H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure
D3.6 - Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures

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
Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures

Report Title: Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures (SCIs)


Responsible Project Partner: SINTEF
Contributing Project Partners: EU-VRi, IVL, VTT, FhG-INT, BZN, MUW, NIS

Document data:
- File name / Release: D3.6 Resilience assessment guideline_v45ko29112018
- Pages: 124
- Status: Final
- Dissemination level: PU

Project title: SmartResilience: Smart Resilience Indicators for Smart Critical Infrastructures
- Grant Agreement No.: 700621
- Project No.: 12135

WP title: WP3. The SmartResilience indicator-based methodology for assessing, predicting & monitoring the resilience of SCIs for optimized multi-criteria decision-making
- Deliverable No.: D3.6

Date:
- Due date: November 30, 2018
- Submission date: November 30, 2018

Keywords: Resilience, resilience assessment, resilience methodology, infrastructure resilience level

Reviewed by:
- Nils Albrecht
- Thomas Knape

Review date:
- November 12, 2018
- November 23, 2018

Approved by Coordinator:
- A. Jovanović

Approval date: November 30, 2018

Trondheim, November 2018
## Release History

<table>
<thead>
<tr>
<th>Release No.</th>
<th>Date</th>
<th>Description / Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>June 30, 2017</td>
<td>Preliminary version as part of MS2. First version ready for testing and validation in WP5. (In addition, MS1 and MS2 were carried out as an event on June 29, 2017, with presentations).</td>
</tr>
<tr>
<td>2</td>
<td>November 28, 2017</td>
<td>Second version with latest updates prior to testing and validation in WP5.</td>
</tr>
<tr>
<td>3</td>
<td>October 28, 2018</td>
<td>Complete draft sent to task partners for comments. The main change is a new chapter on dependency analyses as a “forth pillar” of methodologies in SmartResilience.</td>
</tr>
<tr>
<td>4</td>
<td>November 7, 2018</td>
<td>Draft version for review by internal reviewers.</td>
</tr>
<tr>
<td>5</td>
<td>November 29, 2018</td>
<td>Final version for approval by Coordinator.</td>
</tr>
<tr>
<td>6</td>
<td>November 30, 2018</td>
<td>Final version submitted to EC.</td>
</tr>
</tbody>
</table>

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

These are the main questions tackled by the SmartResilience project.

The project envisages answering the above questions in several steps: (#1) By identifying existing indicators suitable for assessing resilience of SCIs, (#2) By identifying new smart resilience indicators including those from Big Data, (#3) By developing, a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix, (#4) By developing the interactive SCI Dashboard tool, 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 benchmarking the best-practice solutions and identifying the early warnings, improving resilience of SCIs against new threats and cascading and ripple effects. The benefits/savings to be achieved by the project will be assessed by the reinsurance company participant. The consortium involves seven leading end-users/industries in the area, seven leading research organizations, supported by academia and lead by a dedicated European organization. External world leading resilience experts are included in the Advisory Board.
Executive Summary

WHAT
This guideline describes *HOW* to use the methodology for assessing, predicting and monitoring/optimizing resilience of Smart Critical Infrastructures (SCIs), including dependency analyses, and the tools needed. Also, examples of resilience indicator checklists are included.

Assessing, modelling and monitoring resilience (3) and analyzing dependencies (+1) constitute the four main pillars of methodology in the SmartResilience project. The four pillars provide seven methods, listed in the table below.

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Method</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Resilience level assessment</td>
<td>Resilience level (RIL)</td>
</tr>
<tr>
<td>2</td>
<td>Functionality level assessment &amp; Stress-testing</td>
<td>Functionality level (FL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical FL versus criteria/threshold</td>
</tr>
<tr>
<td>3</td>
<td>Monitoring &amp; Optimization (MCDM)</td>
<td>Resilience progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optimal improvement measures</td>
</tr>
<tr>
<td>4</td>
<td>Interdependency identification &amp; Cascading effects loss estimation</td>
<td>Relevant interdependencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Loss from cascading effects</td>
</tr>
</tbody>
</table>

One or more methods can be selected for use, but some of the methods are dependent of some of the other methods, e.g. optimization using Multi Criteria Decision Making (MCDM) will typically require resilience level assessment of the various alternatives.


General advice for the use of the methods and tools are provided related to legislation, organizational factors and ethics, including quality criteria for indicators, and examples are provided using four case studies from the SmartResilience project.

WHY
The main reason to use the resilience methodologies and tools described in this guideline is that they provide new and complementary means to cope with rare events (simple and complex, known and unknown, intended and unintended, in networks and network of networks, in conventional systems and smart systems) affecting critical infrastructures, as compared to traditional risk assessments, emergency preparedness and business continuity planning.

WHO
The main user is the person – within a city or area, or a specific SCI – who is responsible for performing the resilience assessment, prediction or monitoring, including carrying out necessary calculations.

This can be an in-house person performing e.g. self-assessment, or it may be an external assessor performing assessments on behalf of e.g. infrastructure owners/operators, city officers/planners, regional authorities, or national agencies.
Table of Contents

Release History ........................................................................................................ i
Executive Summary .................................................................................................. iii
List of Figures .......................................................................................................... vi
List of Tables ........................................................................................................... viii
List of Acronyms ....................................................................................................... ix

1 Introduction ............................................................................................................. 11
  1.1 About the guideline .......................................................................................... 11
    1.1.1 Limitations - what is outside scope? .................................................... 14
    1.1.2 Guideline structure .............................................................................. 14
    1.1.3 General concepts, terms and definitions ............................................ 14
  1.2 Intended reader ................................................................................................. 15
  1.3 How to use the guideline .................................................................................. 15

2 Resilience assessment ............................................................................................ 18
  2.1 Introduction and purpose ................................................................................ 18
  2.2 Basic concepts and terms .............................................................................. 19
    2.2.1 Concepts of issues and indicators ....................................................... 19
  2.3 Method description – resilience level assessment ........................................ 20
    2.3.1 Define the scenario (scope) ............................................................... 20
    2.3.2 Define the analysis framework ......................................................... 22
    2.3.3 Perform the analysis (“calculate”) ..................................................... 26
    2.3.4 Use the results and make decisions .................................................. 30
  2.4 Conclusion ....................................................................................................... 31
  2.5 Application examples ...................................................................................... 33

3 Resilience modelling – functionality assessment and stress-testing .................. 41
  3.1 Introduction and purpose .............................................................................. 41
  3.2 Basic concepts and terms .............................................................................. 42
    3.2.1 Concepts of functionality level, elements, and indicators .............. 42
    3.2.2 Characteristics of the critical functionality curve – macro-indicators 42
    3.2.3 Concept of stress-testing ................................................................. 44
  3.3 Method description – functionality level assessment ..................................... 44
  3.4 Method description – stress-testing ............................................................... 49
  3.5 Conclusion ....................................................................................................... 52
List of Figures

