H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure
D3.3 - Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure (SCI), based on resilience indicators

Coordinator: Aleksandar Jovanovic EU-VRi
Project Manager: Bastien Caillard EU-VRi
European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart
Contact: smartResilience-CORE@eu-vri.eu
Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure (SCI), based on resilience indicators

Stuttgart, October 2018
## Release History

<table>
<thead>
<tr>
<th>Release No.</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>April 27, 2018</td>
<td>Release of the first draft report (addresses the comments made by project partners in T 3.6 report)</td>
</tr>
<tr>
<td>2</td>
<td>July 4, 2018</td>
<td>Comments from the preliminary review included</td>
</tr>
<tr>
<td>3</td>
<td>Oct. 8, 2018</td>
<td>New version sent to authors</td>
</tr>
<tr>
<td>4</td>
<td>Oct. 18, 2018</td>
<td>Updated version sent to reviewers</td>
</tr>
<tr>
<td>5</td>
<td>Oct. 31, 2018</td>
<td>Reviewers comments implemented</td>
</tr>
</tbody>
</table>
Modern critical infrastructures are becoming increasingly smarter (e.g. smart cities). Making 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 when also 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 this also make it more vulnerable? Would this affect the resilience of a SCI in terms of its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) that need to be looked at?

These are the main questions tackled by SmartResilience project.

The project envisions 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; and (#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 for benchmarking of best-practice solutions and identifying early warning signs, improving resilience of SCIs against new threats as well as 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 and seven leading research organizations, supported by academia and led by a dedicated European organization. External world leading resilience experts will be included in the Advisory Board.

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 – D3.3 Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure (SCI), based on resilience indicators.
Executive Summary

The main objective of T3.3 is to model the impact of a possible disruptive/adverse event on smart critical infrastructures (SCIs). The call text emphasizes the need for the development of specific “modeling approaches that facilitates the understanding and modeling of security risks and related impacts.”

In order to achieve this goal, this task provides a 10-step functionality level (FL) assessment methodology based on indicators. This methodology can be applied across SCIs to model the impacts of disruptive events by using context-specific aspects (“elements”) and indicators. In this methodology, the functionality of a SCI is considered as the role that this infrastructure plays in serving the society, and the loss of functionality of the SCI can have a severe impact on the society. Also, unless the loss of functionality is due to an unexpected extreme event or has a devastating impact on the society, it is not critical for the society. This is what classifies the infrastructure as critical.

The resilience level assessment proposed in T3.2 can benefit from FL assessment by identifying weak areas in different phases of the resilience cycle.

The description of the task further stresses the importance of modeling the impact (absorb capacity and recovery response) based on indicators. The modeling is done by estimating the change in functionality level over the scenario time (time during the course of a disruptive event). Further, this methodology proposes to model the impact of a disruptive event on the resilience of SCIs based on the following macro-indicators: robustness, disruption time, absorption time, downtime, recovery time, recovery rate, loss of functionality, and improvement/adaptation/ transformation. The FL assessment methodology can further be used for:

- Stress testing the resilience of the SCIs
- Benchmarking
- Possibly predicting smart critical infrastructure behavior

This report starts with introductory Chapter 1, which provides background about the needs and requirements of T3.3 (as stated in the call text and task description) and its contributions to work package (WP) 3 and other parts of the project, followed by a list of key vocabulary used in this report. Chapter 2 describes the concept of resilience as considered in the SmartResilience project based on previous work. Chapter 3 describes the functionality assessment methodology followed in the SmartResilience project. Chapter 4 is dedicated to the overall SmartResilience methodological framework. Chapter 5 provides application examples in relation to both a single infrastructure and infrastructure-of-infrastructures. Conclusions are included in Chapter 6. Finally, relevant annexes are included at the end of the report. Specifically, Annex 1 indicates how SCI owners/operators can use the functionality level assessment results.
1.1 Background: needs and requirements ......................................................... 10
  1.1.1 Call text, work description, and aims of the methodology proposed
       in T3.3 ..................................................................................................... 10
  1.1.2 Task 3.3: second pillar in the SmartResilience project methodology ... 10
  1.1.3 Why focus on CI functionality? ............................................................ 11
1.2 Relation to other parts of the project .......................................................... 11
1.3 Vocabulary: Specific terms used in the methodology ................................. 12
1.4 Report structure .......................................................................................... 13
2.1 Resilience definition .................................................................................... 14
2.2 Resilience matrix ....................................................................................... 14
3.1 Functionality concept ................................................................................ 17
  3.1.1 Functionality assessment levels of a SCI ........................................... 18
  3.1.2 Modeling the impact of a disruptive event based on macro-
       indicators ............................................................................................ 20
  3.1.3 Method steps .................................................................................. 23
4.1 What is the possible outcome of an assumed adverse event scenario? Will
       the functionality remain within the prescribed limits? .......................... 31
4.2 How should resilience be monitored? .......................................................... 31
4.3 Investment in resilience optimization: How is the best value for money
       obtained? .............................................................................................. 32
5.1 Single infrastructure ................................................................................... 35
  5.1.1 Step 1: Select the SCI(s) to be assessed ............................................ 35
  5.1.2 Step 2: Identify relevant threats for each SCI and initiate respective
       DCLs ..................................................................................................... 35
  5.1.3 Step 3: Consider if the possible interdependencies of the SCI affect
       the results ............................................................................................. 35
  5.1.4 Steps 4 and 5: Define FE and Fls for each DCL ................................... 35
  5.1.5 Step 6: Assign maximum, minimum, and target values to all Fls
       (optionally assign weights) ........................................................................ 36
  5.1.6 Step 7: Assign time values for the scenario ....................................... 36
  5.1.7 Step 8: Assign values for the Fls at given times ............................... 37
  5.1.8 Step 9: Generate and evaluate the FL-t curve that models the
       impact of disruption through macro-indicators .................................... 38
  5.1.9 Step 10: Consider if the possible interdependencies of the SCI
       affects the results .................................................................................. 39
5.2 Infrastructure-of-infrastructures ................................................................. 39
6.1 General .................................................................................................... 40
6.2 Alignment of approaches to resilience ............................................................ 40
6.3 Possible standardization path ................................................................. 41
### List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1:</td>
<td>Task 3.3 in the SmartResilience methodology</td>
</tr>
<tr>
<td>Figure 2:</td>
<td>Relation to other tasks in the SmartResilience project</td>
</tr>
<tr>
<td>Figure 3:</td>
<td>Levels for assessing the operating level according to the IBCDRP approach, based on [21]</td>
</tr>
<tr>
<td>Figure 4:</td>
<td>Structure to assess the functionality of an infrastructure</td>
</tr>
<tr>
<td>Figure 5:</td>
<td>Complete structure for functionality assessment in a smart city</td>
</tr>
<tr>
<td>Figure 6:</td>
<td>Examples of functionality elements and indicators [9]</td>
</tr>
<tr>
<td>Figure 7:</td>
<td>Functionality level of the SCI over scenario time</td>
</tr>
<tr>
<td>Figure 8:</td>
<td>Level of functionality as stress test limit</td>
</tr>
<tr>
<td>Figure 9:</td>
<td>Time as stress test limit</td>
</tr>
<tr>
<td>Figure 10:</td>
<td>Loss of functionality surface as stress test limit</td>
</tr>
<tr>
<td>Figure 11:</td>
<td>Comparing the FL curve with the stress test criteria</td>
</tr>
<tr>
<td>Figure 12:</td>
<td>Benchmarking one SCI with another</td>
</tr>
<tr>
<td>Figure 13:</td>
<td>Predicting the behavior of SCI</td>
</tr>
<tr>
<td>Figure 14:</td>
<td>Differences in resilience and functionality level assessment of a SCI</td>
</tr>
<tr>
<td>Figure 15:</td>
<td>Long-term monitoring of resilience by means of resilience indicators</td>
</tr>
<tr>
<td>Figure 16:</td>
<td>View on the DCL from the SmartResilience dashboard</td>
</tr>
<tr>
<td>Figure 17:</td>
<td>Investment in resilience optimization - concept</td>
</tr>
<tr>
<td>Figure 18:</td>
<td>FE and FI used in ECHO case, BLEVE scenario</td>
</tr>
<tr>
<td>Figure 19:</td>
<td>Case’s time series</td>
</tr>
<tr>
<td>Figure 20:</td>
<td>Assigned FI values and resulting FE calculated values</td>
</tr>
<tr>
<td>Figure 21:</td>
<td>FL-t curve for the ECHO case study example</td>
</tr>
<tr>
<td>Figure 22:</td>
<td>Multiple FL-t curve for ECHO (blue) and HOTEL (orange) in INDIA</td>
</tr>
<tr>
<td>Figure 23:</td>
<td>Collaboration in the area of resilience, between the US (ANL, Argonne National Laboratory) and the EU (EU-VRi, European Virtual Institute for Integrated Risk Management), covered by the accompanying agreement (approved by the Department of Homeland Security on the US side)</td>
</tr>
<tr>
<td>Figure 24:</td>
<td>Initiating a DCL in the SCI dashboard (DCL Step 1)</td>
</tr>
<tr>
<td>Figure 25:</td>
<td>Selection of FEs for the HOTEL case (DCL Step 2)</td>
</tr>
<tr>
<td>Figure 26:</td>
<td>Selection of the Fls for the HOTEL case (DCL Step 3)</td>
</tr>
<tr>
<td>Figure 27:</td>
<td>Assign maximum, minimum, and best values to the FI (DCL Step 4)</td>
</tr>
<tr>
<td>Figure 28:</td>
<td>Assign time values in the SCI dashboard (DCL Step 4)</td>
</tr>
<tr>
<td>Figure 29:</td>
<td>Assigning values for each FI at different times during the scenario (DCL Step 4)</td>
</tr>
<tr>
<td>Figure 30:</td>
<td>FL-t curve for smart energy supply system (HOTEL)</td>
</tr>
</tbody>
</table>
### List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Resilience matrix in the SmartResilience project</td>
<td>15</td>
</tr>
<tr>
<td>Table 2</td>
<td>Sample combinations infrastructure-scenario targeted by the SmartResilience project</td>
<td>15</td>
</tr>
<tr>
<td>Table 3</td>
<td>Reference approaches for modeling the impact of disruptive events based on macro-indicators</td>
<td>21</td>
</tr>
<tr>
<td>Table 4</td>
<td>Steps for functionality level assessment</td>
<td>23</td>
</tr>
<tr>
<td>Table 5</td>
<td>Typical threats</td>
<td>24</td>
</tr>
<tr>
<td>Table 6</td>
<td>Sample FEs and FIs in the ECHO case study</td>
<td>35</td>
</tr>
</tbody>
</table>
List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANL</td>
<td>Argonne National Laboratory</td>
</tr>
<tr>
<td>BLEVE</td>
<td>Boiling liquid expanding vapor explosion</td>
</tr>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CO</td>
<td>Critical Operation</td>
</tr>
<tr>
<td>DCL</td>
<td>Dynamic Check List</td>
</tr>
<tr>
<td>FE</td>
<td>Functionality Element</td>
</tr>
<tr>
<td>FI</td>
<td>Functionality Indicator</td>
</tr>
<tr>
<td>FL</td>
<td>Functionality Level</td>
</tr>
<tr>
<td>FLI</td>
<td>Functionality Level of the Infrastructure</td>
</tr>
<tr>
<td>FL-t</td>
<td>Functionality Level over time</td>
</tr>
<tr>
<td>IBCDRP</td>
<td>Integrated Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>MBCO</td>
<td>Minimum Business Continuity Operations</td>
</tr>
<tr>
<td>MCDM</td>
<td>Multi-criteria decision-making</td>
</tr>
<tr>
<td>MTDP</td>
<td>Maximum Tolerable Period of Disruption</td>
</tr>
<tr>
<td>NIAC</td>
<td>National Infrastructure Advisory Council</td>
</tr>
<tr>
<td>NWIP</td>
<td>New Work Item Proposal</td>
</tr>
<tr>
<td>OpA</td>
<td>Optimization Alternative</td>
</tr>
<tr>
<td>OEE</td>
<td>Overall Equipment Effectiveness</td>
</tr>
<tr>
<td>RL</td>
<td>Resilience Level</td>
</tr>
<tr>
<td>RI</td>
<td>Resilience Indicator</td>
</tr>
<tr>
<td>SCI</td>
<td>Smart Critical Infrastructure</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>HSE</td>
<td>Health, Safety, and Environment</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Background: needs and requirements

