen Reite/Kysteverket

Joint supervisory action

Interorganizational cooperation can be an important resilience resource, particularly where there are dependencies that cross organizational borders. However, coordination of internal control and more comprehensive management of risk in concentrated industrial areas is a challenge for both the government and the relevant enterprises. One of the follow-up activities of the Sydhavna study was to establish a joint supervisory action, i.e. supervision based on close collaboration between the different supervisory authorities involved with concentrated industrial areas.

One challenge for both DSB and the enterprises is to establish a comprehensive risk landscape for determining when coordination of internal control is required. According to regulations, enterprises should also include external factors in their risk assessments and justify adequately why coordination may not be necessary. However, there is no specific guidance with respect to acceptable level of detail of the risk analyses. The joint supervisory action identified a need for more systematic knowledge about effects and consequences of coordinated supervision and the development of suitable methodology and appropriate models for including external factors in risk assessments.

Report on safety in critical infrastructures and critical societal functions (KIKS)

One lesson learned from supervisory activities is that there has not been a clear definition of the different critical infrastructures and their corresponding societal functions. Furthermore, a description of how such infrastructures and societal functions may be identified has been lacking. This is information which will be a necessary initial step in developing indicators, and the DSB are in the process of publishing a report describing an approach for assessing the performance of critical infrastructures and societal functions (the

KIKS project [52]). The report should support the Ministry of Justice and Public Security in establishing and maintaining an overview of which functions are critical for societal security in a cross-sectoral perspective. The term critical societal function is defined as those functions that are required to meet the population and society's basic needs such as food, water, heating, security and the like [56].

In the KIKS project, societal functions are grouped by the way in which they help to meet the population's safety and welfare. The three categories are: 1) Control ability and sovereignty, 2) Population security, and 3) Society functionality. Within each category, "capabilities" are defined which describe the performance level to be maintained by society at all times. The capabilities are based on two premises: 1) a societal function is particularly critical if an interruption of seven days or less will threaten the population's basic needs, and 2) emergency resources may be challenged within that period. Fourteen critical societal functions and associated capabilities have been developed.

Figure 16 shows the hierarchy between critical societal functions and capabilities.

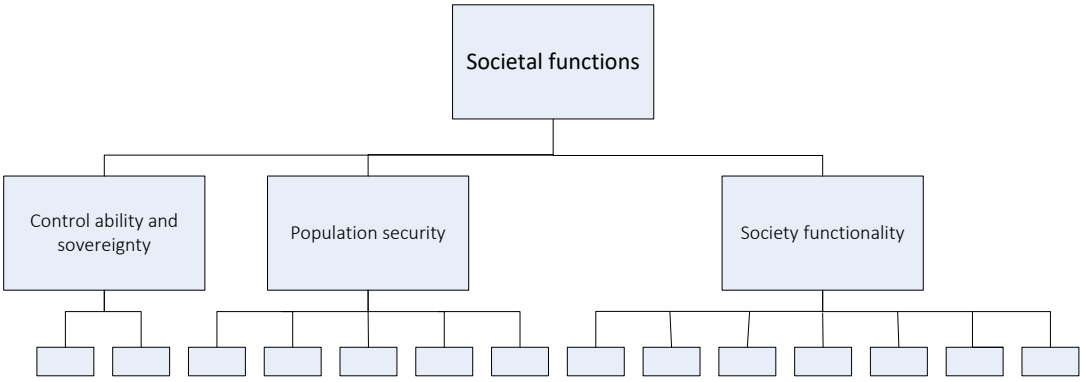

Figure 16: Hierarchy of critical societal functions and capabilities (For illustration).

The next step of the KIKS approach is to develop indicators that may measure the performance level of each category.

4.9.3 Main threats, current challenges, needs and requirements for assessing resilience

Most relevant threats: Sydhavna contains several enterprises with major accident potential. This introduces the potential for domino effects within the area, as well as potentially serious consequences for other critical infrastructures and societal functions. The current challenges, needs and requirements are related to the first part of the Resilience definition (see 1.3), the ability to understand risk and the probability for triggering events. Currently, there is a need for better indicators describing the accumulated risk of an area with concentrated industrial activity. Examples given in the interviews include a better overview of the volume of different hazardous substances, the number of incidents related to personal and process safety, the number of deviations from internal control activities and the level of maintenance.

A better understanding of individual and accumulated risks will enable DSB to achieve three interrelated improvements:

- More continuous follow-up of risks. Currently, the main source of information about risk comes from the direct supervision of companies and areas. However, DSB can only perform a limited number of direct supervisions per year. A set of risk indicators allowing for more continuous monitoring of risks would enable DSB to have broader and more updated information about risk.
- Risk informed selection of topics of supervision. DSB selects different topics for series of supervisory activity. Better indicators would allow for a more informed selection of such topics, thereby ensuring that the emphasis is placed on the most important topics.
- Risk-based selection of objects for supervision. In order to make the most of the available resources, the supervisory activity should be focused on the companies or areas where the risk is the highest.

Indicators providing DSB with an improved understanding of risk would be an important improvement in this respect.

There are some challenges against achieving these improvements. DSB would need indicators aggregating information from several actors. This means that DSB will be dependent on the way data is gathered and processed by the actors they are set to supervise. Companies will, however, have varying capacity in this respect. Larger companies are likely to have sufficient resources and systems in place, while this may not be the case for smaller firms. Another challenge lies in the actors' willingness to share information. Both with regard to competition and security, it may be rational for companies not to share information with the external environment, as long as this is not made mandatory by regulation. In order to meet these challenges, a first step will be to establish a set of guidelines for collecting

4.9.4 Foreseen challenges, needs and requirements for assessing resilience

As already indicated, the first user need to be satisfied from a governmental agency perspective, is finding indicators that enables understanding of risk through continuous monitoring. This involves starting the quest for smart RIs by finding more traditional risk indicators. Addressing the other aspects of resilience, i.e. the capacity to adapt, respond and respond/recover is a more long-term need. Three long-term needs for RIs were highlighted:

- Indicators describing technical and organizational complexity of supervisory objects. Dealing with interconnectivity requires good system descriptions. Finding a measure of how complicated or complex the involved systems are, is seen as an important part of a future set of RIs. Examples of possible indicators include the number of systems and infrastructures that can be said to be connected, the number of owners involved and the extent of organizational changes and changes in ownership.
- Indicators for collaboration and coordination. Several of DSB's studies [55], [54], [53] and investigations into national disasters [56], [57] point to a need for improvement in the collaboration and coordination across organizational and sectoral boundaries. While it is not straightforward to turn information about coordination activities into quantitative indicators, such indicators would be highly valuable for governmental actors with responsibility for supervision of comprehensive risk.
- Indicators for response capability. Currently, DSB assesses the emergency response plans of supervisory objects. Indicators supplementing plan assessment with information about the response capabilities are needed. Among the examples mentioned are the frequency of dialogue with the fire department, the number and type of drills and exercises.

These three issues should be considered in the future development of smart RIs. In table 32 below, the challenges, needs and requirements for the DSB case are summarized. In this case, resilience can be a useful concept for unifying different frameworks, and coordinated terminology a vehicle for addressing organizational diversity.

Table 32. Challenges, needs and requirements for the DSB case.

Current challenges	Foreseen challenges
1. *Most relevant threats:* Sydhavna contains several enterprises with major accident potential. This introduces the potential for domino effects within the area, as well as potentially serious consequences for other critical infrastructures and societal functions. 2. *Main challenges:* More continuous follow-up of risks; Risk informed selection of topics of supervision; Risk-based selection of objects for supervision	1. Indicators describing technical and organizational complexity of supervisory objects. 2. Indicators for collaboration and coordination. 3. Indicators for response capability.
Current needs and requirements	**Foreseen needs and requirements**

1. Currently, the main source of information about risk comes from the direct supervision of companies and areas. A set of risk indicators allowing for more continuous monitoring of risks would enable DSB to have broader and more updated information about risk. 2. DSB selects different topics for series of supervisory activity. Better indicators would allow for a more informed selection of such topics, thereby ensuring that the emphasis is placed on the most important topics. 3. In order to make the most of the available resources, the supervisory activity should be focused on the companies or areas where the risk is the highest.	1. Dealing with interconnectivity requires good system descriptions. Finding a measure of how complicated or complex the involved systems are, is seen as an important part of a future set of RIs. 2. Several of DSB's studies and investigations into national disasters point to a need for improvement in the collaboration and coordination across organizational and sectoral boundaries. 3. Currently, DSB assesses the emergency response plans of supervisory objects. Indicators supplementing plan assessment with information about the response capabilities are needed

4.9.5 Discussion and conclusion

The interconnectivity between infrastructures poses a challenge to the development of indicators with respect to interorganizational coordination and exchange of information. A good set of indicators for a critical infrastructure is likely to require the inclusion of information from external actors. This is a user need that is present both within each infrastructure sector, and for users in need of information about comprehensive risk, like DSB.

There are two important points of feedback from the DSB as an end user. Firstly, it is important to have a solid foundation of risk indicators before turning to the larger questions of RIs. In order to develop valid risk indicators at a governmental level, improvements need to be made in the way data is gathered and processed by risk owners. The KIKS approach represents an important foundation in this respect. Secondly, indicators need to be able to cover both the inherent, physical risk and risks related to organization and decision-making (as described in the SmartResilience matrix [37]). Interconnectivity poses a demanding management challenge that needs to be addressed in addition to technical matters. Analyzing the current and foreseen challenges, needs and requirements according to the five dimensions of resilience for the DSB case can be summarized in table 33 below.

Table 33. Summarizing the most important issues for which the Smart Resilience methodology can be used for identifying, visualizing and assessing resilience in the DSB case study.

Dimensions of resilience	Examples from DSB
System/physical: Technical aspects, physical/technical networks, interconnectedness	Potential for domino effects within the area, as well as potentially serious consequences for other critical infrastructures and societal functions.
Information/data: Technical systems dealing with information/data	Indicators describing technical and organizational complexity of supervisory objects. Indicators for collaboration and coordination. Indicators for response capability.
Organizational/business: Business-related, financial and HR aspects and organizational networks	A set of risk indicators allowing for more continuous monitoring of risks would enable DSB to have broader and more updated information about risk. Organizational complexity raises challenges for data collection.
Societal/political: The broader societal/social context, indirect stakeholders	A need for improvement in the collaboration and coordination across organizational and sectoral boundaries.
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Dealing with interconnectivity requires good system descriptions. Finding a measure of how complicated or complex the involved systems are is seen as an important part of a future set of indicators.