Figure 1: Resilience phases and loss of critical functionality ................................................. 14
Figure 2: Connections between the methodologies ................................................................. 16
Figure 3: The six levels in the hierarchical model ................................................................. 18
Figure 4: Issues measured by indicators ............................................................................. 19
Figure 5: Issues measured by indicators (indicator coverage) ............................................... 20
Figure 6: Scoring process ..................................................................................................... 30
Figure 7: Resilience assessment by indirect measurements using indicators ....................... 32
Figure 8: Example of scenario definition (area – SCIs – threats) ......................................... 33
Figure 9: Defining/identifying issues (level 5) within the phases – for threat no. 1 ............... 34
Figure 10: Defining/identifying issues (level 5) within the phases – for threat no. 2 .......... 34
Figure 11: Identifying indicators for each issue ................................................................... 35
Figure 12: Trending of overall resilience level - example ..................................................... 38
Figure 13: Resilience status at different levels - example ..................................................... 39
Figure 14: Critical functionality curve and its characteristics ............................................... 41
Figure 15: The four-level structure for functionality assessment of a smart city ................. 42
Figure 16: Functionality level, elements and indicators ....................................................... 42
Figure 17: Stress-testing SCIs using the resilience curve (based on [29]) ............................... 44
Figure 18: Examples of functionality elements and indicators ............................................ 46
Figure 19: Improving resilience .......................................................................................... 48
Figure 20: Benchmarking one SCI with another ................................................................. 49
Figure 21: Functionality level as stress-test limit ................................................................. 50
Figure 22: Time as stress-test limit ...................................................................................... 50
Figure 23: Loss of functionality surface as stress-test limit ............................................... 51
Figure 24: Comparing the FL curve with the stress-test criteria ........................................ 51
Figure 25: FE and FI used in ECHO case, BLEVE scenario .................................................. 53
Figure 26: ECHO case time series for BLEVE scenario ....................................................... 54
Figure 27: Assigned FI values in the ECHO case ................................................................. 54
Figure 28: FL-t curve and results table for the ECHO case ................................................... 55
Figure 29: Calculated values of the macro-indicators for the ECHO case ............................ 56
Figure 30: Assessing interdependencies of critical infrastructures in SmartResilience ... 61
Figure 31: Conceptual model for analysis of cascading effects [31] .................................... 62
Figure 32: Dependencies and interdependencies between infrastructures [27] ......... 63
Figure 33: Schematic overview of the ABM [36] ................................................................ 64
Figure 34: The data upload functionality in the SCI dashboard ........................................... 65
Figure 35: Workflow for use of big data indicators [54] ...................................................... 66
Figure 36: Main menu in the tool ....................................................................................... 68
Figure 37: Links between main methodologies and relevant parts of the tool .................... 69
Figure 38: Providing case study name and description ......................................................... 70
Figure 39: Adding a new scenario and examples of existing scenarios .............................. 70
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Short description of the resilience phases</td>
<td>15</td>
</tr>
<tr>
<td>Table 2</td>
<td>Short description of the dimensions</td>
<td>15</td>
</tr>
<tr>
<td>Table 3</td>
<td>Methods and results</td>
<td>16</td>
</tr>
<tr>
<td>Table 4</td>
<td>Scores and resilience levels</td>
<td>18</td>
</tr>
<tr>
<td>Table 5</td>
<td>Method steps</td>
<td>20</td>
</tr>
<tr>
<td>Table 6</td>
<td>Critical infrastructure sectors and subsectors</td>
<td>21</td>
</tr>
<tr>
<td>Table 7</td>
<td>Typical threats</td>
<td>22</td>
</tr>
<tr>
<td>Table 8</td>
<td>Sources for issues and indicators</td>
<td>26</td>
</tr>
<tr>
<td>Table 9</td>
<td>Determining indicator value ranges (Step 7)</td>
<td>27</td>
</tr>
<tr>
<td>Table 10</td>
<td>Example of assigning weights to resilience indicators</td>
<td>28</td>
</tr>
<tr>
<td>Table 11</td>
<td>Determining ranges of values for each indicator - examples</td>
<td>36</td>
</tr>
<tr>
<td>Table 12</td>
<td>Example of assigning weights to resilience issues</td>
<td>37</td>
</tr>
<tr>
<td>Table 13</td>
<td>&quot;Top five&quot; and &quot;bottom five&quot; issues - example</td>
<td>39</td>
</tr>
<tr>
<td>Table 14</td>
<td>Steps for functionality level assessment</td>
<td>45</td>
</tr>
<tr>
<td>Table 15</td>
<td>Sample FEIs and FIs in the ECHO case [48]</td>
<td>53</td>
</tr>
<tr>
<td>Table 16</td>
<td>Examples of optimization alternatives</td>
<td>58</td>
</tr>
<tr>
<td>Table 17</td>
<td>Examples of (multiple) criteria for decision-making for optimizing resilience of SCIs</td>
<td>59</td>
</tr>
<tr>
<td>Table 18</td>
<td>Checklist on organizational factors</td>
<td>97</td>
</tr>
<tr>
<td>Table 19</td>
<td>Overview of ethical recommendations</td>
<td>98</td>
</tr>
</tbody>
</table>
### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABM</td>
<td>Agent-based Model</td>
</tr>
<tr>
<td>AHP</td>
<td>Analytic Hierarchy Process</td>
</tr>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>BCMS</td>
<td>Business Continuity Management System</td>
</tr>
<tr>
<td>BLEVE</td>
<td>Boiling Liquid Expanding Vapor Explosion</td>
</tr>
<tr>
<td>BUD</td>
<td>Budapest Liszt Ferenc International Airport</td>
</tr>
<tr>
<td>CascEff</td>
<td>Cascading Effects (FP7 EU project)</td>
</tr>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CIR</td>
<td>Critical Infrastructure Resilience</td>
</tr>
<tr>
<td>CIWIN</td>
<td>Critical Infrastructure Warning Information Network</td>
</tr>
<tr>
<td>CRISIS</td>
<td>Complexity Research Initiative for Systemic Instability (FP7 EU project)</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities and Exposures</td>
</tr>
<tr>
<td>D</td>
<td>Deliverable</td>
</tr>
<tr>
<td>DCL</td>
<td>Dynamic Checklist</td>
</tr>
<tr>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECI</td>
<td>European Critical Infrastructure</td>
</tr>
<tr>
<td>EPCIP</td>
<td>European Critical Infrastructure Protection</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUR-Lex</td>
<td>(Official website of European Union law and other public documents)</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>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GRI</td>
<td>Global Reporting Initiative</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>HH</td>
<td>High-high</td>
</tr>
<tr>
<td>HNP</td>
<td>Hungarian National Police</td>
</tr>
<tr>
<td>HSE</td>
<td>Health, Safety and Environment</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>ID</td>
<td>Identity</td>
</tr>
<tr>
<td>IED</td>
<td>Improvised Explosive Device</td>
</tr>
<tr>
<td>IIO</td>
<td>Inoperability Input Output (model)</td>
</tr>
<tr>
<td>IND</td>
<td>Indicator</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>L</td>
<td>Low</td>
</tr>
<tr>
<td>L</td>
<td>Lower</td>
</tr>
<tr>
<td><strong>Acronym</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>LL</td>
<td>Low-low</td>
</tr>
<tr>
<td>LPG</td>
<td>Liquefied Petroleum Gas</td>
</tr>
<tr>
<td>M</td>
<td>Medium</td>
</tr>
<tr>
<td>MCDM</td>
<td>Multi Criteria Decision Making</td>
</tr>
<tr>
<td>MOC</td>
<td>Management of Change</td>
</tr>
<tr>
<td>MS</td>
<td>Milestone</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>n</td>
<td>number</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Systems</td>
</tr>
<tr>
<td>NIS</td>
<td>Naftna Industrija Srbije (Serbian oil company)</td>
</tr>
<tr>
<td>NO</td>
<td>Nitrogen Oxide</td>
</tr>
<tr>
<td>NPK</td>
<td>Nitrogen Phosphorus Potassium</td>
</tr>
<tr>
<td>OEE</td>
<td>Overall Equipment Effectiveness</td>
</tr>
<tr>
<td>OpA</td>
<td>Optimization Alternative</td>
</tr>
<tr>
<td>PO</td>
<td>Project Officer</td>
</tr>
<tr>
<td>PP</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>PR</td>
<td>Public Relation</td>
</tr>
<tr>
<td>Q</td>
<td>Question</td>
</tr>
<tr>
<td>RESILENS</td>
<td>Realising European Resilience for Critical Infrastructure (H2020 EU project)</td>
</tr>
<tr>
<td>RI</td>
<td>Resilience Indicators</td>
</tr>
<tr>
<td>RIL</td>
<td>Resilience Level (=RL)</td>
</tr>
<tr>
<td>RL</td>
<td>Resilience Level (=RIL)</td>
</tr>
<tr>
<td>RSD</td>
<td>Serbian Dinar (currency)</td>
</tr>
<tr>
<td>S</td>
<td>Score</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCI</td>
<td>Smart Critical Infrastructure</td>
</tr>
<tr>
<td>SGI</td>
<td>Smith-Glasser Index</td>
</tr>
<tr>
<td>SMHI</td>
<td>Swedish and Meteorological and Hydrological Institute</td>
</tr>
<tr>
<td>SO</td>
<td>Sulphur Oxide</td>
</tr>
<tr>
<td>t</td>
<td>time</td>
</tr>
<tr>
<td>T</td>
<td>Task</td>
</tr>
<tr>
<td>U</td>
<td>Upper</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UV</td>
<td>Ultraviolet</td>
</tr>
<tr>
<td>v</td>
<td>Weight (resilience indicators)</td>
</tr>
<tr>
<td>w</td>
<td>Weight (issues or functionality indicators)</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>XLS</td>
<td>Microsoft Excel (file format)</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 About the guideline

This guideline describes the use of the methodology for assessing, predicting and monitoring/optimizing resilience of Smart Critical Infrastructures (SCIs), including dependency analyses, and the tools needed. Also, examples of resilience indicator checklists are included.