1.1.1 Call text, work description, and aims of the methodology proposed in T3.3

The call text [1] states that “a better understanding of critical infrastructure architecture is necessary for defining measures to achieve a better resilience against threats in an integrated manner including natural and human threats/events.” Furthermore, it stresses the need to focus on “potential threats caused by attacks or accidents,” thereby asserting that projects should “address the need for a paradigm shift in the area of design for safety and resilience.”

Moreover, it emphasizes the need for the development of “specific models and modeling approaches” that “facilitate the understanding and modeling of security risks and related impact.” The approach should be able to “anticipate current and emerging threats.” Furthermore, the call text asks for a “… holistic approach at all levels (e.g. EU, country, local) …” Regarding expected impact, “the action is expected to proactively target the needs and requirements of public bodies” [1].

In addition, the approach should take into account interconnectedness that may have “devastating impact on the functioning of the society.”

Consequently, the title of the task in the work description is “Modeling the impact of an adverse event on the “absorb” and “recover” capacity of a smart critical infrastructure (SCI), based on resilience indicators.”

Hence, the aim of this task is to propose a methodology that models the impact of the “potential threats caused by attacks or accidents (human error or terrorist/criminal attacks) on critical infrastructures at all levels (EU, country, local),” which forms the part of the scenario. The proposed 10-step methodology measures the functionality level of the critical infrastructure (CI) throughout the duration of the scenario. This assessment forms the basis for modeling the impact of a disruption on the CI(s) in terms of the proposed macro-indicators. It also provides the basis for stress test exercises, prediction, and benchmarking.

1.1.2 Task 3.3: second pillar in the SmartResilience project methodology

The SmartResilience methodology is comprised of three main pillars: resilience assessment based on the resilience assessment methodology in T3.2 [1], resilience modeling based on functionality assessment of SCIs in T3.3, and monitoring and optimization based on the decision-making models such as multi-criteria decision-making (MCDM) in T3.4. This task describes the second pillar of the SmartResilience methodology.
The methodology described in T3.3 aims to achieve the above-stated aspects of the call text by:

1. Understanding the smart critical infrastructure (SCI) by means of quantifying its *functionality* based on indicators;
2. Providing a systematic level based on a 10-step methodology to measure the functionality of SCIs before, during, and after disruptive events, such as attacks or accidents and related impacts;
3. Modeling the impact (“absorb capacity”) of a disruption and recovery response (“recover capacity”) based on indicators; and
4. Providing the *basis for stress testing* the infrastructure, anticipating current and emerging risks by means of predicting the behavior of the SCI, and benchmarking to improve resilience.

### 1.1.3 Why focus on CI functionality?

In the SmartResilience project, the resilience assessment methodology developed in T3.2 is aimed at deriving the resilience level (RL) of the SCI and identifying weak points where measures are needed to improve its resilience; however, this methodology is not aimed at obtaining a resilience curve [1]. In resilience assessment methodology, the resilience curve is treated as a conceptual model for defining the phases in the resilience cycle. This implies that resilience assessment does not consider the exact shape, size, or area of the curve directly; instead, it uses issues (what) and indicators (how) within each of the five resilience phases to assess resilience indirectly.

In order to model the absorb capacity and recovery/response, it is necessary to consider the shape of the resilience curve, i.e. the changes in the critical functionality of the SCI as a function of time (during the course of the scenario).

A tacit assumption has been that “functionality” is something that the analysts or the infrastructure owner/operator will be able to define, possibly explicitly and simply. However, the case studies developed in the SmartResilience project have shown that this is not a trivial task [24]. For example, no matter how intuitively one might think that the critical functionality of an airport is in order to “keep the air traffic going,” it is challenging to precisely define what critical functionality is provided for the society, which if lost due to an extreme event (such as a terror attack or cyber-attack) would have a “devastating impact on the functioning of the society.”

This task goes beyond the conceptual model of resilience and focuses on operationalization of the functionality level assessment of an infrastructure over time in order to understand how a disruptive event affects the critical functionality of an infrastructure.

### 1.2 Relation to other parts of the project

The relation of T3.3 to other tasks in the project is illustrated in Figure 2. Work package (WP) 1, specifically T1.3, describes the needs and requirements of the SCIs in the project. WP2 (challenges) provides input on threats, vulnerabilities, and impacts for SCIs. Furthermore, within WP3, the D3.1 provides an overview of contextual factors. These tasks are used to develop the examples for implementing the proposed methodology. Further, the quality criteria for defining indicators in T3.2 are also considered useful for defining indicators for functionality assessment, and hence, these criteria are adapted for the methodology proposed in this task. The outputs of this task are integrated into the guideline that provides direction for CI owners/operators on applying the functionality method. This task provides input for developing the SCI dashboard in T3.7.

This task also sets the foundation for the stress tests to be conducted by the project case studies in WP5. In particular, the method steps for the stress test are described in the D5.2 report and applied in T5.3 to T5.11. The results of the methodological application will be summarized in T5.12 report, i.e. the Test and evaluation manual.
1.3 **Vocabulary: Specific terms used in the methodology**

<table>
<thead>
<tr>
<th>Functionality of a SCI:</th>
<th>Considered as the role that a SCI plays in order to serve the society.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functionality level:</td>
<td>The level at which the SCI is operating at a given moment.</td>
</tr>
<tr>
<td>Functionality elements:</td>
<td>The most relevant functions of the SCI that contribute to its overall functionality (see Figure 6).</td>
</tr>
<tr>
<td>Functionality indicators:</td>
<td>Measurable units used to measure the functionality elements (FEs).</td>
</tr>
<tr>
<td>Steps:</td>
<td>In SmartResilience, the functionality assessment method consists of 10 steps.</td>
</tr>
<tr>
<td>Robustness:</td>
<td>The capacity of the SCI to endure the effects of a negative event and thereby absorb its impact.</td>
</tr>
<tr>
<td>Disruption time:</td>
<td>Total time taken by the SCI to recover. It is also seen as a measure for recover capacity of the SCI to return to a desired functionality level.</td>
</tr>
<tr>
<td>Absorption time:</td>
<td>Time at which the SCI absorbs the disruptive event, decreasing its initial functionality.</td>
</tr>
<tr>
<td>Downtime:</td>
<td>Time duration for which the functionality level of the infrastructure remains below the threshold level of functionality.</td>
</tr>
<tr>
<td>Recovery time:</td>
<td>Time taken by the SCI to recover to the initial functionality level after a disruptive event.</td>
</tr>
<tr>
<td>Recovery rate:</td>
<td>Rate at which the SCI recovers from the disruptive event and returns to its initial functionality level after the disruptive event.</td>
</tr>
</tbody>
</table>
## Functionality of a SCI:
Considered as the role that a SCI plays in order to serve the society.

| Improvement/adaptation/transformation: | Capacity of the SCI to improve/adapt/transform from the disruptive event (e.g. a revision of plans, modification of procedures, introduction of new tools and technologies, etc.). |
| Loss of functionality: | The loss in functionality of the SCI in a given threat situation, measured in percentage loss of functionality at a given point in time. |

### 1.4 Report structure

Following this introductory chapter, Chapter 2 describes the concept of resilience as considered in the SmartResilience project based on previous work. Chapter 3 describes the functionality assessment methodology followed in the SmartResilience project. Chapter 4 is dedicated to the overall SmartResilience methodological framework. Chapter 5 provides application examples in relation to both a single infrastructure and infrastructure-of-infrastructures. In Chapter 6, questions related to the proposed methodology are discussed. These questions include those raised by end-users, CIRAB members, and project partners. Conclusions are stated in Chapter 7. Finally, relevant annexes are included at the end of the report. Specifically, Annex 1 indicates how SCI owners/operators can use the functionality level assessment results.
2 Resilience concept in SmartResilience

2.1 Resilience definition

The definition of resilience has been adapted in the SmartResilience project based on the initial work conducted in T1.1 [33] and T1.2 [15].