5 Survey to members of the Community of Users of Safe, Secure and Resilient Societies

5.1 Results

Less than half of the respondents (4 out of 12) of the survey have substantial experience of resilience, while approximately half of the respondents have substantial experience of risk management (7 out of 12) and business continuity (6 out of 12). Half of the respondents (6 out of 12) have limited experience of resilience, see Figure 17.

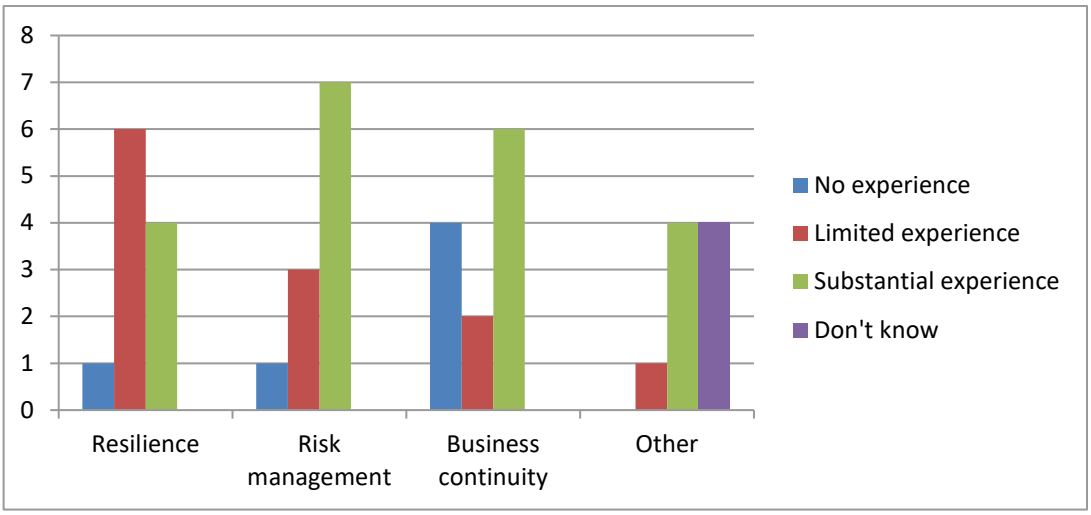

Figure 17: Do you have professional experience of working with any of the following concepts?

Concerning resilience usefulness in comparison with other approaches, half of the respondents (6 out of 12) consider resilience more useful than risk management. Less than half of the respondents (5 out of 12) find resilience more useful than business continuity (see Figure 18).

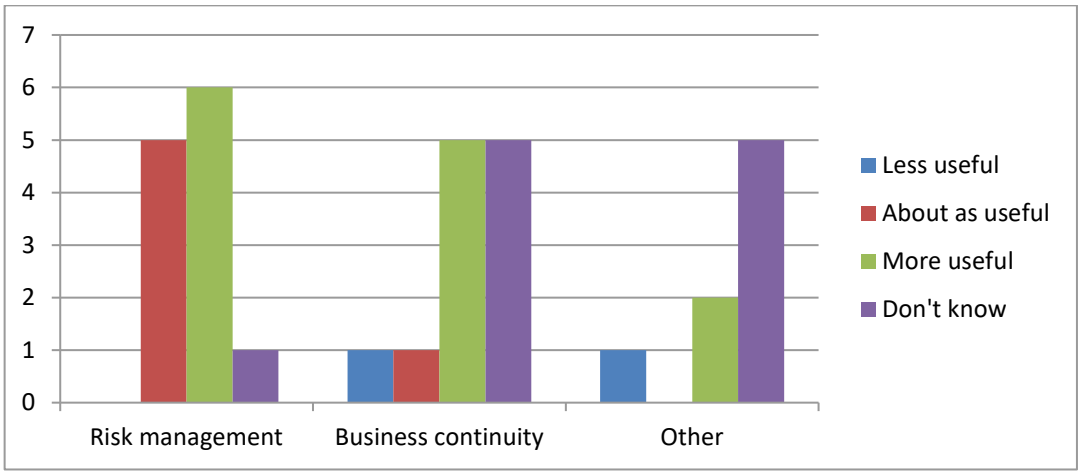

Figure 18: In your opinion, how does resilience compare to the following approaches in terms of usefulness? Resilience models are.....than....

A majority of the respondents consider current assessments of different phases[4] of resilience"very useful" or"more useful than not". Possible explanations for this result could be that the respondents, which to a large degree have professional experience of working with resilience, are already satisfied with current assessments and don't see the need for investing in additional concepts/tools. Another possible explanation could be that the terms used in the survey may have a different meaning to the respondents and/or the random influences due to the low response rate. Regarding this question on the usefulness of current assessments, one respondent commented that is it important to learn from disruptions. Focus should not be on restoring back to the operational level which was before the disruption, but rather on evolving and upgrading in order to avoid new disruptions.

In response to the open question "*In your opinion, what is needed to improve current assessments of resilience?"* the following responses are highlighted:

- "Mathematic models should be used, and the ability to understand 'how complex is the infrastructure' and the key elements of high natural resilience must be integrated".
- "The inclusion of cost assessments and resource expenditure is important in responding to and respond/recovering from a disruption. The assessments need to be able to consider real data, interdependencies among open systems of systems, understand and retro-analyze past events and create databases of real case studies."
- "The current assessments need to be improved regarding handling the variety of socio-economic contexts and potential risks (e.g. local, global, short-term and long-term)."
- "The indices and variables of resilience for variety of topics, e.g. social, economic, employment, education, occupation, infrastructure, community life, need to be defined."

It is interesting to note the large variety in suggested needs for improvement, despite the small number of respondents. However, several of these quotes illustrate the need for taking specific contexts into account: the complexity of the infrastructure in focus; building on real data and real case studies; handling a variety of socio-economic responses and risks; for a variety of topics.

5.2 *Implications of results for usefulness*

Although the low response rate calls for caution in interpreting the results of the survey to CoU, the responses suggests a number of challenges for the SmartResilience project. First, the need for the project to create assessments and RIs that are clearly regarded as providing added value in relation to end users' current and foreseen needs. Second, the challenge to design assessments and RIs that can be widely disseminated, while at the same time taking different contexts into account. Should the project focus on a smaller number of contributions that are designed in line with contextual requirements and what contributions should then be prioritized (for example, those closest to the purpose of the project or those in most need of improvement)?

[4] The respondents were asked "*In your opinion how useful are current assessments of the following phases of resilience?*" concerning: Ability to understand risk, Ability to anticipate changing conditions, Ability to prepare for changing conditions, Ability to adapt to changing conditions, Ability to withstand disruption, Ability to respond to disruption and Ability to respond/recover rapidly from disruption. The unknown/unexpected was not included. See also Annex 6.

6 Analysis and discussion

6.1 Introduction

Task 1.3 in the SmartResilience project has focused on the assessment of resilience; in particular end users' challenges, needs and requirements for doing so. This chapter analyses the empirical data collected for the case studies ALPHA-HOTEL and the case study DSB, the literature review and the survey to CoU, as well as discusses the main findings. Although this report has argued for the need to contextualize indicators and be attentive for context-specific developments, it is still possible to see patterns that are common across several cases. The SmartResilience project should be aware of such common challenges, needs and requirements, and these have been synthesized in Table 13 and 14.

Attention is first directed to current and foreseen challenges and then to the current and foreseen needs and requirements. Some challenges can be translated to needs and requirements, but other challenges are better described as conditions that cannot be changed, only managed. The chapter concludes with a discussion of the findings in light of the actor analysis approach used in this study and how actor analyses relate to stakeholder management.

6.2 Analysis of current and foreseen challenges

The research conducted in Task 1.3 has confirmed a number of challenges for assessing resilience, which were used as a point of departure for designing SmartResilience. Yet, this study also provides insight into what these challenges contain by providing examples from the case studies. Not only does this provide a broader understanding of the challenges, but it also suggests what cases of critical infrastructure(s) that share common challenges.

Table 34 lists a number of examples that illuminates key challenges addressed in SmartResilience, and what empirical data from this study that confirms or supports these challenges. The examples can serve as further input to the development of the resilience assessment methodology and smart RIs within SmartResilience from an end user perspective.

Table 34: Current and foreseen challenges among end users

Challenges	Examples	Empirical support
The concept of resilience	Use of the term	ECHO, FOXTROT, HOTEL
	Confusion on difference from other terms or the added value	Survey to CoU, ALPHA, FOXTROT
	Different levels of "maturity" in assessments and indicators of resilience	BRAVO, FOXTROT
	Emphasis on different phases of resilience	DELTA, ECHO
External threats (climate change, cyber-attacks, terrorist attacks, flooding)	Uncertain and different time frames	ALPHA, CHARLIE, FOXTROT, GOLF
	Appropriate tools for new threats	BRAVO, HOTEL

The complexity of critical infrastructures	Interdependencies	CHARLIE, DELTA, DSB, ECHO
	Fragmentation/segmentation	CHARLIE, FOXTROT, DSB
	Urbanization	BRAVO, ECHO, FOXTROT, HOTEL, DSB
Data management	Data security (sensitive data)	ALPHA, BRAVO, CHARLIE, DSB, ECHO
	Abundance of data	CHARLIE, ECHO FOXTROT

Challenges related to the *concept of resilience* include that all relevant actors in a critical infrastructure do not use the term resilience, nor understands how it relates to other concepts such as risk management, business continuity, vulnerability assessments, emergency preparedness or continuity management. Resilience (if used) is defined, understood and applied in different ways by the end users, even within the same critical infrastructure. The term can also be difficult to translate into other languages. Moreover, the added value of using resilience instead of other term(s) is not always clear. This can lead to that some vital actors may focus on only parts of the phases of the resilience cycle in its "u-curve" (cf. Figure 1). The meaning of these concepts can be specific for the single organization, rather than for the infrastructure as a whole, which can create confusion and hinder effective cooperation. Moreover, resilience is not necessarily part of everyday activities or integrated into current assessment tools. What these challenges have in common is to bring all relevant stakeholders within a critical infrastructure to the same level, using the same terminology.