Failures of critical infrastructures, whether caused by internal malfunctions or external disastrous events, or cascading effects, may have devastating impacts on society. One example is described below [34].

The power outage of 2003 in Italy furnishes an example of scale effects in critical infrastructure cascades. On the night of 28 September 2003, electricity was being imported into Italy from Switzerland via three routes. A short circuit occurred when one transmission line overheated and touched the branch of a tree. Transmission automatically switched to the other two lines and then shut itself down to prevent them from overheating too. A series of blackouts propagated from the Swiss–Italian border progressively as far as Sicily and Geneva, affecting 56 million people. Trains were marooned in tunnels, and people were trapped in elevators. Civil aviation was briefly shut down. In this example, a very localised fault rapidly spread to the level of international system-wide effects. Transportation, health systems, the Internet and building maintenance were affected, and lack of refrigeration put foodstuffs at risk. However, as the blackout occurred in the night on a Sunday morning, many effects were localised and hence on the scale of the original fault. Nevertheless, loss of electrical power to the Internet propagated failure at power stations through inability to transmit control data [2]. The extraordinary extent of the power failure was the result of cascades in independent networks being transmitted to each other through the nodes of contact [7].

We can use this example to illustrate what this guideline can be used for, and what is outside the scope of the guideline. Our focus is smart critical infrastructures being struck by extreme events or cascading events.

1 Resilience level assessment

Each single critical infrastructure, such as trains, civil aviation or other transportation systems need not only protect against internal and external events, including cascading events, but also be prepared to cope with all types of hazards and threats and their potential manifestation as disastrous events. Critical Infrastructure Protection (CIP) is not enough, Critical Infrastructure Resilience (CIR) is required to cope with hazards/threats and extreme events such as terror attacks, cyber-attacks and extreme weather [26]. This includes understanding the risks and being prepared, but also possibly withstand or absorb the event, respond to it and recover as quickly as possible from it. Finally, learning from events may lead to necessary adaptations or transformations, such that the SCI is better prepared for future hazards, threats and events. The level of preparedness to cope with a specific threat, e.g. a cyber-attack, is assessed using the SmartResilience methodology for assessing the resilience level (RIL) of an SCI. Is the level of resilience good or poor on a five-level scale?

Most SCIs have not, and fortunately will not ever, experience an extreme threat or event. Still, it is possible and necessary to assess the level of resilience. It is not just about the (business) continuation of the SCI itself, extreme events will critically impact the society with potential consequences reaching far beyond the
isolated effects on the SCI, especially the secondary effects of reduced or terminated operation or service. This is why the SCI is considered critical in the first place. It is the responsibility of each SCI operator to minimize the effects on society; thus, also to perform resilience level assessments regularly. It will also be in governmental interest to ensure that such assessments are performed by each SCI operator.

2 Functionality level assessment and stress-testing

The resilience level assessment does not consider explicitly the effects of an extreme event in terms of the extent and duration of service disruption. The functionality level (FL) assessment attempts to predict the disruption, using the resilience curve model, for the critical functionality affecting the society, and other functionalities important for the SCI itself. How many percentages of the critical function/service will be lost and for how long?

Based on the critical functionality curve (or resilience curve) the SCIs can be "stress-tested" by comparing the critical functionality curve with thresholds, whether as maximum loss of functionality, duration or a combination of these, e.g. a threshold functionality curve. Thresholds for critical functionality should be established through consultations with local governments or direct consultation with the public being affected. What is considered acceptable in terms of loss of function/service and duration? When should the SCI be fully operational again?

3 Monitoring and optimization

Given that the resilience level assessment reveals weaknesses, either isolated or in comparison with others (benchmarking), or the functionality assessment and/or stress-testing show unacceptable loss of functionality, implementation of improvement measures will be required. Which improvement measure(s) will be the optimal to choose? Given a set of alternatives/options various criteria need to be weighed against each other. This could typically include the effect on resilience (e.g. change in RIL), costs and time to implement the measure(s), but also other criteria may be relevant. The method used to decide on optimal improvement measures is a Multi Criteria Decision Making (MCDM) method.

The effect of the improvement measures, and other changes since last assessment, may be regularly monitored by updating the entire resilience level assessment, or by monitoring a subset of the resilience indicators. This will show the resilience level progress.

4 Interdependencies and cascading effects

The Swiss-Italian power outage is a good example of the interconnectedness between critical infrastructures with the potential for cascading effects. It is the responsibility of each SCI operator to be aware of their own dependencies and interdependencies, and take this into account when assessing and "building" necessary resilience in their SCI. However, it is not necessarily obvious which other SCIs a given SCI are (inter-)dependent on. This task is supported in SmartResilience by a structured approach to identify relevant dependencies of a specific infrastructure, which is then treated as issues in the resilience level assessment (cf. methodology 1).

A second way to address (inter-)dependencies is through an approach that considers infrastructures-of-infrastructures, e.g. energy supply, transportation, health systems, the Internet and power stations in the power outage case. The infrastructures-of-infrastructures assessment is a governmental responsibility; local for a city, regional for an area, national for an entire country and international across countries. However, based on such assessments, the single SCI operators can include the cascading effects (e.g. loss of power) as a threat in their resilience level assessment (cf. methodology 1).

In SmartResilience, though, the developed approach dealing with infrastructures-of-infrastructures focuses on cascading economic effects for a given threat (such as flooding). It estimates direct and indirect losses (i.e. losses through cascading effects). Thus, it is possible to quantify the vulnerability due to economic dependencies. Based on this, it is also possible for single SCI operators to formulate economic resilience indicators, especially relevant for functionality level assessment (cf. methodology 2).
These four pillars of SmartResilience methodology are supported by the SmartResilience integrated web-based tool. The dependency of the tool varies between the methodologies, e.g. the resilience level assessment is possible to perform without using the tool, whereas the infrastructures-of-infrastructures interdependencies assessment requires use of the tool, or other advanced analytics tools. It is carried out as a data analytics background service in the tool. This also applies for the use of big data indicators in general.

This means that the descriptions of the use of the methodologies in this guideline to some extent includes the description of how to perform the assessments using the tool. The main intended reader (see Section 1.2), who is performing the assessments, also needs to consult the document describing the tool, i.e. D3.7 [51]1.

The guideline assembles the work performed and described in other SmartResilience project documents, notably the following methodology deliverables:

- D2.3 Interdependencies and cascading effects of smart city infrastructures [45]
- D3.1 Contextual factors related to resilience [46]
- D3.2 Assessing resilience of SCIs based on indicators [47]
- D3.3 Modelling the impact ("absorb" capacity) and the recovery response ("recover" capacity) based on indicators [48]
- D3.4 SmartResilience MCDM methodology serving as the basis for the "SCIs Dashboard" [49]
- D3.5 Interactive visualization as support to indicator-based decision making [50]
- D3.7 SCIs Dashboard containing the module on Dynamic Intelligent Checklists and the link to the RapidMiner based modules [51]
- D3.8 Assessing resilience level of Smart Critical Infrastructures based on indicators – Update [52]
- D4.2 Resilience indicators for SCIs based on big and open data [54]

Experience during the project has shown that rather extensive guidance is needed for the use of the methodologies and the tool. Thus, the aim has been to keep the guideline as simple as practical while still providing enough support for use. Further details are found in the mentioned reference documents.

Why use this guideline?

The main reason to use the resilience methodologies and tools described in this guideline is that they provide new and complementary means to cope with rare events (simple and complex, known and unknown, intended and unintended, in networks and network of networks, in conventional systems and smart systems) affecting critical infrastructures, as compared to traditional risk assessments, emergency preparedness and business continuity planning.

The threats we are considering, e.g. terror attacks, cyber-attacks and extreme weather, and their manifestations as disastrous events on a given SCI are low-probability, high consequence events. Such events – sometimes referred to as "black swans" – are notoriously hard to plan for.

The normal way of managing threats are usually based on a loose formula in which risk is the product of an event's probability multiplied by its potential harm. This equation helps to set priorities and sometimes dictates the amount that are spent on protective measures. However, if this is your only decision-making tool, "a black swan will eat you for lunch," as expressed by Verchick (in [37]), because the events with extreme low probability will have limited contribution to the overall risk or be neglected all together, arguing that they are not "reasonable." However, history has told us that they have occurred, and they will occur

---

1 The D3.7 document is planned to be published 2 months after this guideline. The tool is still under development.
again, but we don’t know where and we don’t know when. What we do know, and what we can and should do, is to be prepared and resilient.