Box 1. Resilience of an infrastructure (SmartResilience project)

“Resilience of an infrastructure is the ability to understand and anticipate the risks – including new/emerging risks – threatening the critical functionality of the, prepare for anticipated or unexpected infrastructure disruptive events, absorb/waithstand their impacts, respond and recover from them, and adapt/transform the infrastructure or its operation towards improved anti-fragility.”

The main reason for the “update” was the need to bring the definition more in line with other aspects of the approach, namely the resilience indicators, resilience matrix [15], risk (especially emerging risk) analysis, and standards currently applicable in the area [35].

It is important to note that assessment of resilience is not dependent on the occurrence of a disastrous event. Most infrastructures have not experienced, and will never experience, a terror attack or cyber attack. Still, it shall be possible to assess resilience based on potential (anticipated or unexpected) events. Even lessons learned can be based on hypothetical events, or events experienced by others.

2.2 Resilience matrix

So far, resilience approaches have used different numbers of phases to characterize the resilience cycle, ranging from 4 [36] to 8 [37]. SmartResilience proposes to align itself within a 5x5 matrix containing 5 resilience phases:

1. Understand risks
2. Anticipate / prepare
3. Absorb / withstand
4. Respond / recover
5. Adapt / transform / Learn

And 5 resilience “dimensions”:

1. System / physical
2. Information / smartness
3. Organizational / business
4. Societal / political
5. Cognitive / decision-making related

---

1 Anti-fragility: as defined by N. Taleb in “Antifragile” Penguin Books 2012
2 This is ultimately a matter of choice based on factors such as appropriateness and practicality. The chosen phases can always be questioned, e.g. splitting ‘respond’ and ‘recover’ into two phases, using the term ‘learn’ instead of ‘transform’, etc.
An example of the matrix and the issues one could look for in the different cells of the matrix is provided in Table 1. The scenarios (SCIs and threats) being considered in the SmartResilience project are listed in Table 2. These provide part of the background information that is considered when preparing the methodology of this task.

Table 1: Resilience matrix in the SmartResilience project

<table>
<thead>
<tr>
<th>PHASE</th>
<th>DIMENSION</th>
<th>I. UNDERSTAND RISKS</th>
<th>II. ANTICIPATE / PREPARE</th>
<th>III. ABSORB / WITHSTAND</th>
<th>IV. RESPOND / RECOVER</th>
<th>V. ADAPT / TRANSFORM / LEARN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. SYSTEM / PHYSICAL</td>
<td>Review of risks for the physical infrastructure and/or network of infrastructures</td>
<td>State and ability of physical assets e.g. barriers, alert systems, entrance controls</td>
<td>Physical safety system and redundant components</td>
<td>Flexibility in system design, temporary system installation</td>
<td>Ability to update system configurations based on lessons learned</td>
</tr>
<tr>
<td></td>
<td>b. INFORMATION / SMARTNESS</td>
<td>Information about adequacy of existing barriers against possible risks</td>
<td>Information from previous events (what went wrong/right) to learn from</td>
<td>Real-time monitoring and actions triggering smart devices</td>
<td>Information about centralized facilities and distribution of essential supplies and services</td>
<td>Information from smart sensors about events, response operations and lessons learned</td>
</tr>
<tr>
<td></td>
<td>c. ORGANIZATION / BUSINESS</td>
<td>Periodic organizational review of the relevant risks, reports about previous events</td>
<td>Budget and plans for preparedness</td>
<td>Availability of action plan and competent personnel for immediate reaction to event</td>
<td>Availability of enough emergency response budget and resources</td>
<td>Debriefing of the event and the response operations to personnel directly involved</td>
</tr>
<tr>
<td></td>
<td>d. SOCIETAL / POLITICAL</td>
<td>Exchange of knowledge about risks (including risk perceptions in the society)</td>
<td>Seeking information from authorities on threat assessments and preparing</td>
<td>External alert and communication, Coordination between actors</td>
<td>Contact/liaison with authorities/ media and regular communication</td>
<td>Communication with local governments and stakeholders to transform the previous practices</td>
</tr>
<tr>
<td></td>
<td>e. COGNITIVE / DECISION MAKING</td>
<td>Decision criteria of individuals (Risk perception, mental models, values)</td>
<td>Ability (biases previous knowledge used) of the individuals to alert others of specific threat</td>
<td>Situational awareness ability of the individuals to evaluate the performance during the event</td>
<td>Transparency in response and recovery decision making and communication</td>
<td>Improvement in decision making to deal with future events</td>
</tr>
</tbody>
</table>

Table 2: Sample combinations infrastructure-scenario targeted by the SmartResilience project

<table>
<thead>
<tr>
<th>Infrastructure (CI) / Scenarios</th>
<th>Terrorist attack</th>
<th>Cyber attack</th>
<th>Extreme weather</th>
<th>Cross-cutting issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Smart cities (Germany, Ireland)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Insurance, law enforcements, legislation, ...</td>
</tr>
<tr>
<td>2. Smart financial system (UK)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3. Smart health care (hospitals, Austria)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4. Smart energy supply systems (Finland)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5. Smart industrial/production plants (incl. Industry 4.0 plants, Serbia)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6. Smart transportation (airports, Hungary)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7. Smart water supply (Drinking water supply, Sweden)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

(✓) = Partly applicable
In resilience research, the resilience curve concept has been widely used to describe how a system’s resilience changes when subjected to a disruptive event. Further, in order to model the impact of a disruptive event, the assessment of resilience in terms of “loss of critical functionality” needs to be considered, i.e. by assuming that, for a given threat/scenario, the resilience of the infrastructure will be inversely proportional to the loss of critical functionality. In other words, the less critical functionality that is lost, the more resilient the infrastructure is.

In order to quantify this loss of functionality, one has to understand:

1. What does the CI functionality mean, or what does the curve represent?
2. How are the main points on the curve (e.g. those delimiting the resilience cycle phases) calculated?

However, limited knowledge is available from existing literature [5] [17] [11] on how exactly to define functionality of the SCIs, how to quantify it, and how to estimate the main points on the curve. Some of the reviewed literature is summarized below.

The Argonne National Laboratory (ANL) proposes assessing the resilience of a critical infrastructure based on a set of questions. ANL uses these questions to assess resilience indirectly, similar to how indicators (which can also be questions) are used in resilience assessment. In this process, functionality refers to the level of activity (e.g. production, in the case of a manufacturing plant) of a system or of the well-being of a community [5]. The CI resilience “determines both the amount by which the activity/well-being declines and the amount of time required to return to the pre-event equilibrium (or some other new equilibrium).”

Despite its usefulness for understanding resilience components and adverse event timing, the proposed approach does not specify how to quantify the functionality of a CI, since ANL is not focusing directly on the curve itself (as is also the case for resilience assessment).

Kröger (2014) defines the functionality of an energy infrastructure in terms of system performance [17] while conceptualizing CI resilience and possible scenarios for understanding the impact of an event on a system. System performance is considered to be the goal attainment ability of a particular system and is further defined as being “secure, sustainable, and affordable” [17]. “Secure” refers to the continuous availability of a certain amount and quality of electric energy. Kröger also uses the terms “equilibrium” and “initial state of affairs.” The energy system is functional regardless of whether electricity comes from renewable sources, coal, or nuclear power, so long as sufficient energy of good quality is continuously provided in a cost-efficient and sustainable manner [17]. The aspect useful for development of the functionality assessment of a SCI is that a system may have different types of behaviors, such as robust, ductile, collapsing or adaptive, depending on how it performs during stressful situations. This aspect provides the conceptual basis for modeling the impact of disruptive events on SCIs. However, from this conceptualization it is again unclear how the curve is derived.

Sahebjamnia et al. [22] provide a structured way to define operating level, which can serve as the basis for the functionality level assessment method structure. The authors propose an Integrated Business Continuity and Disaster Recovery Planning (IBCDRP) approach, which introduces the operating level concept in context of industrial application. The approach focuses on operational resilience and defines the y-axis based on the Business Continuity Management Standard [37] as the operating level of each key product that is acceptable to the organization to achieve its business objectives.
The structure of this approach consists of three levels (see Figure 3). Level 1 is the overall operating level, which is broken down into level 2, i.e. key services/products. Then, for each of the key services/products, critical operations (CO) are defined; this constitutes the level 3 of the structure. Examples of COs in this assessment approach are process routes, technological level, insuring capability, recovering time, and cost. This approach provides a basis for structuring the functionality levels of SCIs in the SmartResilience project. However, this model is only used to measure a few critical operations to ensure business continuity in industrial operations. In the case of a more complex critical infrastructure environment, a variety of aspects need to be considered. In addition, this approach does not specify how to estimate the main points of the curve in terms of resilience.

3.1 Functionality concept

The functionality of a SCI is considered as the role that an infrastructure plays in serving the society, and SCI loss of functionality can have a severe impact on society. Although it is not straightforward in providing what exactly contributes to the functionality of a given SCI, the IBCDRP approach [21] provides a basis for structuring the functionality level assessment methodology for a SCI. Hence, instead of using the term “operating level,” this methodology proposes the term “Functionality Level (FL)” of the SCI, which implies the main functions performed by a SCI. FL can be further broken down into Functionality Elements (FEs). These FEs are at the same level as the key services/products. FEs can be measured by using Functionality Indicators (FIs). These are similar to the critical operations.