The *external threats* that were explicitly mentioned by end users in this study are climate change, cyber-attacks, terrorist attacks or sabotages, and flooding. End users have described how some organizations within the critical infrastructure focus on short-term response measures while others use longer time horizons. Also, end users have described how the threats caused by climate change, which increased flooding is also related to, will be even more important in the future. These observations suggest a challenge to determine appropriate time frames, in particular when planning for new infrastructure and investment decisions are made with effects for decades ahead. Appropriate tools for new threats are also challenging, such as in the case of cyber-attacks.

With regards to the *complexity of critical infrastructures*, several case studies have shown how interdependencies and interconnectedness poses particular challenges with regards to collaboration and coordination across organizational boundaries. A fragmented or segmented sector, which consists of many different organizations with different capacities and preconditions, makes the challenge of collaboration and coordination even more significant. Smaller companies may not have the appropriate knowledge, systems or resources. The SCIs in SmartResilience become even more complex due to the fact that they are situated in or near cities. This raises challenges in terms of increased urbanization and settlement near vulnerable areas and increases the interconnectedness between different critical infrastructures. This becomes particularly evident in the SmartResilience project which focuses on cities and the fact that many European countries experience significant urbanization.

Two specific challenges were highlighted with regards to *data management* in this study. Much of the information involved in making critical infrastructure more resilient is confidential, sensitive, information. This requires high standards for data security. Also, in the wake of increased smartness of critical infrastructures, many end users find themselves overwhelmed by the abundance of data available. Making this data manageable is seen as an important challenge in order to avoid "information overload".

In sum, the study on end users' challenges confirms several of the challenges that were used as a basis to develop the project SmartResilience. This is not surprising, given that the case studies have been assisted by partners within the project (although complemented with additional actors that are relevant for the particular critical infrastructure). In this sense, this section has provided a broader understanding of what the challenges contain, and suggested what cases of critical infrastructure(s) that share common challenges.

6.3 *Analysis of current and foreseen needs and requirements*

End users' needs and requirements are intimately linked, which is why they are presented jointly in this section. Before turning into the findings from the case studies, an important first issue to be raised is whether current assessments of resilience, or different phases of resilience, already meet the needs of end users. Results from the survey to the CoU seem to indicate that at least some respondents find current assessments satisfactory, or do not see the added value of assessing resilience. However, findings from the case studies suggest that some end users do not assess resilience in all phases of the resilience cycle and that in particular the right part of the "u-curve" is overlooked (cf. Figure 1).

Table 35 lists a number of end users' needs and requirements for identifying, visualizing and assessing resilience identified in this study according to the five dimensions of resilience proposed in D 1.2 (Table 10 in [37]). While the table in D.1.2 describes the dimensions in relation to five different phases of resilience, Table 35 relates the dimensions to examples of current and foreseen needs and requirements among end users that were identified in this study. The five dimensions are system/physical (technical aspects, physical/technical networks, interconnectedness), information/data (technical systems dealing with information/data), organizational/business (business-related, financial and HR aspects and organizational networks), societal/political (the broader societal/social context, indirect stakeholders) and cognitive/decision-making (perception aspects of e.g. threats and vulnerabilities).

Table 35: Current and foreseen needs and requirements among end users, in relation to five dimensions of resilience

Dimensions of resilience	Examples	Empirical support
System/physical: Technical aspects, physical/technical networks, interconnectedness	Manage related technologies outside direct control	ALPHA, BRAVO, HOTEL
	Develop systems to manage incident reports and service requests	GOLF
Information/data: Technical systems dealing with information/data	Collect and aggregate information/data at different levels and units	BRAVO, CHARLIE, DSB
	Develop big data	ALPHA
	Harmonize information/data	ALPHA, CHARLIE, FOXTROT, ECHO
Organizational/business: Business-related, financial and HR aspects and organizational networks	Decrease dependency on individual expertise	ECHO, DELTA, FOXTROT
	Integrate resilience in operational work	ECHO, HOTEL, DSB
	Allocate more resources/change the way resources are allocated	DELTA, HOTEL, DSB
	Crisis management organization, exercises and drills	ALPHA, BRAVO, CHARLIE, DELTA, ECHO
Societal/political: The broader societal/social context, indirect stakeholders	Educate and communicate with the public	DELTA, GOLF, FOXTROT, ECHO
	Involve suppliers	ALPHA, BRAVO
	Examine impact on different	FOXTROT

	stakeholders	
Cognitive/decision-making: Perceptions aspects (of e.g. threats and vulnerabilities)	Ability to make flexible responses	DELTA, ECHO
	A solid understanding of risk before moving to resilience	DSB
	Train and motivate personnel	ECHO
	Common understandings across organizations	ALPHA, BRAVO, ECHO, DSB

Needs and requirements identified with regards to the dimension *system/physical* included examples of relation to other technologies outside direct control. One example is that the increased smartness of the energy supply infrastructure (e.g. due to increased use of "non-predictable" renewable energy sources) increases the need for smart monitoring and measuring steady energy supply, which might cause increased vulnerabilities to cyber-attacks. Another example is increased dependency on digital payments in the financial industry.

The dimension *information/data* included needs and requirements to collect and aggregate information/data at different organizational levels and units. This becomes evident in the case of health care in Austria where different patient information systems are used in different states, but also in the cases of interconnected infrastructures such as the case of DSB where organizational complexity raises challenges for data collection. Develop big data is of interest to for example the financial sector. Harmonize information/data across different organizations within the critical infrastructure has been highlighted in several case studies.

With regards to the dimension *organization/business*, examples included: to decrease the dependency on individual expertise, make sure that resilience and resilience assessment is integrated in the daily work, or provide more resources to work on resilience or assessments of the same. Changing the way that resources are being allocated refers to suggestions for a risk-based strategy to determine resource allocation.

The *societal/political* dimensions are strongly linked to the respond/respond/recovery phase. In this study, the societal and political dimensions refer mostly to different types of stakeholder management. Stakeholder such as the public and suppliers are sought to be involved for different reasons. For example the public needs to be educated in terms of flooding. But it is also important to examine the impact of threats on different stakeholders, for example how farmers would be affected by disturbances in the supply of drinking water.

Cognitive/decision-making refers to perception aspects. The ability to make flexible responses in case of events beyond scenario-planning (improvised resilience) was highlighted as a need in the case of international airport of Budapest. The case of DSB illuminated the need for a solid understanding of risk before moving to resilience. Examples from the case study on the large urban industrial zone in Pančevo include the need to train and motivate personnel, both workers (which generally have low risk awareness) and personnel in the ministries (which may be inadequately trained). There is also a need to convince investors to spend money on near-real resilience assessments. The need for common understandings has been highlighted in several case studies.

In sum, this overview points for the need for indicators and tools to support the relevant actors in the investigated SCIs for a number of issues in all five dimensions in relation to the Smart Resilience project's purpose - identify, visualize and assess resilience – as a means to increase resilience, now and in the future.

6.4 *Actor analyses and stakeholder management*

Each case study presented in this report (ALPHA-HOTEL and DSB) has built on an actor analysis of the key stakeholders for the critical infrastructure(s) in focus. The actor analyses specified what organizations that play the important roles of operator, owner and regulator for the critical infrastructure in focus. The relevant organizations were found at different levels (international, national, regional and local) and of different type (public and private). The case of the health care system in Austria (CHARLIE) showed how the critical infrastructure can be analyzed in terms of individual entities and the system as a whole. In the case of the neighborhood of Heidelberg (BRAVO), a single company (SWH) was described as having a crucial importance for two critical infrastructures: energy and water.

Each organization in the critical infrastructure has in turn a number of stakeholders. The case of BRAVO illustrates an example of how SWH use a stakeholder diagram in order to consider, react and communicate with affected stakeholders, in the context of risk assessment. Stakeholder management tools are common ways in which organizations assess for example the interest and power of different stakeholders. However, this approach puts the single organization at the core of the analysis. While the organizational level of analysis is useful, this study has shown that modern critical infrastructures are highly interdependent and correlated and the benefits of viewing the infrastructure(s) as an interrelated system.

7 Conclusion and outlook

7.1 Overall conclusions

Focusing on increasingly smarter critical infrastructures (SCI), the SmartResilience project aims to identify existing "classic" Resilience Indicators (RI), to produce new "smart" RIs and to put forward a new advanced resilience assessment methodology for SCIs based on these (smart) RIs. With this new indicator-based methodology, the project seek to enable and support end users (authorities, operators and owners of critical infrastructure) to better assess the resilience of their respective critical infrastructures and, as a result, significantly improve the resilience of the same. To ensure that the resilience assessment methodology and (smart) RIs will be usable and attractive to the end users, the SmartResilience project involves its end users throughout the project.

Task 1.3 aims to, already at an early stage in the project; increase the understanding of end users' current and foreseen challenges, needs and requirements in assessing resilience of critical infrastructures and using RIs in doing so. It is seen as important to already from the start ground the development of smart RIs and the resilience assessment methodology on the end users' perspectives to ensure that they will be useful. The identification of end users' challenges, needs and requirements in assessing resilience within Task 1.3 has been guided by an actor analysis approach and is predominantly based on qualitative methods, consisting of semi-structured individual or group interviews with key stakeholders of critical infrastructures, desktop studies and literature reviews. These qualitative methods were complemented with a brief online survey. The task has covered key stakeholders of the eight critical infrastructures within the SmartResilience case studies (ALPHA-HOTEL) as well as an additional case study covering interconnected critical infrastructures (DSB).

The key findings from Task 1.3 are summarized below:

- The literature review showed how indicators can be contextualized in order to fit the end user and increase usability:
    - Designing useful indicators requires definition of the "work" that the indicators are supposed to do, or support.
    - Involving end users extensively in the process of designing indicators, in an iterative manner, allows for integrating them into existing organizational processes.
    - In interconnected infrastructures, there is a need to identify how to support coordination, information sharing, and how to construct incentives, but also how to identify the most pressing problems to address, for example through a risk-based approach.
- End users in the case studies confirmed and provided further insight into the key challenges that the project SmartResilience depart from:
    - The concept of resilience: use of the term; confusion on difference from other terms or the added value; different levels of "maturity" in assessments and indicators of resilience; and emphasis on different phases or parts of the "u-curve".
    - External threats (climate change, cyber-attacks, terrorist attacks, flooding): uncertain and different time frames; and appropriate tools for new threats.
    - The complexity of critical infrastructures: interdependencies; fragmentation/segmentation; and urbanization.
    - Data management: data and information security (sensitive data, sensitive or classified information); and abundance of data.
- End users in the case studies expressed needs and requirements in terms of assessment of resilience related to five dimensions of resilience, presented in D.1.2 [37]:

  - System/physical: manage related technologies outside direct control; develop systems to manage incident reports and service requests.
  - Information/data: collect and aggregate information/data at different levels and units; develop big data; harmonize information/data.
  - Organizational/business: decrease dependency on individual expertise; integrate resilience in operational work; allocate more resources/change the way resources are allocated; exercises and drills.
  - Societal/political: educate and communicate with the public; involve suppliers; examine impact on different stakeholders.
  - Cognitive/decision-making: ability to make flexible responses; a solid understanding of risk before moving to resilience; train and motivate personnel; common understandings across organizations.
- The survey to CoU indicates that some end users do not see the added value of assessing resilience and that respondents emphasize the need to take contextual matters into account. Moreover, the following conclusions are important to keep in mind:
  - The need for the project to create assessments and RIs that are clearly regarded as providing added value in relation to end users' current and foreseen needs.
  - The challenge to design assessments and RIs that can be widely disseminated, while at the same time taking different contexts into account.