Even if less rare and dramatic events occur, all critical infrastructure owners have a responsibility to reduce the effect on society to a minimum, especially the loss of functionality (loss of energy, water, transportation means, health care, etc.). Methodologies, tools and means to deal with this are described in this guideline.

1.1.1 Limitations - what is outside scope?

The RIL assessment, FL assessment and MCDM (cf. methodologies 1-3) are mainly focusing on one specific SCI. It is possible to aggregate several SCIs within an area; however, this only provides a “net sum” of each SCI. For an area consisting of several SCIs, it will be most relevant to include the infrastructures-of-infrastructures approach (cf. methodology 4). Even then, there are additional resilience aspects within an area not covered by the SmartResilience methodologies, such as community resilience issues.

Additional limitations apply for each of the methodologies as described in the reference documents listed above.

1.1.2 Guideline structure

Following the introduction in Chapter 1, Chapter 2 describes how to perform resilience assessment, Chapter 3 how to perform resilience modelling, and Chapter 4 how to perform resilience monitoring and optimization. Chapter 5 includes the analysis of interdependencies. Chapter 6 describes the use of the integrated tool for resilience assessment, modelling, monitoring/optimization, and dependency analyses. Chapter 7 provides advice on legislation, organizational factors and ethics, and Chapter 8 provides descriptions of the four SmartResilience case studies used as examples throughout the guideline. Annex 1 documents the review process and Annex 2 includes the catalogue of selected resilience indicator checklists.

1.1.3 General concepts, terms and definitions

In the SmartResilience project, the resilience of an infrastructure is defined as: “The ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions” [43].

Based on this definition, we derive at the five phases of the resilience curve/cycle as illustrated in Figure 1 and described in Table 1, representing the main resilience attributes in the SmartResilience project.

![Figure 1: Resilience phases and loss of critical functionality](image)

Resilience is measured in two different ways in the SmartResilience project. One is by measuring each phase indirectly through indicators, without considering the shape of the resilience curve (cf. methodology 1). The second is to measure the loss of critical functionality directly, considering resilience as inversely proportional to the loss of critical functionality. In this case, the shape of the resilience curve is modelled (cf. methodology 2).
Table 1: Short description of the resilience phases

<table>
<thead>
<tr>
<th>Phase name</th>
<th>Phase description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase I Understand</td>
<td>Includes and emphasizes understanding of (emerging) risks, and includes knowledge about the context, the systems, and previous events; “What could ‘the event’ be”?</td>
</tr>
<tr>
<td>Phase II Anticipate</td>
<td>Includes planning, proactive adaptation and vigilance/attention; “How to prepare for both expected and unexpected events”? “How to get early warnings”?</td>
</tr>
<tr>
<td>Phase III Absorb</td>
<td>Includes inherent absorption, resilient reaction, robustness and redundancy, and possible cascading/ripple effects; “How steep”? “How deep down”?</td>
</tr>
<tr>
<td>Phase IV Respond</td>
<td>Includes response and recovery capacity, ability and rapidity of the infrastructure and the surrounding environment; “How long”? “How steep up”?</td>
</tr>
<tr>
<td>Phase V Adapt</td>
<td>Includes learning and improvements made in/on the infrastructure and its environment; “How well”? “Sustainable”?</td>
</tr>
</tbody>
</table>

The second axis in the resilience matrix consists of dimensions, which can be used for e.g. identification and structuring of indicators and improvement measures. The dimensions are described in Table 2.

Table 2: Short description of the dimensions

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. System/physical</td>
<td>Includes technological aspects of the given infrastructure, as well as the physical/technical networks being part of a given infrastructure, interconnectedness with other infrastructures and systems</td>
</tr>
<tr>
<td>2. Information/data</td>
<td>Includes also the technical systems dealing with information/data</td>
</tr>
<tr>
<td>3. Organizational/business</td>
<td>Includes business-related aspects, financial and HR aspects as well as different types of respective organizational networks</td>
</tr>
<tr>
<td>4. Societal/political</td>
<td>Includes the broader societal and social context, also stakeholders not directly involved in the operation and/or use of the infrastructure (e.g. social networks)</td>
</tr>
<tr>
<td>5. Cognitive/decision-making</td>
<td>Includes the perception aspects (e.g. perceptions of threats and vulnerabilities)</td>
</tr>
</tbody>
</table>

In SmartResilience, we use the term “scenario” in two ways; one broad and one detailed way. In the broad way, we use it for a specific selection of critical infrastructures and threats for a given area/city, i.e. the selected area, critical infrastructures and threats. In the detailed way, e.g. for stress-testing, we define a very specific scenario describing an anticipated extreme event.

1.2 Intended reader

The main intended reader is the person – within a city or area, or a specific SCI – who is responsible for performing the resilience assessment, prediction or monitoring, including carrying out necessary calculations. This can be an in-house person performing e.g. self-assessment, or it may be an external assessor performing assessments on behalf of e.g. infrastructure owners/operators, city officers/planners, regional authorities, or national agencies.

1.3 How to use the guideline

An overview of the methods included in this guideline, and the results obtained by using them, are presented in Table 3. One or more methods can be selected for use. Connections are illustrated in Figure 2 below.
How to perform resilience assessment, resilience modelling, resilience monitoring (including optimization) and dependency analyses are described in the first four main chapters (Chapter 2-5). This is assisted using the tools described in Chapter 6.

Four SmartResilience project case studies have been used as examples throughout the guideline. These are:

- Transportation - airport security (labelled DELTA in the project)
- Industrial production (labelled ECHO in the project)
- Drinking water supply (labelled FOXTROT in the project)
- Underground fuel storage and energy supply (labelled HOTEL in the project)

All four case studies are used as partial examples, e.g. in Chapter 2. ECHO is used as example case in the method description of RIL and FL assessment in Chapter 2 and 3, and in the tool description of dynamic checklist (DCL) setup, RIL assessment and resilience monitoring in Chapter 6. HOTEL is used as example case in the tool description of FL assessment and resilience optimization (MCDM) in Chapter 6. Descriptions of the example cases are provided in Chapter 8.

General advice related to legislation, organizational factors and ethics, including quality criteria for indicators are provided in Chapter 7.

Connections between the four pillars of methods are illustrated in Figure 2 (main connections – solid lines; possible connections – dashed lines).

### Table 3: Methods and results

<table>
<thead>
<tr>
<th>Chapter and Topic</th>
<th>Method</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2 Assessing resilience</td>
<td>Resilience level assessment</td>
<td>Resilience level (RIL)</td>
</tr>
<tr>
<td>Chapter 3 Modelling resilience</td>
<td>Functionality level assessment</td>
<td>Functionality level (FL)</td>
</tr>
<tr>
<td></td>
<td>Stress-testing</td>
<td>Critical FL versus criteria/threshold</td>
</tr>
<tr>
<td>Chapter 4 Monitoring resilience</td>
<td>Monitoring</td>
<td>Resilience progress</td>
</tr>
<tr>
<td></td>
<td>Optimization (MCDM)</td>
<td>Optimal improvement measures</td>
</tr>
<tr>
<td>Chapter 5 Analyzing dependencies</td>
<td>Interdependency identification</td>
<td>Relevant interdependencies</td>
</tr>
<tr>
<td></td>
<td>Cascading effects loss estimation</td>
<td>Loss from cascading effects</td>
</tr>
</tbody>
</table>

![Figure 2: Connections between the methodologies](image-url)
Each of the methods provides their own results. In addition, they either support or they are a prerequisite for other methods.

*Resilience level assessment* is a prerequisite for monitoring and for optimization (as the criteria "change in resilience level"). *Functionality level assessment* is a prerequisite for stress-testing and it may be used for monitoring. Both *functionality level assessment* and *stress-testing* may support resilience level assessment through identified weak areas, treated as issues. They may also support optimization in the sense that they may indicate a need for improvement measures, for which optimal choices should be made. The same is true for monitoring. *Interdependency identification* supports resilience level assessment by identifying dependent critical infrastructures that can be included as issues in the resilience level assessment of the SCI in question. *Cascading effects loss estimation* supports functionality level assessment through the identification and formulation of economic resilience indicators. It may also support optimization, since ideally investments in improvement measures for one specific SCI should also reflect benefits for other (inter-)dependent critical infrastructures due to potentially reduced cascading effects.
2 Resilience assessment

2.1 Introduction and purpose

Assessing resilience of an SCI starts from assigning values to single indicators, which corresponds to scores on a scale from 0 to 5, where 0 is worst and 5 is best. The scores are aggregated upwards in a six-level hierarchical model until the entire SCI is assessed, or even several SCIs within a city (or some other area) are assessed.