Hence, the methodology proposes to assess the functionality level of SCIs in the SmartResilience project by using:

- Functionality elements (FEs), which are the most relevant societal functions of the SCI that contribute to the overall functionality or output of the SCI (these correspond to issues in the SmartResilience method for assessing the RL), and
- Functionality indicators (FIs), which are quantifiable units used to measure the functionality elements. As in resilience assessment methodology [28], indicators are used for this assessment. However, here the indicators are referred to as “functionality indicators,” instead of “resilience indicators,” since they measure functionality.

FE and FI form the lower two levels in the functionality assessment methodology (Figure 4).
Further, the critical functionality level of a SCI is defined as the minimum level or threshold level for a CI to be operational. This aspect will be further used to define the stress test criteria. It is also important to note that the portfolio of FE and FI shall NOT change over time (i.e. once defined as representative, they shall be used until the end of the cycle).

### 3.1.1 Functionality assessment levels of a SCI

In addition to the two lower levels in the functionality assessment structure, two more levels form the complete structure for functionality assessment in a smart city. Therefore, the complete structure comprises four levels (shown in Figure 5):

- Level 1. Functionality level of the city
- Level 2. Functionality level (FL) of the infrastructure, corresponding to the SCIs in the project
- Level 3. Functionality elements (FEs)
- Level 4. Functionality indicators (FIs)

This structure provides the foundation for functionality assessment of a SCI. Figure 6 presents some examples of FEs and FIs. The end-users must identify core functionality elements for their CIs. Nevertheless, all the levels in the FL assessment are context-specific. Therefore, the choice of the FEs and FIs is also context specific. This implies that SCI owners/operators and analysts can customize and implement the functionality assessment according to their particular requirements and needs. By featuring context, the functionality assessment offers the possibility of modeling the impacts of adverse events based on indicators for each particular SCI.
In SmartResilience, the proposed method aims at measuring the functionality level of a SCI at different points in time, i.e. before, during, and after an event, which is then plotted over the scenario time, as illustrated in the notional diagram in Figure 7. Disruption scenarios characterize the severity, risks, and occurrence time of the disruption. Modeling their impact on the SCI is scenario-specific, as different types of scenarios require different technical, organizational, and social support for a system to be able to cope.

Unless the loss of critical functionality, due to an unexpected extreme event, has a devastating impact on the society, it is not critical for the society. This is also what classifies the infrastructure as critical. The only critical functionality here is the “core,” e.g. the production/output. The other functionality elements are sub-functions (maybe important for the owners, but not for the society). E.g. firewalls will contribute to prevent or reduce the impact of a cyber attack, which then will influence what the SCI delivers to the society (the critical functionality).

The critical functionality should be limited to one or very few measures (maximum 3), and it should be made sure that they are not measuring the same, just in different ways (as is the case for HOTEL in Annex 2, where production and number of people supplied are two sides of the same coin).

Each critical functionality (1 or 2 or 3) should be treated separately, providing separate resilience curves. As it is done now, you are mixing apples and oranges, and the resulting curve has no meaning (e.g. combining production with working hours lost due to incidents, as is done in the HOTEL case in Annex 2).

Introducing a mix of core – critical – functionalities and sub-functions, as is done here, makes the method confusing for the users, and the way they are combined (as illustrated in the HOTEL case in Annex 2) gives wrong/meaningless results.

See further comments in Annex 2.

The points in time are [28]:

- $t_0$: time before the event or starting point of the scenario
- $t_1$: time at which the event occurs
t₂: time at which the infrastructure reaches the minimum functionality level

Path 3: time at which the infrastructure starts to recover

Path 4: time at which the infrastructure reaches the initial functionality level or starting point of a new steady state level

Path 5: time at which the infrastructure increases its functionality through learning and adapting or at which the scenario ends

The notional diagram in Figure 7 shows clear trends and smooth transition in the FL of the SCI. However, actual measures or simulated data are often volatile or noisy, due to the stochastic (i.e. random) nature of many real or simulated processes [30]. Here we use the smoothed FL curve to show a general and simplified trend of the change in the SCI functionality.

<table>
<thead>
<tr>
<th>Event</th>
<th>Functionality Level (FL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>t₀</td>
<td>Starting point of scenario</td>
</tr>
<tr>
<td>t₁</td>
<td>Event</td>
</tr>
<tr>
<td>t₂</td>
<td>Loss of functionality</td>
</tr>
<tr>
<td>t₃</td>
<td>Recovery time</td>
</tr>
<tr>
<td>t₄</td>
<td>Recovery time</td>
</tr>
<tr>
<td>t₅</td>
<td>Improvement / adaptation / transformation (based on lessons learned (improved “antifragility”))</td>
</tr>
<tr>
<td>t₅’</td>
<td>Permanent loss of functionality</td>
</tr>
</tbody>
</table>

Figure 7: Functionality level of the SCI over scenario time

3.1.2 Modeling the impact of a disruptive event based on macro-indicators

A variety of ideas are used to model the impact of a disruptive event on the resilience of the critical infrastructures in areas such as organizational resilience [22] [5], reliability engineering and system safety [28] [30], and community resilience [1]. ANL uses components such as robustness, resourcefulness, and rapid recovery in its Resilience Index [9]. Tran et al. [27] applies total performance factor, absorption factor, recovery factor and recovery time. Bruneau et al. [2] proposes measuring the loss of resilience based on the reduction in the amount of operating level and restoration time.
Table 3: Reference approaches for modeling the impact of disruptive events based on macro-indicators

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Robustness</td>
<td>Absorption factor</td>
<td>-</td>
<td>Robustness</td>
</tr>
<tr>
<td>-</td>
<td>Total performance factor</td>
<td>Reduction in the amount of operating level</td>
<td>Absorption time, Downtime</td>
</tr>
<tr>
<td>Recovery</td>
<td>Recovery factor</td>
<td>-</td>
<td>Recovery rate</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>Recovery time</td>
<td>Restoration time</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>Disruption time</td>
<td>Improvement/adaptation/transformation</td>
</tr>
</tbody>
</table>

In the SmartResilience project, as stated in the work description of the task, modeling the impact of a disruptive event on the functionality of a SCI involves assessing the absorb capacity and recovery response of the infrastructure. Most of the measures, so-called macro-indicators, shown in Figure 7 address the absorb capacity and the recovery response, but the entire curve is also of interest, including "loss of critical functionality" and "improvement/adaptation/transformation." Hence, the following macro-indicators are proposed for modeling the impact of the disruption:

- Robustness
- Absorption time
- Downtime
- Loss of functionality
- Recovery time
- Recovery rate
- Disruption time
- Improvement/adaptation/transformation

**Robustness** characterizes the absorb capacity of the SCI [30]. ANL uses robustness as defined by the National Infrastructure Advisory Council (NIAC) [18], i.e. "the ability to maintain critical operations and functions in the face of crisis" [5]. It can be seen as the protection and preparation of a system facing a specific danger. The objective of the robustness component is to identify measures that can help the system withstand or adapt to a hazard. It emphasizes the ability of an infrastructure to withstand the incident if the protective measures fail. It also integrates the capacity of the infrastructure to function in a degraded state. The importance of robustness is not necessarily defined by how the infrastructure continues to function in the face of an incident but rather by how it is able to continue to accomplish its mission and to provide its products and services through preventative measures, mitigation, or absorption capabilities [5]. In the SmartResilience project, robustness is defined as the capacity of the SCI to endure the effects of a negative event and thereby absorb its impact. As shown in Figure 7, it is measured as the ratio of the percentage of the lowest FL after the disruption, i.e. at time \( t_2 \), to the FL during normal operation, i.e. at time \( t_0 \).

\[
\text{Robustness} = \frac{FL_{t_2}}{FL_{t_0}} \times 100\%
\]

**Absorption time** is defined as the time during which the SCI absorbs a disruptive event while the SCI undergoes a decrease in its functionality level. As illustrated in Figure 7, it is measured as the difference between \( t_3 \) and \( t_1 \).
Absorption time = \( t_2 - t_1 \)

**Downtime** is defined as the time duration for which the system is not functional. In reference to critical infrastructures, this could apply if the CI stops functioning. In this case the functionality level of the infrastructure remains below the **threshold level** of functionality [5]. It can be measured as the difference in time between \( t_3 \) and \( t_2 \) (see Figure 7).

\[ \text{Downtime} = t_3 - t_2 \]

**Note:** This calculation is conducted when the threshold level of functionality is defined (Here it is assumed that the threshold level is \( FL_{t2} (=FL_{t3}) \)).

**Loss of functionality** is the functionality of the SCI lost in a given threat situation. It is measured by the area of the curve (an approximation) between the time when the SCI starts to lose its functionality (\( t_1 \)) to the time when it reaches the initial state (\( t_4 \)) (see Figure 7). The approximation is done for the area above the curve to a well-defined shape, e.g. a triangle. The output would be the percentage loss of functionality in time [22] [1], e.g. losing 10% in 10 hours.

\[ \text{Loss of functionality} = \int_{t_1}^{t_4} [FL_{t1} - FL(t)] \, dt \]

Next in the scenario is the **recovery** state of the SCI. The concept of recovery explains the passage of an infrastructure’s functionality from a degraded state to one of acceptable operation. This concept builds on the concept of robustness in that, if measures of robustness fail to fully prevent, mitigate, or allow the asset to absorb the damage event, recovery constrains the impacts of the event to keep the CI functional. In the SmartResilience project, for the purpose of modeling the impact of a disruptive event, **recovery** refers to the ability to not only return to acceptable operating levels but also to recover fully from the effects of an event [5] in the maximum allowable/acceptable recovery time (as described in the stress test methodology [31]) [21].