The remaining part of this chapter describes how these findings relate to other tasks in SmartResilience and what implications this study bears for indicator development for resilience, in general and for SmartResilience.

7.2 Results in relation to other tasks in SmartResilience

7.2.1 Task 1.3 in relation to previous studies

SmartResilience Task 1.3 was designed to use the conceptual models from Task 1.1 and discuss the results of the analysis with respect to usability and limitations from T.1.2.

The relation between this study and Task 1.1 concerns the concept of resilience. This study confirms the finding put forward in D.1.1 [79] that there are a variety of usages and meanings of the concept of "resilience" (if used) and different views on the linkages between resilience and other concepts such as risk or vulnerability. While Task 1.1 focused on the many different definitions that exist in the literature, this study showed that end users also have different understandings of the term. In addition, this study showed that not all stakeholders are clear on the added value of using resilience. There are also different levels of "maturity" in assessments and indicators of resilience, and the emphasis on different phases or parts of the "u-curve" differs. This is in line with an observation from the DARWIN project, cited in D.1.1, 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*" [79].

Task 1.3 also used the definition proposed in Task 1.1 to construct interview questions and survey questions to end users. Some end users questioned the relevance of the different phases of resilience in the definition. D.1.1 [79] opens up for further evolvement of the definition of resilience and other terms during the project, and the comments from interview respondents suggests a renewed discussion within SmartResilience on how the definition could be made even more relevant to end users. Another topic that deserves further discussion in the project is to what extent the project should take into account end users' needs of determining appropriate time frames. D.1.1 proposed not including the scoping question "resilience of what time frame" in SmartResilience, since it was considered "not relevant for SmartResilience, since it is expected that the methodology and its indicators would capture the status quo and is not per se designed for a specific resilience program" ([79], p.37). However, the findings in this study suggest that determining an appropriate time frame is an important challenge to end users, especially to address threats related to climate change and/or flooding.

Task 1.2 already suggested some adjustments of the definition of resilience. In its main deliverable (D.1.2), it referred to Task 1.3 (and WP5) to further discuss "*the need to reconcile the semantic ambiguity of the concepts use in the formulas with the stakeholders*" ([37], p.154). This study has discussed this need in light of

end users' different understanding and use of the term. Furthermore, D.1.2 [37] suggested that Task 1.3 (and WP5) should address the political impact of indicators. Increasing the chances for a significant impact of the indicators is a fundamental rationale for Task 1.3 and the findings suggest that trust in the source that provides the indicators is an important factor in this regard. Finally, this report has provided examples of RIs, based on the different case studies. These RIs have not been summarized or further analyzed in this report, since it was collected and analyzed thoroughly in Task 1.2.

7.2.2 Input from Task 1.3 to forthcoming studies

Task 1.3 was designed to inform WP3 in the development of an indicator-based resilience assessment methodology as well as WP4 in the development of smart RIs. The forthcoming work on assessment methodology and indicators should recognize the variety of current uses and understandings of resilience and related concepts among end users and their "maturity"; the importance of the different contexts and what is generic and specific in different cases; the restriction in capacity and resources among end users; and the target layers for assessments and indicators (e.g. "resilience for whom?"). The implications for resilience assessment methodology and indicator development are further developed in section 7.3 below.

The cases ALPHA-HOTEL will continue to play important roles throughout the project (and be complemented with the case of INDIA which focuses on cascading effects). In particular, WP5 is largely based on the case studies, in testing the proposed resilience assessment system and validate the indicators, but the cases will also play a crucial role in e.g. Task 2.2 and Task 4.4. Task 1.3 was the first study within the project that met with informants beyond the end users included in SmartResilience, and begun to document their views on assessments of resilience. This report can serve as an input to make sure that their challenges, needs and requirements are kept in mind in order to increase the chances that indicators are made useful. The actor analyses made in each case study is also a starting point to include all relevant actors in the critical infrastructure(s). SmartResilience also has other relevant end users as partners which will be actively involved in forthcoming studies within the project, such as the insurance industry.

Task 3.1 is designed in line with the arguments in this study, in the sense that it is important to direct attention to contextual factors. Task 3.1 will delve further into specific contextual matters such as laws, regulations, organizational or institutional structures and may find interesting empirical examples that illuminate these contextual matters from the case studies in Task 1.3.

WP6 (Dissemination and Exploitation) can be informed by the actor analyses performed in this project, which mapped key stakeholders for critical infrastructures in the case studies ALPHA-HOTEL beyond project partners. Stakeholder mapping is also of interest to WP6, in the sense that these stakeholders can be seen as a target audience for the dissemination activities of SmartResilience. Task 1.3 is also a reminder that relevant individuals can be found within different functions or user groups within the identified organizations. Finally, since WP6 aims for reaching a wide audience, the tool and methods for the actor analysis approach in this study could be further developed. The actor analyses presented in this report is a result of a priority. Earlier versions of the actor analyses include even more organizations linked to each SCI that are likely to be interested in the results of SmartResilience and therefore a possible target audience.

Future research should further explore the specific new aspects brought by "smart cities": sensors, meters, communicating devices, data processing, analytics, protection, access control etc. Another topic for further study is inter-organizational collaboration and coordination triggered by increased interdependencies and interconnectedness within and between critical infrastructures. It is also important to direct future research attention to the cognitive dimension of resilience, since perceptions of crises tend to deepen the overall effect of risks.

7.3 Implications for resilience assessment methodology and indicator development

What do the results from this study imply for the further development of indicators to assess resilience? What should SmartResilience take into account to increase the chances that the assessment methodology and indicators within the project are eventually used?

SmartResilience departs from existing – "classic" – indicators that are already validated and used. In the process of identifying and developing new "smart" RIs, including those from Big Data, there is a need to make sure that the project stays in touch with what is needed among end users; not only the end users that are

part of the project. For resilience assessments and indicators to be useful to various end users, scientific expertise and theoretical insights should be complemented with empirical contextualization.

Against this backdrop, three main implications for resilience assessment methodology and indicator development are suggested:

1. *Developing indicators with an appropriate end user in mind*

   Who are the assessments and indicators developed for? Critical infrastructures typically involve several organizations, which goes well beyond the project partners in SmartResilience, as shown in the actor analyses in this study. In the cases of interconnected infrastructures, the picture is even more complex. For whom is resilience developed? What organization(s) will use the indicators? What functions (e.g. risk identification or evaluation or risk management performance) or user groups (e.g. disaster managers or urban planners) within the organization(s) will use the indicators? Should several relevant end users be identified, one should consider the possibility to aggregate indicators across different end users and levels.

   End users' interest to use indicators to assess resilience in the first place is a fundamental issue that should be considered when developing indicators. Some organizations are already quite content with the assessments that are currently available, whereas others simply do not see the value or appropriateness of assessing resilience at all. There is a need for the project to develop indicators, guidelines and methodology which provide an added value to end users' current practices, in regard to current and foreseen needs.

   Indicators should also be developed and targeted to organizations that have legitimacy to spread this practice within the critical infrastructure. This issue relates to trust in the source that provides the indicators. If there are other sources providing similar indicators, there may be a competing situation in which the end user is likely to choose to use indicators from a source that they already have a long-term reliable relationship with, such as a national regulator or standards organization.

   In sum, developing indicators with an appropriate end user in mind means posing questions such as: What organization, and what function or user group, will use it? What is their interest in using indicators? What is their legitimacy to spread the indicator in the critical infrastructure?

2. *Developing indicators in dialogue with end users*

   End users are already part of SmartResilience as project partners, but to increase the chances that the indicators are ultimately used, there is a need to also take into consideration actors that are not part of the project, yet relevant for the critical infrastructures in focus. The project should also consider end users that are not related to the critical infrastructures in the cases, but are important actors for other critical infrastructures in modern society. End user participation in indicator development allows taking into consideration the experience and knowledge by the ones that will eventually use the indicators and that they gain legitimacy within the critical infrastructure.

   Involving end users increases the ability to develop indicators which:

   - Cover areas that are important to follow up and improve in the particular critical infrastructure
   - Cover areas where there are gaps in which resilience is currently not assessed
   - Are relevant, understandable and legitimate in light of where the end users are in the process of "maturity" of assessing resilience or their current terminology
   - Are designed according to the end users' own reasons and motives for assessing resilience
   - Are designed according to what usefulness means to the end users themselves

   What works for some critical infrastructures may be less relevant for others; yet the results from this study provides preliminary suggestions of which cases in SmartResilience that share common challenges, needs and requirements. A question to bring into the project as it continues is whether SmartResilience should focus on a smaller number of contributions that are designed in line with contextual requirements, and what contributions should then be prioritized (for example, those closest to the purpose of the project or those in most need of improvement)?

In sum, when developing indicators in dialogue with end users, one should aim to increase the likelihood that they cover areas that are relevant and currently not sufficiently covered; are relevant, understandable and legitimate; and are designed according to end users' own motives for assessing resilience and perceptions of usefulness.

3. *Developing indicators in alignment with organizational processes*

The results from this study show that many needs and requirements among end users are of organizational character. This suggests that the project should develop indicators which attunes to organizational processes. Efforts should be spent to ensure that indicators:

- Are easy to understand, in order to decrease the dependency of individual expertise and decrease misunderstandings across different organizations
- Meets the level of capacity of resources that the organization(s) are willing to spend on assessments of resilience
- Allow end users to collect, process and share (big) data, taking data security into account

SmartResilience differs from many other projects in that the project does not only involve end users and stakeholders with the aim to create local support, but also to make sure that they have an active and ongoing role in project design and operation. This study has contributed to a broader understanding of the means and motives for contextualization and end user participation, in order to make the efforts spent in the project useful and a real contribution to developing more resilient European cities.