At each level, the scores – alternatively combined with weights – corresponds to a certain resilience level (given by a character E-A, where E is worst, and A is best). A weighted score between 0 and 1 corresponds to resilience level E, a weighted score 1-2 corresponds to resilience level D, and so on. This is shown in Table 4.

Table 4: Scores and resilience levels

<table>
<thead>
<tr>
<th>Score</th>
<th>Resilience level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-5</td>
<td>A</td>
<td>Excellent</td>
</tr>
<tr>
<td>3-4</td>
<td>B</td>
<td>Good</td>
</tr>
<tr>
<td>2-3</td>
<td>C</td>
<td>Average</td>
</tr>
<tr>
<td>1-2</td>
<td>D</td>
<td>Poor</td>
</tr>
<tr>
<td>0-1</td>
<td>E</td>
<td>Critical</td>
</tr>
</tbody>
</table>

The indicators (level 6 – the lowest level in the hierarchical model) measure the issues (level 5), which are important in order to be resilient in each of the resilience cycle phases (level 4) for the relevant threats (level 3) of each SCI (level 2) within a city or other area (level 1). This is illustrated in Figure 3.

Figure 3: The six levels in the hierarchical model
The purpose of assessing resilience, as described in this guideline, is to obtain a quantitative measure of how resilient an area such as a city or an individual SCI are against severe threats such as terror attacks, cyber-attacks and extreme weather. The resilience assessment uses a holistic approach that goes beyond traditional risk of known events, emergency preparedness and crisis management. It covers e.g. preparing for the unforeseen, imagination, vigilance, flexibility, improvisation, recovery including business continuity aspects, and learning and adaptation.

The results will show the level of resilience and where improvements are most needed, emphasizing and fostering a continuous improvement mindset through regularly updated assessments.

### 2.2 Basic concepts and terms

#### 2.2.1 Concepts of issues and indicators

"Issue" is a very general term referring to anything that is important in order to be resilient against severe threats such as terror attacks, cyber threats and extreme weather. It is WHAT is important, and it is allocated to one of the five phases in the resilience cycle. E.g., it can be "training" performed in the anticipate/prepare phase. "Indicator" is HOW to measure the issues. E.g., it can be "percentage of personnel in a certain response team taken a certain course". The relation and difference between issue and indicator are illustrated in Figure 4.

![Figure 4: Issues measured by indicators](image)

The issues we try to measure, and the indicators we use to measure the issues, are two different things. The indicator will typically be described as a number, ratio, score on some scale, or similar. Without this type of specification or operationalization, we are left with just a theoretical non-measurable issue. We cannot start with the indicators either, since we need to know what we want to measure (i.e. the issues) and why.

A given issue needs to be measured by one or more indicators, as illustrated by multiple arrows in Figure 4. How many indicators that are needed depends on how well the indicator(s) cover all aspects of the issue. This indicator coverage of an issue is illustrated in Figure 5 (size of "bubbles" indicating individual coverage).

The same issue can, and will easily, be measured with different indicators by different users. In Figure 5, it is illustrated that one user uses three indicators (red), whereas another user uses two indicators (blue). These indicators can be the same (as indicator 1), or different indicators.

Further, the figure illustrates that "yes/no" type of indicators typically provide little information with low coverage of the entire issue (small "bubbles"), whereas other types such as number and fractions typically have higher coverage (large "bubbles"). Using only "yes/no" questions as indicators will require a larger set of indicators.

Finally, the figure illustrates that there will, in practice, always be parts of the issue that are not covered by any of the selected indicators, and some indicators may in principle also cover other aspects, not relevant for the issue in question (illustrated as outside the area of the issue).
2.3 Method description – resilience level assessment

The method description is based on e.g. [47], [52] and [63]. For more details, see D3.8 [52]. The method steps are described in Table 5, starting from the top of the model, i.e. at Level 1:

Table 5: Method steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Method step description</th>
<th>Level in model</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Define the scenario (scope)</strong></td>
<td></td>
</tr>
<tr>
<td>Step 1</td>
<td>Select the area, e.g. a smart city</td>
<td>Level 1</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the relevant smart critical infrastructures (SCIs) for the area</td>
<td>Level 2</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select relevant threats for each smart critical infrastructure</td>
<td>Level 3</td>
</tr>
<tr>
<td></td>
<td><strong>Define the analysis framework</strong></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Consider each phase (in the resilience matrix) for each threat</td>
<td>Level 4</td>
</tr>
<tr>
<td>Step 5</td>
<td>Define the issues within each phase (alternatively structured according to the dimensions)</td>
<td>Level 5</td>
</tr>
<tr>
<td>Step 6</td>
<td>Search for the appropriate indicators for each issue</td>
<td>Level 6</td>
</tr>
<tr>
<td></td>
<td><strong>Perform the analysis (&quot;calculate&quot;)</strong></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Determine the range of values for each indicator (and optionally assign weights)</td>
<td>6</td>
</tr>
<tr>
<td>Step 8</td>
<td>Assign values to the indicators</td>
<td>1-6</td>
</tr>
<tr>
<td>Step 9</td>
<td>Perform the calculations (i.e. calculate scores and resilience levels)</td>
<td>1-6</td>
</tr>
<tr>
<td></td>
<td><strong>Use the results and make decisions</strong></td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>Provide status, trends, strength and weaknesses, improvement needs, benchmarking, etc.</td>
<td>1-6</td>
</tr>
</tbody>
</table>

2.3.1 Define the scenario (scope)

The scenario, i.e. the area, SCIs and threats to include in the assessment, is determined in Steps 1-3. This is the scope of the assessment and is relatively straight-forward.

2.3.1.1 Step 1. Select the area (Level 1)

Select the area, which includes the SCIs to be assessed. This is typically a city or an area within a city; however, it can also be a region or even an entire country. If it is only one SCI involved, go to step 2.
2.3.1.2 Step 2. Select the relevant SCIs (Level 2)

Critical infrastructures are often referred to as sectors and subsectors (products or services). Typical examples are shown in Table 6. See also Annex 2 in D3.8 [52].

Table 6: Critical infrastructure sectors and subsectors

<table>
<thead>
<tr>
<th>SECTOR</th>
<th>SUBSECTOR (PRODUCT OR SERVICE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Energy</td>
<td>1 Fuel (e.g. oil and gas) production, refining, treatment and storage, including pipelines</td>
</tr>
<tr>
<td></td>
<td>2 Generation of electricity, heat, industrial steam or cooling</td>
</tr>
<tr>
<td></td>
<td>3 Transmission of electricity, gas, oil and other energy carriers</td>
</tr>
<tr>
<td></td>
<td>4 Distribution of electricity, gas, oil and other energy carriers</td>
</tr>
<tr>
<td>II Information,</td>
<td>5 Information systems and networks protection</td>
</tr>
<tr>
<td>Communication Technologies (ICT)</td>
<td>6 Instrumentation automation and control systems (SCADA etc.)</td>
</tr>
<tr>
<td></td>
<td>7 Internet</td>
</tr>
<tr>
<td></td>
<td>8 Provision of fixed telecommunications</td>
</tr>
<tr>
<td></td>
<td>9 Provision of mobile telecommunications</td>
</tr>
<tr>
<td></td>
<td>10 Radio communication and navigation (e.g. Loran, GPS and Galileo)</td>
</tr>
<tr>
<td></td>
<td>11 Satellite communication</td>
</tr>
<tr>
<td></td>
<td>12 Broadcasting</td>
</tr>
<tr>
<td>III Water</td>
<td>13 Provision of drinking water</td>
</tr>
<tr>
<td></td>
<td>14 Control of water quality</td>
</tr>
<tr>
<td></td>
<td>15 Stemming and control of water quantity</td>
</tr>
<tr>
<td>IV Food</td>
<td>16 Provision of food and safeguarding food safety and security</td>
</tr>
<tr>
<td>V Health</td>
<td>17 Medical and hospital care</td>
</tr>
<tr>
<td></td>
<td>18 Medicines, serums, vaccines and pharmaceuticals</td>
</tr>
<tr>
<td></td>
<td>19 Bio-laboratories and bio-agents</td>
</tr>
<tr>
<td>VI Financial</td>
<td>20 Payment services/payment structures (private)</td>
</tr>
<tr>
<td></td>
<td>21 Government financial assignment</td>
</tr>
<tr>
<td>VII Public &amp; Legal order and Safety</td>
<td>22 Maintaining public &amp; legal order, safety and security</td>
</tr>
<tr>
<td></td>
<td>23 Administration of justice and detention</td>
</tr>
<tr>
<td>VIII Civil Administration</td>
<td>24 Government functions</td>
</tr>
<tr>
<td></td>
<td>25 Armed forces</td>
</tr>
<tr>
<td></td>
<td>26 Civil administration services</td>
</tr>
<tr>
<td></td>
<td>27 Emergency services</td>
</tr>
<tr>
<td></td>
<td>28 Postal and courier services</td>
</tr>
<tr>
<td>IX Transport</td>
<td>29 Road transport</td>
</tr>
<tr>
<td></td>
<td>30 Rail transport</td>
</tr>
<tr>
<td></td>
<td>31 Air traffic</td>
</tr>
<tr>
<td></td>
<td>32 Inland waterways transport</td>
</tr>
<tr>
<td></td>
<td>33 Ocean and short-sea shipping</td>
</tr>
<tr>
<td>X Chemical and nuclear industry</td>
<td>34 Production and storage/processing of chemical and nuclear substances</td>
</tr>
<tr>
<td></td>
<td>35 Pipelines of dangerous goods (chemical substances)</td>
</tr>
<tr>
<td>XI Space and Research</td>
<td>36 Space</td>
</tr>
<tr>
<td></td>
<td>37 Research</td>
</tr>
</tbody>
</table>