**Recovery time** is defined as the time at which the SCI recovers from the disruptive event and gains its initial or desired functionality [30]. It can be measured as the time taken to recover the functionality level, i.e. the time between time \( t_3 \) and \( t_4 \).

\[ \text{Recovery time} = t_4 - t_3 \]

**Note:** Since the functionality level at the end of the scenario may be different from at the start of the scenario, the recovery time may have to be measured at a new steady state level [21].

**Recovery rate** is defined as the rate at which the SCI recovers from a disruptive event and gets back to its initial functionality level [30]. It characterizes the recovery trajectories of the SCI from the point it starts recovering from the scenario to the final recovery. It is measured as the ratio of change in functionality level between time \( t_3 \) and \( t_4 \).

\[ \text{Recovery rate} = \frac{(FL_A - FL_L)}{(t_4 - t_3)} \]

Another measure considered for modeling the impact is **disruption time**. The disruption time is defined as the total time taken by the CI to recover. It is also seen as a measure for recover capacity of the SCI to return to a desired functionality level [30]. In the functionality level over time (FL-t) curve, it is the time between when the event occurs, i.e. at time \( t_1 \), and time when the SCI has fully recovered, i.e. \( t_4 \) (see Figure 7).

\[ \text{Disruption time} = t_4 - t_1 \]

**Improvement/adaptation/transformation:** Final recovery of the FL of a SCI could be equal to, better than, or worse than the original FL [29]. Hence, the model allows for calculation of the “improvement/adaptation/
transformation.” This is the capacity of the SCI to learn from a disruptive event (e.g. a revision of plans, modification of procedures, introduction of new tools and technologies [25]) (see Figure 7). It is measured as the ratio of change in FL during and after the event over the initial FL.

\[
\text{Improvement/adaptation/transformation} = \frac{FL_{t5} - FL_{t0}}{FL_{t0}} \times 100\%
\]

3.1.3 Method steps
The SmartResilience method for defining the SCI functionality has 10 main steps, as shown in Table 4). The FL assessment method is supported by a tool – a Dynamic Checklist (DCL) – accessed through the SmartResilience dashboard. An example of a DCL is presented in A.1.1. The DCL setup consists of four steps, which are included in the 10 FL assessment method steps.

<table>
<thead>
<tr>
<th>FL step no.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the SCIs to be assessed</td>
</tr>
<tr>
<td>2</td>
<td>Identify relevant threats for each SCI and initiate respective DCLs with basic information</td>
</tr>
<tr>
<td>3</td>
<td>Identify interdependencies between the selected SCIs</td>
</tr>
<tr>
<td>4</td>
<td>Define functionality elements (FEs) for each DCL</td>
</tr>
<tr>
<td>5</td>
<td>Define appropriate functionality indicators (FIs) for each FE in each DCL</td>
</tr>
<tr>
<td>6</td>
<td>Assign maximum, minimum, and target values to all FIs (optionally assign weights)</td>
</tr>
<tr>
<td>7</td>
<td>Assign time values for the scenario</td>
</tr>
<tr>
<td>8</td>
<td>Assign values for the FIs at given times</td>
</tr>
<tr>
<td>9</td>
<td>Generate and evaluate the FL-t curve that models the impact of disruption through macro-indicators</td>
</tr>
<tr>
<td>10.</td>
<td>Use the result of the functionality level assessment</td>
</tr>
</tbody>
</table>

3.1.3.1 Step 1: Select the SCI(s) to be assessed
In the SmartResilience project, a SCI is a critical infrastructure whose functionality is enhanced by the use of smart (i.e. intelligent) systems and technologies [25]. In Step 1, the SCI owner/operator selects the SCI(s) to be assessed.

3.1.3.2 Step 2: Identify relevant threats for each SCI and initiate respective DCLs
In Step 2, the user selects the relevant threats that will be included in the assessment of each SCI. Typical threats considered in SmartResilience are included in Table 5. Afterwards, the user must initiate a DCL for the selected SCI(s) and threat(s) in the SmartResilience dashboard, as well as providing basic information on the scenario (e.g. scenario name, description, DCL name, type of SCI, threats, and DCL description). In addition, the user (data provider) has to define critical information and values for the identified threats, as these might be needed for the stress test scenario (e.g. the extreme value for water level in a river that would cause a flooding event in a city).
3.1.3.3  Step 3: Consider if the possible interdependencies of the SCI affects the results
Smart cities comprise a number of SCIs, which in many cases are interdependent upon each other. Therefore, in case of a possible disruptive event, a disruption in functionality of one SCI may affect the functionality of another. In order to consider these interdependencies, define the interdependencies between the selected SCIs and check if the FL of other CIs is also affected. These can be considered in evaluation of the FL of the SCI. The user may consider the D2.3 [32] and the D5.1 [24] reports in the SmartResilience project to elaborate further on this step.

3.1.3.4  Step 4: Define FEs for each DCL
For each DCL, the user has to define the portfolio of functionality elements that contributes to the overall functionality of the SCI. At this point, it is important to consider the relevant threats. The FEs should include core functionalities, such as production, flight operations, and key banking services. Figure 6 provides some examples of FEs.

3.1.3.5  Step 5: Define appropriate FIs for each FE in each DCL
In Step 5, appropriate FIs for each FE are defined. Figure 6 provides some examples of FIs.

3.1.3.6  Step 6: Assign maximum, minimum, and target values to all FIs (optionally assign weights)
Assign the maximum, minimum, and target values of functionality indicators. These values should be assigned in terms of measurable units such as percentages, numbers, etc. Minimum, maximum, and target values can be used to define the current FL of the infrastructure as a percentage and to set the stress test limit.
Also assign best values. These are used to decide on the direction of the measurement, i.e. dependent on whether the minimum value is assigned as the best value or if the maximum is assigned as the best value.
For the purpose of simplicity, the default weights are equal. However, the user may choose to assign different weights. In the DCL, these values can be assigned by entering the detailed field in the FI form in the SmartResilience SCI dashboard. More elaborated description of this step is provided in the example case (see A.1.2).

3.1.3.7  Step 7: Assign time values for the scenario
The user has to provide values for the times that characterize the FL-t curve of the possible disruptive event, i.e. where the curve changes the gradient. These times can be broadly categorized as follows:
\[ t_0: \text{time before the event or starting point of the scenario} \]
\[ t_1: \text{time at which the event occurs} \]
\[ t_2: \text{time at which the infrastructure reaches the minimum functionality level} \]
\[ t_3: \text{time at which the infrastructure starts to recover} \]
\[ t_4: \text{time at which the infrastructure reaches the initial functionality level or starting point of a new steady state level} \]
\[ t_5: \text{time at which the infrastructure increases its functionality through learning and adapting or at which the scenario ends} \]
It is recommended to define at least these six time values. However, in some cases, the series of events may differ and the user has the possibility to define more time values than six points. In the SmartResilience dashboard, the user may select the desired number of time points and enter the values for these.

The time can be defined in three different ways, namely:

- Equidistant time
- Relative time (from $t_0$)
- Calendar time

**3.1.3.8 Step 8: Assign values for the FIs at given times**

Assign values for FIs at each point in time. The user has the option of choosing to add real values for the FIs. In this case, the user should also assign maximum, minimum, and target values (best values). Based on these values, the SmartResilience dashboard will calculate the score between 0 to 100 for the FL. The user could also choose to use percentage for each FI. In this case, the SmartResilience dashboard will simply plot the values for FL at different points in the scenario time.

The FL at $t_0$ can be labeled as a typical/current/normal functionality level, and the FL levels for the other points in time would be defined relative to $t_0$.

**3.1.3.9 Step 9: Generate and evaluate the FL-t curve that models the impact of disruption through macro-indicators**

After obtaining the FL-t curve, the following macro-indicators are calculated by the FL assessment tool in the SmartResilience dashboard (as illustrated in Figure 7):

- Robustness
- Disruption time
- Absorption time
- Downtime
- Recovery time
- Recovery rate
- Improvement/adaptation/transformation
- Loss of functionality

**3.1.3.10 Step 10: Consider if the possible interdependencies of the SCI affects the results**

Smart cities comprise a number of SCIs, which in many cases are interdependent of each other. Therefore, in case of a possible disruptive event, a disruption in functionality of one SCI may affect the functionality of another. In order to consider these interdependencies, define the interdependencies between the selected SCIs and check if the FL of other CIs is also affected. The user may consider the D2.3 [32] and the D5.1 [24] reports in the SmartResilience project to elaborate further on this step.

**3.1.3.11 Step 10: Use the result of the functionality level assessment**

Use the result to compare the functionality level assessment (FL-t curve) against the stress test criteria in order to perform benchmarking (i.e. comparing two or more similar SCIs) and to predict the behavior of a SCI.

**Stress test**

The stress test framework is used to test whether, in a given threat situation, the SCI is/will be resilient enough to be able to continue functioning within the prescribed limits. The FL-t curve(s) obtained in step 9 are compared with the stress test criteria and limits in order to evaluate whether the SCI has passed or failed the stress test. In order to do the stress test, the user needs to decide on the thresholds/limits representing acceptable/non-acceptable values for each criterion. The stress test criteria can be related to:

- Functionality Level
- Time (to absorb, to recover)
- Cumulative loss of functionality (area)

Functionality Level ("vertical loss")
The stress test limits can be set based on the overall functionality level, at single functionality element(s), and/or at single functionality indicator(s). The limit could be a certain minimum level of functionality (i.e. the lowest point of the resilience curve should be above this FL_{min}). The functionality level at the lowest point below the curve is sometimes referred to as "robustness," which can be set as a stress test limit. This is illustrated in Figure 8.