References

[1] Airmic, A., Irm, A. (2010). *Structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, The Public Risk Management Association, London, UK.

[2] Airports Council International Europe (2016). Airport Traffic Report (December Q4 and Full Year 2015), ACI, Brussels,

[3] Al-Dahidi, S., Liu, X. (2015). Resilience analysis of critical infrastructures exposed to external disturbances and affected by uncertainty. In *25th European Safety and Reliability Conference.* Zürich, Sep 7-10, 2015, CRC Press, pp. 2703-2710.

[4] Alfieri, L., et al. (2015). Ensemble flood risk assessment in Europe under high end climate scenarios, *Global Environmental Change,* vol. 35, pp. 199-212.

[5] Allet, T. (2004). Budapest 'New' EU Airport, *Airports International,* Vol 37, No. 4, pp. 37-39.

[6] American Water Works Association (2001). *Emergency Planning for Water Utilities*, Manual of Water Supply Practices, Denver.

[7] Auerswald, P., et al. (2005). The challenge of protecting critical infrastructure, *Issues in Science and Technology*, vol. 22, no. 1, pp. 77-83.

[8] Australian Government (2010). Critical Infrastructure Resilience Strategy, ISBN: 978-1-921725-25-8.

[9] Bank of England (2016).Financial market infrastructure supervision, http://www.bankofengland.co.uk/Pages/home.aspx, accessed on Sep 12, 2016.

[10] Barnett M.L., et al. (2012). Physician patient-sharing networks and the cost and intensity of care in US hospitals, *Med Care*, Vol. 50, no. 2, pp. 152-60.

[11] Bialas, A. (2016). Critical Infrastructure Protection—How to Assess the Protection Efficiency, in W. Zamojski et al. (eds.), *Dependability Engineering and Complex Systems, Advances in Intelligent Systems and Computing*, Springer International Publishing, Switzerland.

[12] Birkmann, J. (2007). Risk and vulnerability indicators at different scales: applicability, usefulness and policy implications, *Environmental Hazards*, Vol. 7, No. 1, pp. 20-31.

[13] BS EN ISO 25999-1:2006 Business continuity management Code of practice

[14] Buldyrev S. V., et al. (2010). Catastrophic cascade of failures in interdependent networks, *Nature,* Vol. 464, pp. 1025-1028.

[15] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2005). *Leitfaden für die Errichtung und den Betrieb einer Notstromversorgung in Behörden und anderen wichtigen öffentlichen Einrichtungen*, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn.

[16] Bundesministerium des Innern (2005). *Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen*, Bundesministerium des Innern, Berlin.

[17] Bundesministerium des Innern (2009). *Nationale Strategie zum Scutz Kritischer Infrastrukturen (KRITIS-Strategie)*, Bundesministerium des Innern, Berlin.

[18] Bundesministerium des Innern (2011). *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement / Leitfaden für Unternehmen und Behörden*, Bundesministerium des Innern, Berlin.

[19] Bundesverband der Energie- und Wasserwirtschaft e.V. (2012). Smart grids in Deutschland, BDEW Bundesverband der Energie- und Wasserwirtschaft e.V, Berlin.

[20] City of Heidelberg (2016). Bahnstadt. http://www.heidelberg.de/hd,Lde/HD/Rathaus/Ziele.html, Accessed Oct. 14, 2016.

[21] COM (2014) 2015. Communication from the Commission on effective, accessible and resilient health systems.

[22] Egli, T. (1999). *Richtlinie Objektschutz gegen Naturgefahren*. Gebäudeversicherungsanst. des Kantons St. Gallen, St. Gallen.

[23] Federal Emergency Management Agency (2011). *Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Building and Infrastructure Protection Series FEMA 426, Federal Emergency Management Agency.

[24] Federal office of civil protection and disaster resilience (2016). Homepage, http://www.bbk.bund.de/EN/Home/home_node.html, accessed on Oct. 17, 2016.

[25] Fenstad, J. (2012). Organizational Challenges Regarding Risk Management in Critical Infrastructures, In: Hokstad, P., Utne, I.B., Vatn, J. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer-Verlag, London

[26] Grieshaber, K. (2004). Germany: Sentencing In 1991 Attack On Jews, *New York Times*, Sept. 29, 2004, World Briefing.

[27] Gustin J. F. (2004). *Disaster & Recovery Planning: A Guide for Facility Managers,* The Fairmont Press Inc., Lilburn. IBSN-10: 0-88173-640-6.

[28] Heidelberg-Bahnstadt (2016). Portrait of Bahnstadt, http://heidelberg-bahnstadt.de/en/portrait-bahnstadt, accessed on Oct. 10, 2016.

[29] Helen (2016). Energy Production, https://www.helen.fi/en/helen-oy/about-us/energy-production/, accessed on Sep. 20, 2016.

[30] Helen (2016-09-08). Telephone interview

[31] Hernantes, J., et al. (2013). Learning before the storm: Modeling multiple stakeholder activities in support of crisis management, a practical case, *Technological Forecasting and Social Change*, Vol. 80, No. 9, pp.1742-1755.

[32] Herrera, I. A., Hollnagel, E., Håbrekke, S. (2010). Proposing safety performance indicators for helicopter offshore on the Norwegian continental shelf. In *PSAM 16 - 10th International Conference on Probabilistic Safety Assessment and Management*. Seattle, June 7-11, 2010, pp. 10.

[33] Innenministerium Baden-Württemberg und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2010). Krisenhandbuch Stromausfall. Langfassung. Krisenmanagement bei einer großfl ächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg, Innenminesterium Baden-Würtenberg, Stuttgart.

[34] ISO 31000:2009 Risk management.

[35] ISO/IEC 27001:2013 Information security management.

[36] Janic, M. (2000). An assessment of risk and safety in civil aviation, *Journal of Air Transport Management,* Vol. 6, No. 1, pp. 43-50.

[37] Jovanovic, A., et al. (2016). SmartResilience D1.2: Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[38] Jungbluth, F. (2005). *Recht & Haftung für technische Manager. Grundlagen, Aufbau und Methoden eines effektiven Notfallmanagements*, Euroforum Verlag, Düsseldorf.

[39] Kalakou, S., Psaraki-Kalouptsidi, V., Moura, F. (2015). Future airport terminals: New technologies promise capacity gains, *Journal of Air Transport Management*, Vol. 42, pp. 203-212.

[40] Landon B.E. (2012). Variation in patient-sharing networks of physicians across the United States, *JAMA*, Vol. 308, No. 3, pp. 265-73.

[41] Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience, *Natural Hazards Review*, Vol. 14, No. 1, pp. 29-41.

[42] Lee, WK. (2006). Risk assessment modeling in aviation safety management, *Journal of Air Transport Management*, Vol. 12, No. 5, pp. 267-273.

[43] London Economic Plan and Major Industries (2016). London's financial industry, http://www.uncsbrp.org/finance.htm, accessed on Sep 30, 2016.

[44] Martin, EG., Helbig, N., Shah, NR. (2014). Liberating data to transform health care, *JAMA*, Vol. 311, No. 24, pp. 2481-2.

[45] National Emergency Supply Agency (2009). Operational Continuity Management.

[46] National Emergency Supply Agency (2016). Organisation, http://www.nesa.fi/organisation/ , accessed on Sep. 20, 2016.

[47] National Emergency Supply Agency (2016). HUOVI-portaali, http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/huovi/, accessed on Sep. 20, 2016.

[48] National Emergency Supply Agency (2016). Security of Supply, http://www.nesa.fi/security-of-supply, accessed on Sep. 20, 2016.

[49] National Emergency Supply Agency (2016). Sopimuksiin perustuva varautuminen – SOPIVA, http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/ , accessed on Sep. 20, 2016.

[50] National Emergency Supply Agency (2016-09-30). Telephone interview

[51] NFPA 1600:2004 Standard on Disaster/Emergency Management and Business Continuity

[52] Norwegian Directorate for Civil Protection (2012). *Sikkerhet i kritisk i infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*, KIKS-prosjektet, Norwegian Directorate for Civil Protection, Tønsberg.

[53] Norwegian Directorate for Civil Protection (2015). *HarbourEx15*, Norwegian Directorate for Civil Protection, Tønsberg.

[54] Norwegian Directorate for Civil Protection (2015). *Risavika – helhetlig risikostyring i områder med forhøyet risiko*, Norwegian Directorate for Civil Protection, Tønsberg.

[55] Norwegian Directorate for Civil Protection (2015*). Sydhavna (Sjursøya) – an area with increased risk*, Norwegian Directorate for Civil Protection, Tønsberg.

[56] NOU 2006:6 - Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.

[57] NOU 2012:14 - Rapport fra 22. juli-kommisjonen.

[58] Österreichisches Bundesministerum für Gesundheit (2013). *The Austrian health care system, key facts*, Österreichisches Bundesministerum für Gesundheit, Vienna.

[59] Pham, HH., et al. (2016). Primary care physicians' links to other physicians through medicare patients: the scope of care coordination, *Annals of Internal Medicine*, Vol. 150, pp. 236-42.

[60] Price, J., Forrest, JS. (2016). *Practical Airport Operations, Safety, and Emergency Management*, Butterworth-Heinemann, Oxford. IBSN: 978-0-12-800515-6.

[61] Prior, T., & Hagmann, J. (2014). Measuring resilience: Methodological and political challenges of a trend security concept, *Journal of Risk Research*, Vol. 17, No. 3, pp. 281-298.

[62] Roe, E., Schulman, P.R. (2012). Toward a Comparative Framework for Measuring Resilience in Critical Infrastructure Systems, *Journal of Comparative PolicyAnalysis: Research and Practice*, Vol. 14, No. 2, pp. 114-125.

[63] Sahebjamnia, N., Torabi, AS., Mansouri, SA. (2015). Integrated business continuity and disaster respond/recovery planning: Towards, *European Journal of Operational Research*, Vol. 424, No. 1, pp. 261-273.

[64] Schneeweiss, S. (2014). Learning from big health care data. New England Journal of Medicin, Vol. 370, pp. 2161-3.

[65] Silipä, J. (2013). Emerging risk issues in underground storage of bituminous coal, Doctoral dissertation, Aalto University.

[66] SOU 2007:60 - Climate and Sustainability Inquiry.