Select the relevant sectors and/or subsectors. If necessary, adapt the subsectors or add new subsectors. If more than one sector or subsector are selected, they will be weighed against each other during the calculations (see Section 2.2.3).
2.3.1.3  Step 3. Select the relevant threats for the SCIs (Level 3)

Select the threats that will be included in the assessment of each SCI. Typical threats to consider are included in Table 7 (not complete).

<table>
<thead>
<tr>
<th>Type of threat</th>
<th>Specific threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorist attack</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Bomb attack</td>
</tr>
<tr>
<td></td>
<td>Other (specify)</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Denial of service</td>
</tr>
<tr>
<td></td>
<td>Other (specify)</td>
</tr>
<tr>
<td>Natural threats (incl. extreme weather)</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td>Urban floods</td>
</tr>
<tr>
<td></td>
<td>Other (specify)</td>
</tr>
<tr>
<td>New technology related threats</td>
<td>-</td>
</tr>
<tr>
<td>Other</td>
<td>Interruption in critical supply</td>
</tr>
<tr>
<td></td>
<td>Other (specify)</td>
</tr>
</tbody>
</table>

Each threat will be assessed separately (for each SCI) and weighed against each other during the calculations (see Section 2.2.3). Alternatively, a simplified “all-threats” approach can be adopted, which includes issues and indicators for all relevant threats in one generic assessment (for each SCI).

How to treat cascading effects?

Cascading effects where the SCI in question is affected from the outside by this cascading effect as a threat, should be treated as a specific threat e.g. toxic cloud, flooding, etc. If the effect is in the form of loss of service, then it is treated as dependencies as described in Step 5, i.e. explicitly as issues.

Internal escalation of an event is treated explicitly as issues (Step 5) reflecting the required safety systems or barriers needed to prevent escalation.

2.3.2  Define the analysis framework

Each phase is considered for each threat scenario, and issues and indicators are established for each of the phases. This is carried out in Steps 4-6, corresponding to levels 4-6 in the hierarchical model. To define appropriate issues and indicators (Steps 5-6), in order to obtain a realistic and trustworthy resilience assessment, are perhaps the most challenging parts of the methodology. Thus, they are described in some detail.

2.3.2.1  Step 4. Consider each phase for each threat (Level 4)

As illustrated in Figure 3, the resilience matrix consists of phases and dimensions; however, the main emphasis is on the phases. The dimensions are just a means to structure the issues and indicators within each phase. The phases structure or categorize the issues and indicators, but in addition they are used in the calculations (in Step 9), which the dimensions are not.

It is not always easy to decide which phase an issue belongs to, and in some cases one issue (and corresponding indicators) may be relevant in more than one phase. This is considered further in Step 5.
2.3.2.2 Step 5. Define the issues for each phase (Level 5)

Defining and allocating issues can be challenging. Thus, some advices are provided below.

Advice – allocate issues to the phase they are performed/occur

Many issues that are performed in the anticipate/prepare phase (before an event occurs) influence the phases after the event, e.g. in the respond/recover phase. However, it should be allocated to the phase it is performed, not to the phase(s) it has an effect. E.g. "planning" and "training" are carried out in the anticipate/prepare phase but influences respond/recover. It should only be included in the anticipate/prepare phase and not repeated in the later phases like the respond/recover phase.

Advice – specify the issues sufficiently

A broadly defined issue may be relevant in more than one phase, but if it is measured with different indicators in different phases, it should be split into more specific issues. E.g. "communication" could be split in "communication of anticipated threats" in the anticipate/prepare phase, and "communication during response" in the respond/recover phase.

Advice – provide enough issues

It is up to the users to define a required number of issues (and indicators) to provide a sufficiently complete resilience picture; however, as a rule of thumb a minimum of seven to eight issues per phase should be aimed for. Thus, we may have about 35-40 issues for one specific threat for one critical infrastructure. Much less may lead to an incomplete resilience picture.

There are several sources for defining/selecting issues. Some of these are:

1. The dynamic checklists (DCLs) in the SmartResilience Integrated Tool (issues and indicators)
2. The SmartResilience database (containing all collected issues and indicators)
3. The candidate issues (and indicators) provided in SmartResilience deliverable D4.1 [53]
4. The candidate issues provided in deliverable D3.2 Annex 3 [47]
5. Existing indicators in use (in-house) from which issues may be deduced
6. Dimensions used as triggers to define issues

For the three first sources, the issues are already combined with corresponding (candidate) indicators; thus, Step 5 (issues) and Step 6 (indicators) are closely related. This means that these sources are also used for the search for appropriate indicators for each issue. Each of the sources are briefly described below.

1. The dynamic checklists (DCLs) in the SmartResilience Integrated Tool (issues and indicators)

The DCLs for resilience assessment are either new or existing lists of issues and indicators for given scenarios (SCIs and threats). These DCLs are made from the approved issues and indicators in the database based on the users’ selection of relevant SCIs and threats. Using the same DCLs across different users will ensure comparability, if the results are used for benchmarking. End-users may create a new or adapt an existing DCL, i.e. they may remove or add issues and indicators; thus, customizing the DCLs to their case. This will make them more relevant for the single end-user, and provide a good basis for trending; however, the more the DCLs are customized, the less relevant they are for benchmarking.

By including the so-called Core DCL with common generic issues applicable for all, a "partial" benchmarking may be obtained, even if the complete User DCL includes other user-specific issues. The Core DCL part can be benchmarked with others.

2. The SmartResilience database (containing all collected issues and indicators)

The DCLs are created based on the approved issues and indicators in the database. An existing DCL may be adapted by including additional issues through search in the database. If a new issue, not in the database, is included, it must first be added to the database with required information, and then be approved.

3. The candidate issues (and indicators) provided in SmartResilience deliverable D4.1

If access to the database and the DCLs is not provided or available, issues (and indicators) can be reviewed and manually selected from the SmartResilience deliverable D4.1 [53]. The D4.1 report includes the
collection of issues (and indicators) during the first part of the SmartResilience project. These issues (and indicators) are included in the database, which will be further developed by adding new issues (and indicators).

4. The candidate issues provided in D3.2 Annex 3

In total 143 generic candidate resilience issues are provided in D3.2 [47]. They are complementary to the issues in the SmartResilience deliverable D4.1 [53] and the SmartResilience database, although some issues may occur in both/all sources. The issues in D3.2 were established focusing specifically on "genuine" resilience issues, also capturing typical topics discussed in resilience literature, i.e. those issues that can provide "added value" compared to the traditional approaches (risk management, business continuity, etc.).

The generic candidate issues in D3.2 can be reviewed by all critical infrastructures to check if any of them are considered relevant and important. Only for those selected, i.e. being relevant and important, it is necessary to establish indicators to measure the selected issues (in Step 6).

5. Existing indicators in use (in-house) from which issues may be deduced

Resilience issues may be deduced from the indicators already in use by an end-user. For each indicator, the question raised is "why do we use this indicator – what is it that we measure by this indicator?"