![Figure 8: Level of functionality as stress test limit](image)

**Time ("horizontal loss")**

When subjected to a threat/event, a SCI may set the limits on time (e.g. maximum time to absorb the event, maximum time to partially recover after the event, or maximum time to fully recover after the event). The last time interval, i.e. time between when the event occurs and the SCI is fully recovered, is referred to as disruption time when modeling the impact of a disruptive event (see Section 3.1.2). This is sometimes also referred to as "rapidity" and can typically be used as a stress test limit. For example, the stress test limit could be the time from when the event occur until 90% of the functionality is restored, or some combination of various criteria. This is illustrated in Figure 9.

![Figure 9: Time as stress test limit](image)
Loss of functionality (area)

As explained in Section 3.1.2, loss of functionality is the functionality of the SCI that is lost in a given threat situation. In Figure 10, the maximum allowed cumulative loss of functionality is illustrated as area \( A_2 \). The actual (or assumed/assessed) loss of functionality area can be smaller (\( A_1 \)) or larger (\( A_3 \)) than the limit, leading to either success or failure of the stress test, as illustrated in Figure 10.

![Figure 10: Loss of functionality surface as stress test limit](image)

The example of a stress test in Figure 11 illustrates three alternative FL-t curves for one specific functionality level (whether it is on overall, element, or indicator level) of the SCI. The stress test criterion is, in this case, only related to the level of functionality, as in Figure 8 (not to time or surface/area).

![Figure 11: Comparing the FL curve with the stress test criteria](image)

The alternative shown by the small dotted line is at all times above the stress test limit, which means that it clearly passes the stress test. Also, this alternative recovers faster and achieves better FL than before the adverse event. The alternative shown by the continuous curve touches the stress test limit; hence, it barely passes the stress test. Also, in this alternative, the recovery occurs slower than in the first alternative, and the new FL is below the initial FL. The last alternative shown by the line with long dashes falls below the stress test limit and therefore fails the stress test. Furthermore, it recovers the slowest and to a level much lower than the initial functionality level.

The case illustrated in Figure 11 uses only functionality level as stress test criteria. The exact points in time of \( t_0 \) to \( t_5 \) are not important, as time is not part of the criteria. However, if time is used (as shown in Figure 9) or if the surface for "loss of functionality" is used (as shown in Figure 10), then it is also necessary to assign/log the values for the times \( t_0, t_1, t_2, t_3, t_4, t_5 \) in addition to the corresponding FL values.
Benchmarking (comparing with others)

The methodology proposed for functionality assessment can be used for benchmarking, i.e. comparing the functionality of different SCIs. This comparison can be done between similar types of SCIs. This could help in understanding best practices undertaken by one SCI and how another SCI could improve and invest to ensure better business continuity, resilience, etc.

**FL assessment may also be used to predict the behavior of a SCI during a disruptive event**

Measuring functionality over time may also help to predict the behavior of a SCI. If the SCI learns from a previous event and undertakes certain measures to deal with events in future, it may have better functionality if it is subjected to a similar situation again. This could lead to better resilience, i.e. better absorb capacity, faster recovery, smaller loss of functionality, better adaptive capacity, and shorter downtime (see Figure 13). Furthermore, in case of a different event, the behavior of the system can change and be recorded. This could be useful for devising measures to adapt/transform from the event to improve resilience of the SCI.
4 SmartResilience methodological framework

As discussed in section 1.1.2, the FL assessment is one of the three pillars in the SmartResilience methodology, in addition to the Resilience Assessment Methodology in task 3.2 [1] and optimization of resilience based on the decision-making models, such as MCDM in task 3.4. The contribution of each pillar is detailed in Figure 14. The pillars may be conducted in a flow as shown in Figure 14, but they can also be conducted mostly independently based on the needs of the end-users. The end-user can choose between the following options (and combinations of these options):

1. RL assessment
2. RL assessment + MCDM
3. FL assessment
4. Stress testing (including specific FL assessment)

These options can be performed once or repeatedly. The methodology for FL assessment is proposed in Chapter 3. The resilience level assessment proposed in T3.2 [1] can benefit from FL assessment by identifying the weak areas in different phases of the resilience cycle. This can be accomplished by assessing the FL in a particular scenario and plotting the relevant curve, which can then provide information about various macro-indicators. If the curve is obtained correctly by considering the core functionality elements, the FL assessment provides insights about the outcomes of a disruptive event (scenario) in terms of the change in the FL of the SCI. Once the change in FL is plotted, the loss of functionality is obtained. The CI operators may conduct a stress test to check if the SCI is able to sustain its minimum threshold criteria during the scenario. Considering this information, the SCI operators may consider these outcomes while doing the resilience assessment, as the stress test provides information on strong and weak points in the SCI.

After doing the resilience level assessment of the SCI, findings are used further in the MCDM methodology to identify the best optimization alternatives for improving resilience of the SCIs and investing in them.

In addition, it should be noted that the level structures in functionality assessments and resilience assessments are different. Level four in resilience assessment [1] consists of “phases” of the resilience cycle; in functionality assessment, this level does not exist. Also, in relation to level five, i.e. resilience issues in the RL method, the FL method involves FEs (i.e. single functionalities of the CI which contribute to the overall functionality of the CI, e.g. production). Furthermore, level six, i.e. RIs in RL method, is comparable to FIs in FL method. The MCDM methodology is essentially structured based on the resilience assessment structure. In addition, each resilience assessment forms part of the Optimization Alternatives (OpAs) in MCDM methodology. Optimization Alternatives are used to evaluate the best alternative against the criteria (e.g. cost, time, change in RL, etc.) defined by the end-users.

Further, functionality level assessment methodology is based on FIs; it provides a direct measurement of loss of resilience (and test of acceptability, through stress testing). Resilience assessment methodology [1], in comparison, is based on RIs and provide an indirect measurement of resilience (see Figure 14). These RIs address the issues important for the CI and contribute to its resilience in different phases of the resilience cycle, i.e. understand risk, anticipate/prepare, absorb/withstand, respond/recover, and adapt/transform. By undertaking Optimization Alternatives decided through MCDM to improve the resilience in each phase, the system becomes resilient against an identified threat, thereby reducing the threat’s impact and ensuring continuous functioning.

With the support of these proposed methodologies, the SmartResilience project aims to answer the questions listed in the this chapter.
SmartResilience: Indicators for Smart Critical Infrastructures

SmartResilience – D3.3 Modeling the impact of an adverse event on the "absorb" and "recover" capacity of a smart critical infrastructure (SCI), based on resilience indicators

Main CI:
- Risk
  - FI
- Functionality Element
- Phase
- macrow
- RI
- MACRO
- CRITERIA
- Dimensions
- Indicators

Outcome of a Disruptive Event
- Resilience of an Infrastructure
- Investment in Resilience Optimization

Solution path

Results
- Functionality Level (FL) at times during the scenario & stress-test
- Resilience Level (RL) at given times
- Best optimization alternative for improvement in the Resilience Level

Macro-indicator: FL per phase

CI: Critical Infrastructures; FI: Functionality Level of the Infrastructure; FE: Functionality Element; Fl: Functionality Indicator; RI: Resilience Indicator; OpA: Optimization Alternative, RL: Resilience Level; t: time; V: Value

Figure 14: Differences in resilience and functionality level assessment of a SCI
4.1 What is the possible outcome of an assumed adverse event scenario? Will the functionality remain within the prescribed limits?

SmartResilience answers this question based on the methodology proposed in chapter 3.

4.2 How should resilience be monitored?

SmartResilience examines resilience indicators to demonstrate how an infrastructure is prepared for an adverse event, how it can withstand the event, and then how it can recover, possibly adapting afterwards. The assessment result is the “Resilience Level” (a number/a composite indicator) that allows for comparison of one infrastructure against other infrastructures (i.e. “benchmarking”) and/or monitoring of changes and trends in resilience over the operation time (Figure 15). One possible way to do this is to select a few indicators and monitor them on a frequent basis. This is referred to as “short-term monitoring.”

The assessment of the resilience level can be made in the SmartResilience dashboard. In order to assess and monitor the level of resilience, the user needs to create a Dynamic Checklist (DCL). The DCL consists of issues and indicators for each issue, which are relevant from the particular infrastructure’s perspective. The view of the DCL from within the system is shown in Figure 16.
After the DCL is finished, the user shall fill in the values for all selected indicators and define the minimum, maximum, and target values for each of the indicators.

4.3 Investment in resilience optimization: How is the best value for money obtained?

In order to reduce harmful impact on the infrastructure from an adverse event, one should consider increasing the level of resilience by implementing protective and corrective measures. Enhancing the RL of a SCI reflects a complex decision process that is comprised of multiple conflicting criteria, both quantitative and qualitative. MCDM models are suitable to deal with these type of decisions. Decisions are dependent on the available resources, needs, and requirements of each particular SCI, and therefore they differ from one SCI to another. In order to make a decision regarding the optimal investment in resilience strengthening, according to the method proposed within the project, the user has to consider/define the following:

- **Alternatives** - possible options
- **Criteria** - a set of principles or standards by which the decision may be made
- **Weights** - importance of each criterion
- **Values** - possible values for scoring each alternative
- **Decision** - choice between Optimization Alternatives (OpAs) based on multiple criteria

Single alternatives are equal to indicators values. In the proposed method, the user does not consider single alternatives but rather considers a portfolio of Optimization Alternatives (OpAs). Implementation of these measures (portfolios), e.g. educating people, improving communication, investing in new equipment, etc., leads to improving the resilience level (ΔRL) of an infrastructure, but this investment will have its own associated costs and time needed for implementation. In the decision-making process, different criteria (which may have different importance and/or weights from the user’s perspective) can be taken into account and included into the search for the optimal portfolio of measures to improve resilience, either phase-wise or dimension-wise (refer to Figure 17).