[67] SOU 2016:32 - Drinking Water Inquiry.

[68] Stadtwerke Heidelberg (2016). Profile, https://www.swhd.de/de/SWH/Unternehmen/Profil/Die-Stadtwerke-Heidelberg_163643.html, accessed on Oct. 10, 2016.

[69] Sudmeier, K. I., Jaboyedoff, M., & Jaquet, S. (2013). Operationalizing "resilience" for disaster risk reduction in mountainous Nepal, *Disaster Prevention and Management*, Vol. 22, No. 4, pp. 366-377.

[70] Swedish Civil Contingencies Agency (2014). *Övergripande inriktning för samhällsskydd och beredskap*, Rapportnummer MSB708, Swedish Civil Contingencies Agency.

[71] Swedish Civil Contingencies Agency (2016). *Nationell risk- och förmågebedömning 2016*, Diarienummer 2015-1467, Swedish Civil Contingencies Agency.

[72] Tamasi, G., Demichela, M. (2011). Risk assessment techniques for civil aviation security, *Reliability Engineering & System Safety*, Vol. 96, No. 8, pp. 892-899.

[73] UK Financial Authorities (2013). *2012 Resilience Benchmarking*, Bank of England, Her Majesty's Treasury & Financial Conduct Authority, London.

[74] UK Financial Authorities (2013). *Technology and Cyber Resilience Benchmarking Report 2012*, Bank of England, Her Majesty's Treasury & Financial Conduct Authority, London

[75] Umweltbundesamt Bundesrepublik Deutschland (2001). *Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitungen*. Nr. 10: Betriebliche Alarm- und Gefahrenabwehrplanung.

[76] Umweltbundesamt Bundesrepublik Deutschland (2001). *Checklisten für die Untersuchung und Beurteilung des Zustandes von Anlagen mit wassergefährdenden Stoffen und Zubereitu*ngen. Nr. 11, Hochwassergefährdete Anlagen.

[77] Vähäaho, I. (2014). Underground space planning in Helsinki, J*ournal of Rock Mechanics and Geotechnical Engineering,* Vol 6, pp. 387-398.

[78] Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports, *Public Administration*, Vol. 89, No. 2, pp. 381-400.

[79] Vollmer, M., et al. (2016). SmartResilience D1.1.: Initial Framework for Resilience Assessment, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[80] Zentrum für Alpine Umweltforschung (2000). Leitfaden für erdbebensicheres Bauen, Sion.

ANNEXES

Annex 1 Actor Analysis Template 90
Annex 2 List of respondents 1
Annex 3 Interview protocol 3
Annex 4 Interview guidelines 4
Annex 5 Information sheet and consent form 6
Annex 6 Survey to CoU 9
Annex 7 Related projects from an end user perspective 11
Annex 8 Review process 16

Annex 1 Actor Analysis Template

Template actor analysis

Task 1.3. SmartResilience

Table 1

Case study:	
City/country:	
Smart Critical Infrastructure:	

Table 2

Guiding questions	Name of organization (original language)	Name of organization (English)	Level	Type	Role/responsibility in case study*	Priority for interview	Proposed contact person(s)	Other information
What organization is the governmental representative with responsibility for the country's overall emergency management, distaster reduction or resilience?								
What organization(s) operates the critical infrastructure in focus for this case study?								

What organization(s) owns the critical infrastructure in focus for this case study?								
What organization(s) regulates the critical infrastructure in focus for this case study? (e.g. policy development, supervision etc).								
What other organization(s) has an important stake in the critical infrastructure for this case study?								

Annex 2 List of respondents

Case study	Organization	Date of interview	Mode of interview	Type of interview
ALPHA	Worldpay	Sept 13, 2016	Telephone	Individual
ALPHA	Lloyds	Sept 15, 2016	Telephone	Group
ALPHA	Lloyds	Sept 15, 2016	Telephone	Group
BRAVO	Stadtwerke Heidelberg Netze	Aug 25, 2016	Face-to-face	Individual
CHARLIE	General Hospital Vienna	Aug 26, 2016	Face-to-face	Individual
CHARLIE	Main Association of Social Security Institutions	Sept 12, 2016	Face-to-face	Individual
CHARLIE	Medical University of Vienna	Sept 12, 2016	Face-to-face	Individual
ECHO	Ministry of Agriculture and Environmental Protection	Aug 2, 2016	Face-to-face	Group
ECHO	Ministry of Agriculture and Environmental Protection	Aug 2, 2016	Face-to-face	Group
ECHO	Ministry of Agriculture and Environmental Protection	Aug 2, 2016	Face-to-face	Group
ECHO	Ministry of Interior affairs	Aug 29, 2016	Face-to-face	Group
ECHO	Ministry of Interior affairs	Aug 29, 2016	Face-to-face	Group
ECHO	Pančevo City-City Administration	Aug 10, 2016	Face-to-face	Group
ECHO	Pančevo City-City Administration	Aug 10, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	HIP Petrohemija	Aug 11, 2016	Face-to-face	Group
ECHO	NIS j.s.c. Novi Sad	Aug 15, 2016	Face-to-face	Individual
DELTA	Budapest Airport	Sep 16, 2016	Face-to-face	Group
DELTA	Budapest Airport	Sep 16, 2016	Face-to-face	Group
DELTA	National Transport Authority	Sep 16, 2016	Face-to-face	Group
DELTA	National Transport Authority	Sep 16, 2016	Face-to-face	Group

Case study	Organization	Date of interview	Mode of interview	Type of interview
DELTA	NUPS Institution for Disaster Management	Sep 16, 2016	Face-to-face	Group
DELTA	National Security Agency	Sep 16, 2016	Face-to-face	Group
DELTA	National Security Agency	Sep 16, 2016	Face-to-face	Group
DELTA	Counter-terrorism Center	Sep 16, 2016	Face-to-face	Group
DELTA	HungaroControl	Sep 16, 2016	Face-to-face	Group
DELTA	National Disaster Management	Sep 16, 2016	Face-to-face	Group
FOXTROT	Stockholm Water	Sep 16, 2016	Telephone	Individual
FOXTROT	Norrvatten	Sept 13, 2016	Telephone	Individual
FOXTROT	Swedish Civil Contingencies Agency	Sept 13, 2016	Telephone	Individual
FOXTROT	Swedish National Food Agency	Sept 8, 2016	Telephone	Individual
GOLF	Cork City Council	Sep 19, 2016	Face-to-face	Individual
GOLF	Cork City Council	Sep 19, 2016	Face-to-face	Individual
GOLF	Cork City Council	Sep 19, 2016	Face-to-face	Individual
GOLF	Cork City Council	Sep 19, 2016	Face-to-face	Individual
HOTEL	Helen Energy Company	Sept 8, 2016	Telephone	Individual
HOTEL	National Emergency Supply Agency	Sept 30, 2016	Telephone	Individual
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group
DSB	Norwegian Directorate for Civil Protection	Sept 20, 2016	Face-to-face	Group

Annex 3 Interview protocol

INTRODUCTION

This introduction aims to inform the respondent about the project and the aim of the interview. This information will also be provided in the letter of consent that the respondents should receive before the interview. Feel free to adapt this introduction to your own preference.

About the project SmartResilience

This is a research study conducted as part of the SmartResilience project, funded within the EU research and innovation program Horizon 2020. The purpose of the study is to deliver best-practice solutions and identifying the early warnings, improving resilience (*i.e. ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption*) of "smart" critical infrastructures against new threats and cascading and ripple effects.

Modern critical infrastructures are becoming increasingly "smarter" (e.g. cities). Making the infrastructures "smarter" usually means making them smarter in normal operation and use: more adaptive, more intelligent… But will these smart critical infrastructures behave equally "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 smart critical infrastructures regarding its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? These are the main questions tackled by SmartResilience.

The project defines resilience of an infrastructure as "the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption."

About the interview

This interview is part of a task in SmartResilience that aims at identifying end user's challenges, needs and requirements for assessing resilience (i.e. *the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption)* in critical infrastructure such as [*this critical infrastructure*].

The interview intends to cover how issues of resilience are addressed with regard to [*this critical infrastructure*]. The interview will be based on an interview guide, which is a list of questions related to resilience. We will not necessarily follow this in a strict order, but rather try to make the interview an informal conversation about the topic of resilience. We regard the interview protocol as a checklist, or reminder about important issues to cover.

Your input will feed into a report where the challenges, needs and requirements concerning a number of critical infrastructures in Europe will be described, based on interviews from case studies in eight European countries.

Annex 4 Interview guidelines

INTRODUCTION

The interviews can be made by phone or face-to-face. It can be made in the language of your choice. Before the interview, you should have sent out:

1. An invitation letter (to initiate contact and decide on an appointment).
2. A letter of consent (to be signed either before or at the time of the interview).
3. The interview protocol with interview questions.

Your role as an interviewer is to guide the interviewee through a set of questions provided in the interview protocol, without biasing the interviewee's responses. Your mission as an interviewer is organized around four stages:

1. Opening up the interview
2. Administering the questions
3. Closing the interview
4. Summarizing and analyzing the interview

STAGE 1 - OPENING UP THE INTERVIEW

When preparing the interview, please follow the steps below:

1. Have the material ready. Bring all relevant materials with you - typically, a notebook, pen, and any recording equipment (audio) needed. Ensure that your recording option (note-taking, taping) is workable in the context in which you will be doing the interview (either by phone or face-to-face).

2. Choose a setting with little distraction. Avoid loud lights or noises, ensure the interviewee is comfortable.

3. Explain the purpose of the interview. You find some brief information in the introduction of the interview protocol.

4. Address terms of confidentiality. Clearly convey terms of confidentiality regarding:

a. Access to interview material. Explain that only the project team will get access to the interviewee's answers and that his/her answers will be analyzed and used for a report.

b. Informed consent. Get the interviewee's written permission to use their comments in the study by asking them to sign the letter of consent (unless already done before the interview).

c. Right to review. Explain that in case we want to use a quote based on the interview, we will send the proposed text to the interviewee for revision before the report is published. In other words, the interviewee will be given the opportunity to review the results, and have the option to amend your input.

d. Anonymity. Explain that we will not reveal any individual names in the report. In case a quote is used, we will refer to the organization that the respondent represents

e. Access to results. The report will be published in the fall 2016.

5. Indicate how long the interview usually takes. The interview should take about 45 minutes.

6. Ask them if they have any questions before you both get started with the interview.

7. Do not count on your memory to recall their answers. Ask for permission to record the interview or bring along someone to take notes.