6. Dimensions used as triggers to define issues

The five dimensions being part of the resilience matrix can be used as triggers to check if additional issues should be included in any of the five phases. The dimensions were provided in Table 2 (in Chapter 1).

It should be noted that we are focusing on internal resilience, i.e. those issues that the SCI itself can control. Thus, some of the dimensions, e.g. societal/political, with corresponding issues may be less relevant.

In addition to the above-mentioned sources, one could also ask oneself "what is important in order to understand risks, being prepared, be able to absorb, etc.?" This may provide additional issues to those already identified and selected, by using the phases directly as triggers.

How to treat (inter-)dependencies, interoperability, and smartness opportunities and vulnerabilities?

Dependencies and interdependencies

Critical infrastructures, or other infrastructures, services or systems that the SCI are dependent on, should be addressed explicitly as issues in the relevant phases for the relevant threats. This could e.g. be the need for redundant energy supply or communication networks.

Interdependencies are treated in the same way. The difference is that the SCI being dependent on "your" SCI, need to explicitly include this as issues in their resilience assessment framework. Interdependency identification are explained in Chapter 5.

If the scope of the resilience assessment covers multiple SCIs, i.e. an area, city, region, etc., then dependencies and interdependencies between these SCIs should be assessed in a separate dependency analysis, including cascading and ripple effects, in addition to the individual assessments described in this report. However, such dependency analyses of multiple SCIs are not the responsibility of the single SCI, but rather a governmental responsibility at some level (local, regional, national or international/across countries). Loss estimation from cascading effects are described in Chapter 5.

Interoperability

If it is an internal concern, e.g. in case of interoperable communication systems, then it should be treated as an issue. If it is related to external interoperability in the sense of external backup systems, e.g. "bus for train," then it should be included explicitly as an issue (e.g. cooperation agreements), if this is the responsibility of the SCI being assessed.

Smartness opportunities and vulnerabilities

The relevance of smartness opportunities and smartness vulnerabilities related to smart features (sensors, gateways, processors, actuators, etc.) should be considered explicitly as issues in each phase. (It is included at the end of each phase in D3.2 Annex 3 [47]).
2.3.2.3 **Step 6. Search for appropriate indicators for each issue (Level 6)**

In Step 6, we search for appropriate indicators to measure the issues defined (in Step 5). Whereas issues are WHAT is important to be resilient against severe threats (e.g. "training"), indicators are HOW we measure the issues (e.g. "percentage of personnel in a certain response team taken a certain course").

The SmartResilience methodology for assessing resilience is flexible in that all types of indicators may be used, i.e. yes/no questions, numbers, fractions, etc.; thus, there are no restrictions in the use of existing indicators. However, if only yes/no questions are used, a larger number of indicators are required to obtain sufficient coverage (cf. Figure 5).

**Advice – consider indicator quality attributes relevant for you**

There are many quality attributes for indicators, which can be stated in general, and we return to these below. However, for a specific indicator it is difficult to state whether a quality attribute or requirement is fulfilled, because this varies between the users. As an example, "necessary data should be available or capable of being generated" is one of the quality attributes or requirements. For one specific user, the necessary data may be readily available, whereas for another this may not be the case, and it may require a lot of resources to obtain this. Thus, the quality of the same indicator may be considered differently among different users.

When reviewing, and selecting indicators, the user may consider – at least some – quality attributes that are most relevant for him/her. The indicators should be:

1. Measurable
2. Sensitive for change
3. Possible to obtain sufficient amount of data for
4. Controllable
5. Individually valid
6. Collectively provide sufficient coverage
7. Easy to understand, simple and unambiguous
8. Using available data

An indicator needs to be **measurable**. If not, it is not an indicator. It also needs to be **sensitive for change**, i.e. changeable. If not, it is not necessary to perform repeated measurements. This is also related to obtain **sufficient amount of data** to know that a change is statistically significant or just random. The indicator (or rather the issue it measures) also needs to be **controllable**, i.e. that it is possible to influence and change its measurement values. The indicators should be **individually valid**, i.e. that they measure the most important aspects of the issue, but even more important; they should **collectively provide sufficient coverage**, i.e. that they collectively measure all the most important aspects of the issue (see Figure 5). The indicators should obviously be **easy to understand, simple and unambiguous**, i.e. it should be obvious and excepted by "anyone" that they say something about the resilience (of critical infrastructures). Finally, in order not to make the list of criteria too comprehensive, **availability of data** needs to be considered. Quite often, users insist in only using existing information systems, in order not to put extra burden on the organization by requiring new data to be collected, and they may also insist on only using automatically harvested data, i.e. no manual collection of data.

Quality criteria are also discussed in Chapter 7 related to ethical considerations.

---

2 Note that most of these quality criteria are not relevant or valid for single Yes/No questions. A series of Yes/No questions are needed in order to provide a meaningful measurement of an issue. Each single Yes/No question carries limited information, as illustrated in Figure 5.

3 Other obvious candidates for quality criteria are reliability, i.e. that the same measurement should be obtained by different persons/observers, and that the indicators should not be (easily) manipulated. However, as already mentioned, the list of potential quality criteria is long. (See e.g. SmartResilience deliverables D3.2 [47] for more examples).
As for issues, there are several sources for indicators, some which were mentioned in Step 5. Examples of sources for indicators are:

1. The dynamic checklists (DCLs) in the SmartResilience Integrated Tool (issues and indicators)
2. The SmartResilience database (containing all collected issues and indicators)
3. The candidate issues and indicators provided in SmartResilience deliverable D4.1 [53]
4. Workshops answering the question "what would tell us that we are doing well with issue X?"
5. Existing indicators in use (in-house)

1. The dynamic checklists (DCLs) in the SmartResilience Integrated Tool (issues and indicators)
In this case, the resilience indicators are provided along with the issues. However, the proposed indicators in the checklists may be removed/rejected (not applicable), adjusted or new ones included. For new DCLs, indicators need to be associated to the issues.

2. The SmartResilience database (containing all collected issues and indicators)
Similar as for source no. 1, the resilience indicators are provided along with the issues, and again, the proposed indicators may be removed/rejected (not applicable), adjusted or new ones included.

3. The candidate issues and indicators provided in SmartResilience deliverable D4.1
As for the sources no. 1 and 2 above, the resilience indicators are provided along with the issues. Also, for this case, the proposed indicators may be removed/rejected (not applicable), adjusted or new ones included.

4. Workshops answering the question "what would tell us that we are doing well with issue X?"
What information provide us with a status on issue X? How can we use the information to measure issue X? This is relevant when we have defined issues without any corresponding indicators, i.e. sources 4 and 6 in Step 5. It also applies if new issues are included or changes are made to those candidate issues being reviewed.

5. Existing indicators in use (in-house)
Safety, risk, emergency, business continuity, or other types of indicators already in use should be considered included as resilience indicators. This was actually part of Step 5 (source 5), since the indicators need to be linked to issues.

To summarize, Table 8 gives an overview of the sources for identifying and selecting issues and indicators.

### Table 8: Sources for issues and indicators

<table>
<thead>
<tr>
<th>Issues</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is important for each of the phases?</td>
<td>What would tell us that we are doing well with issue X?</td>
</tr>
<tr>
<td>The dynamic checklists (DCLs) in the SmartResilience Integrated Tool (both issues and indicators)</td>
<td></td>
</tr>
<tr>
<td>The SmartResilience database (containing all collected issues and indicators)</td>
<td></td>
</tr>
<tr>
<td>The candidate issues and indicators provided in SmartResilience deliverable D4.1</td>
<td></td>
</tr>
<tr>
<td>Candidate issues provided in D3.2 Annex 3</td>
<td>Workshops to identify relevant information/indicators</td>
</tr>
<tr>
<td>Deducing issues from existing indicators</td>
<td>Existing indicators in use (in-house)</td>
</tr>
<tr>
<td>Dimensions used as triggers to define issues</td>
<td>Workshops to identify relevant information/indicators</td>
</tr>
</tbody>
</table>

#### 2.3.3 Perform the analysis ("calculate")

When all issues and corresponding indicators have been identified and those to be included in the resilience assessment have been selected, we need to determine the range of values for each indicator and, if necessary, provide weights (Step 7), to assign the real values to the indicators at a certain point in time (Step
and perform the calculations to obtain resilience scores and resilience levels (RILs) at all aggregation levels in the model (Step 9).