To make a structured decision within the context of the SmartResilience project, the following steps should be taken:

1. **Define the decision problem** - create a DCL in the SmartResilience Dashboard (Indicator-based creation of the decision problem)
2. **Define the current status of resilience** (assign values to the indicators)
3. **Define decision alternatives**, i.e. Optimization Alternatives (OpAs)
4. **Define important criteria to appraise the alternatives against** (Methodology developed within SmartResilience projects suggests using at least the following: ΔRL - positive change in resilience after the corrective measures were implemented, Cost, and Time of implementation)
Step 5. Set criteria weights (if they are not equivalent)
Step 6. Appraise the alternatives according to the specified criteria
Step 7. Choose the best alternative amongst the options

The outcome of the assessment is shown in the chart and tabular summary in Figure 17. As mentioned previously, the method proposed in the SmartResilience project enables specification of in which phase of the resilience cycle the investment will be the most beneficial. Through the SmartResilience project method, it is also possible to specify in which dimension(s) the improvement should be made. The latter is particularly important from the Critical Infrastructure owners/operators perspective because it allows these individuals to decide in which sector (dimension) the biggest investment should be made. The assessment results indicate where investment is needed the most, such as in physical systems of the infrastructure protection (e.g. fences) versus in information gathering systems, etc.
SmartResilience – D3.3 Modeling the impact of an adverse event on the “absorb” and “recover” capacity of a smart critical infrastructure (SCI), based on resilience indicators

Outcome: Improvement in the Resilience Level for particular RIP per PHASE

**ΔRL Improvement (per phase)**

**EXAMPLE OF THE IMPROVEMENT IN RESILIENCE:**

<table>
<thead>
<tr>
<th>Category</th>
<th>Current status</th>
<th>Action</th>
<th>Improved value for RIP 1</th>
<th>Improved value for RIP 2</th>
<th>Improved value for RIP 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>People qualified?</td>
<td>5</td>
<td>More trainings</td>
<td>6</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>System/physical</td>
<td>5</td>
<td>Increase scope</td>
<td>7</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>Equipment ok?</td>
<td>5</td>
<td>Invest in assets</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

CRITERIA FOR THE RIP SELECTION:

$$\Delta R = R_{RL} - R_{RL_{current}}$$

- time for implementation
- € cost

Legend:
- The higher value, the better score
- The lower value, the better score

**RESULTS:**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>RIP 1</th>
<th>RIP 2</th>
<th>RIP 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δ RL</td>
<td>0.58</td>
<td>0.31</td>
<td>0.41</td>
</tr>
<tr>
<td>Time for Implementation (days)</td>
<td>90</td>
<td>90</td>
<td>90</td>
</tr>
<tr>
<td>Cost (€)</td>
<td>5 000</td>
<td>3 000</td>
<td>12 000</td>
</tr>
<tr>
<td>Overall RIP value</td>
<td>0.57</td>
<td>0.17</td>
<td>0.21</td>
</tr>
</tbody>
</table>

Recommended solution: RIP 1

Figure 17: Investment in resilience optimization - concept
5 Application examples

Reiterating Chapter 3, the SmartResilience method for defining SCI functionality follows 10 main steps (as shown in Table 4) and is supported by the tools of the SmartResilience dashboard.

5.1 Single infrastructure

This example, which is taken from the ECHO case study in SmartResilience, assesses the functionality of a petro-chemical plant that experienced an explosion.

5.1.1 Step 1: Select the SCI(s) to be assessed

The smart industrial zone in BRAVO city consists of several major infrastructures, one of which is the oil refinery. These infrastructures are interconnected and interdependent, and the entire zone is regarded as one large CI or CIs.

5.1.2 Step 2: Identify relevant threats for each SCI and initiate respective DCLs

This example will focus on one possible scenario from the ECHO case study: a BLEVE (boiling liquid expanding vapor explosion), which is identified as the major accident with the most severe potential consequences based on calculation and modeling conducted and presented in the safety report. Suppose that following a leakage from a hydrogen reservoir, which is a pressurized vessel, this reservoir explodes, sending a shock wave and debris to neighboring infrastructures. The consequences of such an explosion could hypothetically have a “domino” effect due to thermal radiation and flying debris [24].

The relevant threats are both unintentional, such as disasters or poor maintenance, and intentional, such as terror/criminal attacks.

Following the explosion event, a Dynamic Checklist (DCL) is setup in the SCI Dashboard application.

5.1.3 Step 3: Consider if the possible interdependencies of the SCI affect the results

In this particular case, other SCIs’ effects are not relevant for consideration. The effects of the refinery’s functionality loss on other SCIs will be considered at the end of the assessment.

5.1.4 Steps 4 and 5: Define FEs and FIs for each DCL

Functionality Elements (FEs) and Functionality Indicators (FIs) are defined to reflect the assessed functionality levels in the scenario. Note that functionality is defined by the assessor on a per-case basis and depends on the desired results; in this case, functionality is measured by the refinery’s output, and the FEs and FIs are defined to measure this. Sample FEs and FIs are listed below in Table 6.

Table 6: Sample FEs and FIs in the ECHO case study

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element</td>
<td>Production performance</td>
<td>The production output is one of the key functions of any infrastructure, e.g. for the example of a refinery, the total volume of oil produced per day, and in an airport, the total number of flights operated each day, etc.</td>
<td>Source: GRI G4 (2013) [12]</td>
</tr>
</tbody>
</table>
SmartResilience: Indicators for Smart Critical Infrastructures

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Domestic gas production</th>
<th>Level of the production measured in million m³/day</th>
<th>Source: GRI G4 (2013)[12] Predefined values:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;High&gt;: x ≥ 80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;Medium&gt;: 80 &gt; x ≥ 70</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;Average&gt;: 70 &gt; x ≥ 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;Low&gt;: 50 &gt; x ≥ 30</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt;Very low&gt;: x ≤ 30 [million m³ /day]</td>
</tr>
</tbody>
</table>

| Indicator | Overall Equipment Effectiveness (OEE) | This indicator is used as an operational measure to monitor production performance. | Source: Anderson, C., Bellgran, M. (2015) OEE = (TotalAvailableTime- (PlannedDowntime+Breakdown+Setup+Adjustments+Idling+MinorStoppages+ReducedSpeed+QualityLosses)) / (TotalAvailableTime-PlannedDowntime)*100 |

The complete list of FEs and FIs that are assigned to the case’s DCL are shown in Figure 18.

Figure 18: FE and FI used in ECHO case, BLEVE scenario

5.1.5 Step 6: Assign maximum, minimum, and target values to all FIs (optionally assign weights)

Maximum, minimum, and target values of functionality indicators are assigned in this step.

5.1.6 Step 7: Assign time values for the scenario

Based on the scenario, the case’s time values are categorized as follows (see Figure 19):

- t₀: time before the event or starting point of the scenario
- t₁: time at which the BLEVE occurs
- t₂: time at which the refinery’s output reached the minimum functionality level
- t₃: time at which the refinery contained the event and starts to recover
\( t_4 \): time at which the refinery reaches the initial functionality level or starting point of a new steady state level

\( t_5 \): time at which the refinery increases its functionality through learning and adapting, or at which the scenario ends

---

5.1.7 **Step 8: Assign values for the FIs at given times**

Values are assigned for the FIs at each point in time (refer to Figure 20). The FL at \( t_0 \) is considered as a typical/current/normal functionality level, and the FL levels for the other points in time are defined relative to \( t_0 \).
Figure 20: Assigned FI values and resulting FE calculated values

5.1.8 Step 9: Generate and evaluate the FL-t curve that models the impact of disruption through macro-indicators

The results for the assessment are plotted as a functionality over time (FL-t) curve to visualize the effects over time (see Figure 21). Given actual (real) times, the assessor can then easily recognize and calculate the areas of functional loss and devise macro-indicators that can be used for benchmarking (see Chapter 3.1).
5.1.9 **Step 10: Consider if the possible interdependencies of the SCI affects the results**

These results should be considered in relation to neighboring and connected infrastructures that are reliant on the SCI’s functionality, using the resulting macro-indicators to identify whether critical thresholds (as stress testing limits) were crossed or in danger of doing so, thereby requiring immediate action. Figure 8 demonstrates a stress test limit.

### 5.2 Infrastructure-of-infrastructures

The functionality assessment process can also be applied for an infrastructure-of-infrastructures by splitting it into its component SCIs, assessing each component SCI under the same functionality definitions (including considering interdependencies), and aggregating the results back into one assessment. In the SCI Dashboard application, this can be accomplished by performing the additional assessment within the same case study and setting the time points on the same schedule.

Deliverable D5.11 in SmartResilience – case study INDIA – involves multiple SCIs that are interconnected in the case’s smart city BRAVO. The FL-t curve below in Figure 22 depicts the effects the scenario had on the functionality of ECHO and HOTEL:

![Figure 22: Multiple FL-t curve for ECHO (blue) and HOTEL (orange) in INDIA](image-url)
6  Conclusions

6.1 General

Task 3.3 aims to understand the outcome of a possible/assumed adverse event on a critical infrastructure. To do so, the SmartResilience project looks primarily at the functionality of an infrastructure to model the impact of a disruptive/adverse event based on indicators.

In line with this objective, Task 3.3 describes the SmartResilience functionality level assessment methodology. The functionality level of an infrastructure uses different aspects (“elements”) of its functionality (e.g., material production/output performance, security system performance) and indicators to estimate the SCI functionality level over scenario time. The functionality level assessment methodology enables users to select the most appropriate functionality elements and indicators for their particular case, following 10 main steps.

By following these 10 main steps, the user is able to estimate the following functionality related macro-indicators: robustness, disruption time, absorption time, downtime, recovery time, recovery rate, improvement/adaptation/transformation, and loss of functionality. These macro-indicators can be used to model the impact of a disruptive/adverse event.