It can be useful to consider including an additional interviewer. Ideally, this second interviewer can also help with note-taking while the first interviewer focuses on questions. A second interviewer can also be an expert on a specific domain touched by the interview and be the person asking questions related to that. The additional interviewer can also help provide perspective after the interview is complete to be sure that all the relevant information is included in the minutes and to clarify any doubtful points.

STAGE 2 - ADMINISTERING THE QUESTIONS

Following the interview protocol to the extent that this is possible, you should ask the interviewee the questions, while recording their answers by hand, or by an audio recorder. If the interviewee cannot answer a question, move on to the next question. The interview is of a semi-structured structure with the openness to ask more specific follow-up questions relevant for the specific critical infrastructure.

Pay close attention to the emerging themes, perspectives, opinions, and underlying logic which is being elicited in the interviewee's answers – all of these should be noted. And do not be afraid to ask the interviewee to provide further clarifications on any aspects of his/her answer that might seem unclear or inconsistent with previous statements.

STAGE 3 – CLOSING THE INTERVIEW

At the end of the interview protocol, you should ask the interviewee whether he/she has anything further to add.

Always thank the interviewee for his/her time, involvement and cooperation at the end of the interview.

STAGE 4 – SUMMARIZING AND ANALYZING THE INTERVIEW

Immediately after closing down the interview, take time to expand or complete any notes you made during the session, possibly with the help of the additional interviewers, if any.

The notes of the interview will be valuable material for you when providing the input from the case study to the report. However, the task leader will not require the notes from the interviews.

The input to the report shall be written in English and structured according to the report template. The input shall be sent to the task leader (katarina.buhr@ivl.se) according to the agreed time schedule.

Annex 5 Information sheet and consent form

Informed Consent Form and Information Sheet
for participation in SmartResilience study

The purpose of this document is to obtain your informed consent to participate in a SmartResilience study and inform you about what your participation entails. Please read this information sheet carefully and ask as many questions as you like before you decide whether you want to participate in this research study. You are free to ask questions (and entitled to understandable answers) at any time before, during, or after your participation in this research. Participation is voluntary.

Project Information

Project Title:
SmartResilience

Project Duration:
2016-2019

Principal Investigator:
Prof. Dr. Aleksandar Jovanovic

Coordinator:
European Virtual Institute for Integrated Risk Management
Lange Straße 54, 70174 Stuttgart, Germany
Tel: +49 71141004129
E-mail: jovanovic@eu-vri.eu

PURPOSE OF THIS RESEARCH STUDY

You are being asked to participate in a research study conducted as part of the SmartResilience project. The purpose of the study is to deliver best-practice solutions and identifying the early warnings, improving resilience of smart critical infrastructures (SCIs) against new threats and cascading and ripple effects.

Modern critical infrastructures are becoming increasingly “smarter” (e.g. cities). Making the infrastructures “smarter” usually means making them smarter in normal operation and use: more adaptive, more intelligent etc. But will these SCIs behave equally “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? These are the main questions tackled by SmartResilience.

2. PROCEDURES

Your participation in this study involves being interviewed about end user’s challenges, needs and requirements for assessing resilience in critical infrastructures. The interview intends to cover how your organization addresses issues of resilience with regard to a critical infrastructure. The project is interested in your knowledge and experience about working with resilience (if you do) and other related concepts. Your input will feed into a report where the challenges, needs and requirements concerning a number of critical infrastructures in Europe will be described, based on interviews from case studies in eight European countries.
The interview should take about 45 minutes of your time to complete and interview questions will be sent to you prior to the interview as to familiarize yourself with the questions.

3. RISKS

There are no risks associated with your participation in this research study. No sensitive or personal information will be required or sought from participants. Personal data will not be passed on to any other party; the collected data will only be evaluated in a means which ensures the anonymity of the participant.
Any new information developed during the SmartResilience study that may affect your willingness to continue participation will be communicated to you.

4. OWNERSHIP AND DOCUMENTATION OF INFORMATION

Your personal identity will be kept completely anonymous. Your answers will be separated from any information from which your identity may be determined. You will be given the opportunity to review the results of this interview, and have the option to amend your input.
Any and all data gathered as a result of these participatory exercises will be retained in full accordance with the relevant national regulations and legislation regarding data protection. No confidential, sensitive or personal information will be required or sought from participants. This data will only be retained for the maximum period of time for which it is required, during which time it will be stored in as secure a manner as is possible, and following this will be deleted. Anonymity will thus be guaranteed and personal data will not be passed on to any other party; the collected data will only be evaluated in a means which ensures the anonymity of the participant.

5. POSSIBLE BENEFITS

By participating in this research, you will be making an important contribution to the development of exciting and innovative approaches for safer, more resilient urban infrastructure. You may also gain knowledge and insight on innovative approaches that are being developed for more resilient urban environments.

6. FINANCIAL CONSIDERATIONS

There is no financial compensation for your participation in this research.

7. AVAILABLE ALTERNATIVES

N/A

8. CONFIDENTIALITY

Your identity in this study will be treated as confidential. The results of the study, including any data, may be published for scientific purposes but will not give your name or include any identifiable references to you or the location therein.
However, any records or data obtained as a result of your participation in this study may be inspected by the European Commission, by any relevant agency, by the SmartResilience Steering Committee, or by the persons conducting this study (provided that such inspectors are legally obligated to protect any identifiable information from public disclosure, except where disclosure is otherwise required by law or a court of competent jurisdiction.) These records will be kept private in so far as permitted by law.

9. TERMINATION OF RESEARCH STUDY

You are free to choose whether or not to participate in this SmartResilience project study. You will be provided with any significant new findings developed during the course of this study that may relate to or influence your willingness to continue participation.
If at any time during or after the study you wish for your data to be deleted from dataset, you may contact the coordinator:

Prof. Dr. Aleksandar Jovanovic
European Virtual Institute for Integrated Risk Management
Lange Straße 54, 70174 Stuttgart, Germany
Tel: +49 71141004129
E-mail: jovanovic@eu-vri.eu

Annex 6 Survey to CoU

SmartResilience
Smart Resilience Indicators for Smart Critical Infrastructures

Survey to the Community of Users

This survey is part of a task within SmartResilience that aims at identifying end user's challenges, needs and requirements for assessing resilience in critical infrastructures. The survey aims to increase the project's understanding of how potential users assess the **usefulness of current assessments of resilience** and what can be done to improve these. The survey only takes a few minutes to fill in.

Please, base your input of your own opinion. Your response will remain anonymous. The overall result from the survey will feed into a report where the challenges, needs and requirements concerning a number of critical infrastructures in Europe will be described.

Deadline for your responses are October 7th.

Thank you for your valuable contribution!

Yours sincerely,

Johan M. Sanne, IVL Swedish Environmental Research Institute

johan.sanne@ivl.se

Tel. +46 10 788 66 59

The SmartResilience project defines resilience of an infrastructure as "the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption."

1. Do you have professional experience of working with any of the following concepts or models:

	No experience	Limited experience	Substantial experience	Don't know
Resilience	◻	◻	◻	◻
Risk management	◻	◻	◻	◻
Business Continuity	◻	◻	◻	◻
Other	◻	◻	◻	◻

If other, please state which

2. In your opinion, how does resilience compare to the following approaches in terms of usefulness?

Resilience models are……

	Less useful	About as useful	More useful	Don't know
Risk management	◻	◻	◻	◻
Business continuity	◻	◻	◻	◻
Other	◻	◻	◻	◻

If other, please state which

3. In your opinion, how useful are current assessments of the following phases of resilience?

	Not useful at all	Somewhat useful	More useful than not	Very useful	Assessment not available	Don't know
Ability to understand risks	◻	◻	◻	◻	◻	◻
Ability to anticipate changing conditions	◻	◻	◻	◻	◻	◻
Ability to prepare for changing conditions	◻	◻	◻	◻	◻	◻
Ability to adapt to changing conditions	◻	◻	◻	◻	◻	◻
Ability to withstand disruption	◻	◻	◻	◻	◻	◻
Ability to respond to disruption	◻	◻	◻	◻	◻	◻
Ability to recover rapidly from disruption	◻	◻	◻	◻	◻	◻

Comments?

4. In your opinion, what is needed to improve current assessments of resilience?

Annex 7 Related projects from an end user perspective

Project name, funder and time	Project description	End user engagement: who and how	Comment in view of T1.3.
PREDICT – PREparing for the Domino Effect in Crisis situations **Horizon 2010** **April 2014 – (ongoing)**	PREDICT solution: methodologies, models and software tools. Increase the awareness and understanding of cascading effects by crisis response organizations, enhance their preparedness and improve their response capability to respond in case of cascading failures.	Partners include crisis management and critical infrastructure organizations and assessing the work done based on their operational expertise Members of the Advisory Board: External experts from civil protection organizations, national ministries, and critical infrastructures Series of iterative workshops around three use cases	Very similar end users as SmartResilience would like to engage Interim and final results of tool developments will be offered for evaluation by end users using workshops Serious ambition to contextualize final products to be used
EWENT – Extreme Weather impacts on European Networks of Transport **FP7** **2010-2012**	Assess the impacts and consequences of extreme weather events on EU transport system	Some end user partners Estimation of impacts and consequences of hazards – based on empirical experiences and applied to scenarios Stakeholder interviews and innovations seminar	Focused on finding cost-effective solutions No contextualized end user products
RESILENS – Realising European ReSILiencE for Critical Infrastructure **Horizon 2020** **April 2015 – (ongoing)**	European Resilience Management Guideline to support the practical application of resilience to all CI sectors.	Key stakeholders from various CI Stakeholder consultation around concepts of resilience Current resilience state of practice in stakeholder organizations Indicating potential impact of developed tools on stakeholder organizations.	Similar purpose and methods as SmartResilience Preliminary findings similar to the results from case studies in Task 1.3
ANYWHERE – EnhANcing emergencY	Develop tools to support decision-makers in real-time coordination of	Presents their work to the CoU of Safe, Secure and Resilient Societies	Not clear how end users' needs are included in specification phase