In addition, users can further use the functionality level assessment for:

- Stress testing the resilience of the SCI, i.e., analyzing if the behavior of the CI remains within the safety margins of operation in the case of an assumed disruptive/adverse event
- Benchmarking best practices undertaken by other SCIs
- Predicting SCI behavior in case of a disruptive/adverse event

In summary, the SmartResilience functionality assessment methodology will enable users to assess the impacts of disruptive/adverse events by assessing the behavior of infrastructures and gathering insights about an infrastructure’s ability to “absorb” the shock, as well as its “recover” capacity. It may also be able to contribute to resilience assessment by analysis of loss of functionality.

Furthermore, this methodology provides a basis for modeling the impact of a disruptive event not only for the SCIs within the project but also for other SCIs outside the project, including cities and member states within the EU. The project will be focusing on collaboration and exploitation activities such as standardization to ensure wider acceptance of this methodology.

6.2 Alignment of approaches to resilience

Exercises like the EU Workshop (conducted in conjunction with the Community of Users Meeting on September 13-14, 2017) confirm the need to increase levels of collaboration with the goal to increase the level of alignment of approaches, metrics, and tools. Apart from such exercises, targeted agreements and joint projects among institutions active in the area are necessary. An example of such a targeted agreement is the agreement between ANL and EU-VRi (see Figure 23), which covers issues such as resilience indicators, resilience assessment methods, resilience assessment tools, and resilience auditing and certification, as well as the networking of stakeholders, projects, and data pools.
6.3 Possible standardization path

Based on the work in different parts of the EU and other projects, as well as the work related to the ISO 31000 standard (revision 2 released in 2018, the initial revision 1 in 2009) and the standards of the ISO 223xx family, much of the current alignment in the risk and resilience standardization is focused on the effort to create an aligned procedure on how to manage emerging (i.e. new/unknown) risks coupled with the concepts of risk management and resilience management covered by the ISO 223xx-series of standards. Practically, this will mean establishing an internationally agreed-upon procedure on how to look (“scan the horizon”) for emerging risks and proposing metrics for assessing resilience. A New Work Item Proposal (NWIP) on “Emerging risks and resilience” is being prepared as a new standard in the ISO 31000:2018(E) family of standards. It will include, but will not be limited to, terminology, criteria, principles, and technical specifications for the procedures and their implementation. In addition, it will include recommendations for the definition of common metrics, primarily in the form of indicators, both for the characterization of emerging risks and for definition of the resilience framework.

References


International Organization for Standardization.

doi: 10.1038/nclimate2227 (2014).

Resilience based Early Warning Indicators. SINTEF report A22026 (2012).

Requirements.Termsanddefinitions.In:Termsanddefinitions.Switzerland:Inter-
ANNEXES

Annex 1  Functionality assessment
Annex 2  Review tables
Annex 1 Functionality assessment

A.1.1 Functionality level calculation

The functionality level estimation is computed taking into account the user assessment for each functionality indicator at \( t_0 \) (current value of functionality indicator) as a reference. Given that functionality indicators can use different measures (numbers, fractions, frequencies, etc.) and corresponding scales, the values are normalized using the following equations based on whether the best/target value is the minimum or the maximum value:

- If the best value is the minimum (as a percentage):
  \[
  F_{I_i}^{\text{norm}} = \frac{\max(F_{I_i}) - F_{I_i}}{\max(F_{I_i}) - \min(F_{I_i})} \times 100
  \]

- If the best value is the maximum (as a percentage):
  \[
  F_{I_i}^{\text{norm}} = 1 - \frac{\max(F_{I_i}) - F_{I_i}}{\max(F_{I_i}) - \min(F_{I_i})} \times 100
  \]

Next, the user needs to assess the values for each functionality indicator at the remaining times in relation to the functionality for that indicator at \( t_0 \).

When the user enters the values (time points and corresponding functionality levels) in the SmartResilience Dashboard, the system computes an estimation of the functionality level, i.e. combines the indicators, based on equivalent weights (the default option). However, the user has the option to assign weights to each functionality indicator. In this case, the system will follow the weighted sum model, where the functionality level of the SCI is calculated according to the following equation:

\[
FL = \sum_{i=1}^{n} F_{I_i}^{\text{norm}} \cdot w_i, \text{ where } w_i > 0 \text{ for all } i = 1, \ldots, n \text{ and } \sum_{i=1}^{n} w_i = 1
\]

where: \( FL \) is the functionality level, \( F_{I_i}^{\text{norm}} \) is the normalized assessment of \( F_{I_i} \), \( w_i \) is the weight concerning the \( F_{I_i} \), and \( n \) is the number of functionality indicators.

A.1.2 Application of functionality assessment: HOTEL case study: smart energy supply system (Helsinki)

This section aims at applying and testing the functionality assessment for the HOTEL case study, which represents an energy supply CI. The case study was developed in collaboration with the HOTEL case study partners.

Step 1: Select the SCI(s) to be assessed

The HELEN Oy is a city-owned energy company that provides district heating supply, cooling, and electricity for the city of Helsinki (Finland). The energy generation system from the large underground fuel storage is a unique system that was established in 2004. For the case study, the district heating supply infrastructure was selected as the SCI to be assessed. A network of suppliers in the city provides district heating. This has an impact on the possibility of back-up heating in case of an adverse event and influences how critical a disruption would be for the society.

Step 2: Identify relevant threats for each SCI and initiate respective DCLs

The HOTEL case study partners identified one of the possible relevant threats as a new-technology related accident triggering a fire. If a fire is triggered in the underground fuel storage facility, it could have significant
impacts on the citizens’ lives during a cold winter (details about the HOTEL case are provided in [24]). In the SmartResilience SCI dashboard, a DCL was initiated and basic information related to the case was provided, as shown in Figure 24 (Only one DCL was initiated, since there was just one SCI and one threat assessed in this case).

Figure 24: Initiating a DCL in the SCI dashboard (DCL Step 1)

Step 3: Define FEs for each DCL

The FEs relevant for the HOTEL case (single) DCL are:

1. CORE: District heat production and supply from Salmisaari plant, Helsinki
2. HSE: Health, Safety, and Environment performance
3. Inter-connectedness of the district heating system
4. Economic performance of the Salmisaari plant

In the DCL, the relevant FEs were selected for the functionality assessment, as shown in Figure 25.
Step 4: Define appropriate FIs for each FE in each DCL.

In the HOTEL case study, the FIs chosen for each FE (for the single DCL) were:

1. **CORE**: District heat production and supply from Salmisaari plant, Helsinki
   1.1. Number of people supplied with district heating;
   1.2. Production for district heating (percentage of the full capacity);
2. **HSE**: Health, Safety and Environment performance;
   2.1. Percentage of working hours of relevant personnel (lost due to incidents);
3. **Inter-connectedness of district heating system (with the healthcare system)**;
   3.1. Percentage of production for district heating from another major plant;
   3.2. Number of high priority people supplied with district heating;
4. **ECONOMY**: Economic performance of the Salmisaari plant;
   4.1. G4-9: Revenues (% of production at full capacity);

In the DCL, FIs were assigned to the respective FEs, as shown in Figure 26.
Step 5: Assign maximum, minimum and best values to all FIs (optionally assign weights)

In the DCL, maximum, minimum, and best values were assigned to all FIs (see Figure 27). The weights were considered equivalent for each FI.

Figure 26: Selection of the FIs for the HOTEL case (DCL Step 3)

Figure 27: Assign maximum, minimum, and best values to the FI (DCL Step 4)
Step 6: Assign time values for the scenario

The time values for this scenario were defined in terms of relative time, as shown in Figure 28:

- **t₀ (0th hour):** Self-heating/auto ignition occurs in silos, the plant running at 100% of the system capacity.
- **t₁ (6th hour):** Operator intervention starts, water into the silos, removal of heat starts. The plant is still running at 100% of the capacity.
- **t₂ (11th hour):** Heated fuel causes conveyor damage, plant reaches to minimum the power (40%); Automatic alarm reaches the rescue services.
- **t₃ (16th hour):** The storage is non-functional. The plant continues to operate at 40% capacity as they get the fuel from different plants by truck (Hanasaari plant).
- **t₄ (130th hour):** The conveyor belt has been repaired, and Salmasaari plant starts to operate at full capacity (100%).
- **t₅ (300th hour):** The nearby heating plant is also recovered and running at 100% of the capacity so that all parts of the western district are supplied with heating as required by the demand.

![Figure 28: Assign time values in the SCI dashboard (DCL Step 4)](image)

Step 7: Assign values for the FIs

In the DCL, FIs values were added for the different times during the scenario (see Figure 29).
Step 8: Generate and evaluate the FL-t curve that models the impact of the disruption through robustness, absorption time, disruption time, downtime, recovery time, recovery rate, loss of functionality, and improvement/adaptation/transformation.

Once the values were assigned, the FL-t curve was generated by the system for the HOTEL case, as shown in Figure 30.

These results can then be used for evaluating the impact of the disruptive event.

Robustness = 70 / 83.33 = 84%
Absorption time = 15 - 10 = 5 hours
Downtime = 0 h
Loss of Functionality = (83.33 - 70) / (130 - 6) = 0.1% / hour
Recovery time = 130 - 16 = 114 hours
Recovery rate = (83.33% - 70.83%) / (130h - 16h) = 0.110% / hour
Disruption time = 130 - 6 = 124 hours
Improvement/adaptation/transformation = 0%
**Step 9: Identify interdependencies between the selected SCIs**

The energy supply infrastructure in Helsinki, Finland, is dependent on the electricity supply and drinking water supply Cis, and it provides input to the hot water supply infrastructure. Hence, these infrastructures will be affected/affect the Salmasaari plant.

**Step 10: Use the result of the functionality level assessment**

To compare the FL-t curve against the criteria, evaluate the stress test result. For example, the minimum functionality of the Salmasaari plant should not reach below 60%. In the example above, the lowest functionality level was 70%. Hence, the SCI passed the stress test.
Annex 2  Review tables

The review tables will be provided in the Periodic Report submitted to the European Commission.