management and response to extreme WeatHER and climate Events Horizon 2020 June 2016 – (ongoing)	emergency management during extreme weather and climate events Adaptation to local needs and requirements Show the actual improvement of the end user operational capabilities	User-driven pilot sites implementation and demonstration Market uptake ensured by cooperation with an SME and Industry Collaborative Network	
BroadMap - Mapping Interoperable EU PPDR Broadband Communication Applications and Technology Horizon 2020 May 2016 – (ongoing)	Collect and validate the Public Protection and Disaster Relief organizations' existing requirements Developing: specifications, roadmap for procurement, broadband applications and interoperable radio communication solutions	A large number of public stakeholders Using a series of end user workshops around Europe	Similar approach as in SmartResilience
IMPROVER - Improved risk evaluation and implementation of resilience concepts to critical infrastructure Horizon 2020 June 2015 – (ongoing)	Improve European critical infrastructure resilience to crises and disasters through the implementation of resilience concepts to real life examples of pan-European significance	Stakeholders not consulted: First responders, owners of large complex facilities and inhabitants Pilot implementation of methodology in two living labs	Unclear how tools are validated regarding end user' needs
ResiStand - Increasing disaster Resilience by establishing a sustainable process to support Standardization of technologies and services Horizon 2020, May 2016 – (ongoing)	Develop a new, sustainable process to improve and support future standardization work	Standards Advisory Group, End User Community Supplier Community Identification of standardization needs and requirements through desktop, surveys and workshops	Similar approach as in SmartResilience
STORM - Safeguarding Cultural Heritage through Technical and Organisational Resources Management Horizon 2020 June 2016 –	Determine how different vulnerable materials, structures and buildings are affected by different extreme weather events together with risks associated to climatic conditions or natural hazards	Partners include heritage site organizations and rescue organizations Capturing of STORM system and user requirements. In-field evaluation of prototypes Scenarios and requirements tested	Unclear methods for end user involvement

(ongoing)	Offering improved, effective adaptation and mitigation strategies, systems and technologies.		
HERACLES – Heritage Resilience against Climate Events on Sites Horizon 2020 May 2016 – (ongoing)	Design, validate and promote responsive systems/solutions for effective resilience of CH against climate change effects Involvement of different expertise's (end users, industry/SMEs, scientists, conservators/restorers and social experts, decision, and policy makers)	End users are project partners Advisory board with end users	Unclear methods for end user involvement
SMR – Smart Mature Resilience Horizon 2020 June 2015 – (ongoing)	Resilience Management Guideline to support city decision-makers in developing and implementing resilience measures in their cities.	Cities part of consortium, working closely with research partners to develop and validate tools through pilot activities Workshops for various issues with city experts	The specific inputs from end user engagement difficult to discern in requirements report
BRIGAID – BRIdges the GAp for Innovations in Disaster Resilience H2020 May 2016 – (ongoing)	Provide integral support for innovations for climate adaptation, focusing on climate-driven disasters like floods, droughts and extreme weather.	Innovators and Communities of Innovation	Unclear methods for end user involvement
RESCCUE – RESilience to Cope with Climate Change I Urban arEas H2020 May 2016 – (ongoing)	Provide practical and innovative models and tools to end users facing climate change challenges to build more resilient cities	City managers and Urban system operators	Unclear methods for end user involvement
PREEMPTIVE - PREventivE Methodology and Tools to protect utilitIEs FP7 March 2014 – (ongoing)	Identify and evaluate 'Hybrid Risk Metrics' for assessing and categorizing security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms		Not relevant for SmartResilience

DRIVER - Driving Innovation in Crisis Management for European Resilience **FP7** **October 2014**	Design and develop prevention and detection tools Define guidelines for improving Critical Infrastructure (CI) surveillance	End user advisory board support with: Definition of operational requirements and scenarios Testing, validating and assessing the results of the research activities	Unclear methods for end user involvement
HARMONISE - A Holistic Approach to Resilience and SysteMatic ActiOns to Make Large Scale UrbaN Built Infrastructure Secure **FP7** **2013-2016**	Improving civil society resilience Strengthening first responders Training and learning solutions	A strong focus is set on the needs and requirements of the DRIVER platform providers and connected end users Testbeds Experiments	Unclear methods for end user involvement Unclear conclusions to be learned for SmartResilience in terms of end user needs and requirements
CRISMA - Modelling crisis management for improved action and preparedness **FP7** **2012-2015**	Concept to improve the security and resilience of this infrastructure, encompassing the design and planning phases of such projects	Three cities are partners HARMONISE tools used by a variety of potential end users from planners, construction teams, designers, to security teams	Stakeholder interviews – focused on in advance specified tools The source of needs and requirements often unclear in requirements report
AFTER – A Framework for electrical power systems vulnerabilities identification, defense and restoration **FP7** **2011-2014**	Simulation-based decision support system, for modelling crisis management, improved action and preparedness.	No local communities as partners National crisis management agencies or the like are partners	Unclear methods for end user involvement
DARWIN - Expecting the unexpected and know how to respond **H2020** **June 2015 – (ongoing)**	Methodology and tool for the integrated, global vulnerability analysis and risk assessment of the interconnected Power Systems considering interdependencies with ICT	Two grid operators are partners Advisory board with additional grid operators	Unclear methods for end user involvement The source of needs and requirements often unclear in requirements report
HiPoW – Protection of Critical Infrastructures against High	European resilience management guidelines aimed at policy makers, service providers and first responders. The guidelines	Designated Community of Practitioners serve as forum to encourage information sharing amongst infrastructure operators,	Unclear methods for end user involvement The source of needs and requirements often unclear in requirements

Power Microwave Threats **FP7** **2012-2016**	will be user-friendly, accessible and dynamic, allowing those in the crisis community to comprehend and digest them in times of crisis. Develop a holistic regime for protection of critical infrastructures against threats from electromagnetic radiation. Assist the embryonic European policy on protection of critical infrastructures to mature. Reducing Critical infrastructures vulnerabilities regarding EMP/HPM threats.	policy makers and other stakeholders. End user group	report

Annex 8 Review process

Points raised by reviewers and task leader's response

Reviewer's point	Task leader's response
Reviewer 2	
The executive summary misses out some important findings presented on page 59 results section 5 are missing, 76. 68 and 69. The summary and the conclusions are good but the content is missing in the executive summary. I would also mention that some actors do not see a need to develop Resilience KPIs because current practices seem to be sufficient.	The executive summary has been rewritten to include and elaborate on the findings pointed out by the reviewer: the results from the survey to CoU (p.59, section 5) and the implications for resilience assessment methodology and indicator development (pp.68-69). A text has also been added to the executive summary to describe that some actors do not see a need to develop Resilience KPIs because current practices seem to be sufficient. With regards to p.76, it is "Annex I: Actor Analysis Template" which contains no findings. However, when scrolling the document, Word shows p.76 for p.68. Therefore, p.76 has been interpreted as a typo which is why the reviewer's request to include findings from this page number has been ignored.
p.4, 2nd paragraph: The referral to tasks 1.1. 1.2. etc. makes it cumbersome to read, please indicate content of tasks.	The paragraph has been rewritten to indicate the content of the tasks mentioned in order to make it more reader friendly.
p. 4, Fig 1: Fonts too small, not readable.	The figure has been replaced with a sharper (identical) figure and increased in size, in order to make it more readable.
p. 5: Unclear section about end-user and stakeholder.	The section has been clarified. It now focuses on the main distinction in the report between end user and stakeholder.
p.5, outline: What shall task 1.3. deliver, unclear section.	What task 1.3 shall deliver is clearly explained in section 1.2: "About Task 1.3 and relationship to other tasks/WPs". The section on p.5 (outline) is devoted to giving an outline of the report and explains the allocation of responsibilities within T1.3.
p.25, Fig 7: Too small fonts, not readable.	The figure has been deleted, since it was not vital.
P. 63, Table 14: Comments are actually the needs indicated in the title.	The column "Comments" has been merged with the column "Dimensions of resilience". The content of both these columns have been extracted from D.1.2, as explained in the text. The column "Comments" was simply an explanation of each dimension of resilience from D.1.2.
p. 65, Fig 19: Makes only sense if you group the	The figure, and its corresponding explanatory text,

actors into the matrix, otherwise I do not see the value in showing this matrix.	has been deleted. Instead, the following shorter text has been included, in order to relate actor analysis to stakeholder management: "Each organization in the critical infrastructure has in turn a number of stakeholders. The case of BRAVO illustrates an example of how SWH use a stakeholder diagram in order to consider, react and communicate with affected stakeholders, in the context of risk assessment. Stakeholder management tools are common ways in which organizations assess for example the interest and power of different stakeholders. However, this approach puts the single organization at the core of the analysis. While the organizational level of analysis is useful, this study has shown that modern critical infrastructures are highly interdependent and correlated and the benefits of viewing the infrastructure(s) as an interrelated system."
I would strongly recommend to add an overview about the entire project, e.g. p.30/131 Project description version of August 17, 2015) to make it clear that this report belongs to WP1 and should clarify the starting position.	An overview of the project structure has been added (in text) to the introduction, with a clear reference to T 1.3 as part of WP1. No explanatory figure has been added as it risks taking too much focus from the aims of the task.
In addition, the 9 case studies revealed a multitude of resilience KPI's. I would recommend to collect them and show them based on the case studies the originate (example p.33 Delta Budapest Airport: Quantitative Resilience KPI i.e. time measurement, Qual: Level 3 Priority Scale) or page 42 Foxtrot KPI Sustainable capacity, Redundancy and raw water quality. or: GOLF: p.48 System KPI for resilience: tidal flood event advisory system, avoid developments in floodplains, invest in infrastructure...	Resilience indicators, based on the different case studies, has been collected and analyzed thoroughly in Task 1.2. A reference to this work (to refer interested readers in the right direction) has been added in the in the conclusions (section 7.2.1).
In general, I can hardly find any "smart city" aspects. Going forward, one should explicitly focus on the new aspects of the smart world. Sensors, meters, communicating devices, data processing, analytics, protection, access control, downtime of ICT infrastructure, new vulnerabilities. Most of the cases show current resilience issues without mentioning future challenges related to "smart" infrastructure.	A paragraph has been added in the conclusions (last paragraph of section 7.2.2), which describes these future challenges as topics that should be subject to further research.
Reviewer 3	
p. 62: "With regards to the complexity of critical infrastructures, several case studies have shown how interdependencies and interconnectedness poses particular challenges with regards to collaboration and coordination across organizational boundaries". Should be pointed out as a topic for further study, as interlinkages and public perception of crises tend to deepen the overall effect of risks.	A paragraph has been added in the conclusions (last paragraph of section 7.2.2), which describes that this should be subject to further research.