### 2.3.3.1 Step 7. Determine the range of values for each indicator (and optionally weights)

We are using a five-point score scale and need to determine for each indicator (of any type) the range of values in the five categories. We use the terms LL (Low-low), L (Low), M (Medium), H (High) and HH (High-high) for the value ranges.

These value ranges correspond to score ranges and score values as show in Table 9. For simplicity, we use – as default – average range values as scores, i.e. (0.5, 1.5, 2.5, 3.5, 4.5), except for Y/N questions, where the default values are 0 or 5. In addition, it is possible to "overrule" these default values with other exact values within the score range, e.g. a low (L) indicator value being close to medium (M) could be assigned to 1.9.

| Indicator values, score values and resilience levels |
|---------------------------------|---|---|---|---|---|
| Indicator values | LL | L | M | H | HH |
| Indicator value ranges | LL-LU | L-LU | ML-MU | HL-HU | HHL-HHU |
| Score label | Critical | Poor | Average | Good | Excellent |
| Score range* | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 |
| Score values (default) | 0.5 | 1.5 | 2.5 | 3.5 | 4.5 |
| Score values for Y/N questions (default) | N=0 | | | | Y=5 |

As indicated in Table 9 (with yellow shading), everything except the indicator value ranges are predefined. The indicator value ranges must be determined by the user for each indicator (except Y/N questions), by defining lower (L) and upper (U) values within each of the five categories. E.g., the number of available fire fighters could be (< 3, 4-7, 8-11, 12-15, >16) corresponding to LL, L, M, H and HH. If the measured indicator value in Step 8 is for example 11 fire fighters, then this corresponds to a medium (M) value, which by default gives a score of 2.5 (an average score). This score is possible to overrule by any exact value within the range (2-3), e.g. it could be 2.8, arguing that it is close to a high (H) value.

It is also possible to overrule the default values for Y/N, e.g. using 4.5 and 0.5 instead of 5 and 0. The argument for using 0 and 5 is that there may be no reason to give any credit to a No answer (i.e. not even 0.5), or any discredit for a Yes answer (i.e. 4.5, which is a reduction of 0.5 from the maximum top score). It is also possible to simplify the scoring by providing a direct score without indicator value ranges, as described below.

#### Direct scoring

A simple way of providing scores is to ask directly for a score between 0 and 5 (either integer values or decimal values). E.g., "on a scale of 0 to 5 how do you rate this indicator?" The disadvantage is that this is a subjective assessment, which may differ depending on the person(s) providing the scores.

---

* For simplicity, the ranges are written as O-1, 1-2, and so on. They are in fact non-overlapping, i.e. \([0 \leq \text{Critical} < 1], [1 \leq \text{Poor} < 2], \) and so on.

---

4 We use the SmartResilience ECHO case as an example throughout Section 2.2.3 (calculation) and 2.2.4 (use of results). It is not a "real" case, since the value ranges and the "real values" are only assumed values.
Assigning weights (optional)

For all levels, it is necessary to determine weights, i.e. whether one indicator is more important than the other indicators, whether one issue is more important than the other issues, and so on, or if they are considered equally important (or there is no evidence of giving them unequal weights). It is advocated that one should be cautious with the use of unequal weights unless it is considered highly unrealistic to use equal weights. It is both challenging to establish trustworthy weights, and it results in less transparent calculations. The weights are by default equal; however, it is possible for the user to adjust the weights. This should be justified and documented. Equal weight of n indicators is simply 1/n.

Whether equal or unequal weights, the sum of weights should of course sum up to unity (1.0).

If the default equal weights are considered too unrealistic, the weights can be changed. A simple method to assign weights is to use a type of pairwise comparison. It is not only stating which are the most important resilience indicator (RI) of the two being compared, but also the relative difference. Thus, there are two questions asked:

Q1: Which of the RIs is the most important indicator in measuring issue k, i.e. the RI*?
Q2: How many more times important is this RI* compared to each of the RIs, i.e. RI*/RIj?

Assume that issue no. k is assessed by nj different indicators, j=1,…, m. The weight of each indicator, $v_{kj}$, is then calculated as:

$$v_{kj} = \frac{1}{RI_j} / \sum_{j=1}^{m} \frac{1}{RI_j}$$

The method is easiest explained using an example. Table 10 shows an example with four resilience indicators measuring one issue (issue no. k).

**Table 10: Example of assigning weights to resilience indicators**

| Indicator (RI) | Q1: Most important RI? | Q2: Relative importance? RI*/RIj | Inverted importance 1/(RI*/RIj) | Weight ($v_{ij}$) [1/(RI*/RIj)]/SUM | Weight [%] $v_{ij} \times 100$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>R1i</td>
<td></td>
<td></td>
<td>1/2</td>
<td>0.177</td>
<td>17.7</td>
</tr>
<tr>
<td>R1z</td>
<td>R1i</td>
<td></td>
<td>1/1</td>
<td>0.353</td>
<td>35.3</td>
</tr>
<tr>
<td>R1s</td>
<td></td>
<td></td>
<td>1/3</td>
<td>0.118</td>
<td>11.8</td>
</tr>
<tr>
<td>R1s</td>
<td>R1i</td>
<td></td>
<td>1/1</td>
<td>0.353</td>
<td>35.3</td>
</tr>
<tr>
<td>SUM</td>
<td></td>
<td></td>
<td>2.83</td>
<td>1.0</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 10 shows that the answer to Q1 is resilience indicator no. 2. This is then compared with all the indicators (including itself) by asking Q2. The example answers are that R1* (=R1i) is 2 times as important as R1i, equally important as itself of course, 3 times as important as R1s, and equally important as R1s. These values are then inverted and summarized (in column 4).

The weights are obtained by dividing the inverted importance values for each RI with the sum of the inverted importance values (in column 5). The weights can also be presented as percentages (in column 6).

---

5 In principle, the method can also be adapted to direct scoring of issues, but then it is no longer an indicator-based method.
The same procedure applies for issues (importance for each of the five phases), for phases (importance for each threat), for threats (importance for each SCI), and finally for SCIs (importance for an area).

Unequal weights are most relevant for resilience indicators and resilience issues. There should be extraordinary reasons to change the weights of the phases from 20% each. The resilience assessment methodology is a holistic approach considering all phases of the resilience cycle. Allowing for unequal weighting of phases may result in unequal weights due to bias toward certain phases, not because it can be proved or argued that they are more important. For threats, one should be cautious not to mix the weights with the likelihood of the events. The resilience assessment is not a probabilistic assessment. Finally, assigning unequal weights of SCIs is a political matter, which is not up to an assessor to decide. If necessary, unequal weights should be decided by e.g. a city council.

Assignment of unequal weights should be substantiated and documented, including who the expert or experts are, and how the relative importance was obtained.

**Direct weighting**

A very simple way of assigning weights is to assign or distribute weights directly. Instead of a group of experts answering the questions Q1 and Q2 above, they can simply distribute the total weight of 1.0 on the set of indicators (or issues). E.g. they could assign 0.20, 0.35, 0.10 and 0.35 to the four indicators in Table 10 directly, and then perhaps make some adjustments to these based on discussions/justifications in the group. Even if a simple approach is applied, it should be documented.

### 2.3.3.2 Step 8. Assign values to the indicators

This is the step where data is collected for the indicators, i.e. where the real values of the indicators are assessed/determined.

The values of the indicators can be assigned by experts, come from monitoring systems or from big data analysis.

The real values of the indicators are used to determine indicator scores and aggregated calculations in Step 9. The calculations start from the indicators (level 6) and are aggregated upwards to issues (level 5), phases (level 4), threats (level 3), SCI (level 2) and finally area (level 1).

### 2.3.3.3 Step 9. Perform the calculations (i.e. calculate scores and resilience levels)

The resilience assessment methodology in SmartResilience is deliberately made simple and transparent, and it is possible to perform the calculations by hand. However, it is more practical to use an Excel spreadsheet or some other tool to perform the calculations, in particular for use of the results in Step 10. The resilience assessment calculations can also be performed using the SmartResilience Integrated Tool described in Chapter 6.

The overall scoring process – level by level (from indicator to area) – is illustrated in Figure 6. The left part of the figure illustrates the assigned real indicator values, which are converted to a score between 0 and 5 according to the description in Step 7 (Table 9). Each indicator will then have an exact score between 0 and 5, which corresponds to a resilience level between E and A, e.g. a score in the range [0, 1) corresponds to RIL=E, and so on. Similar applies for the issues, which are sums of weighted scores for the indicators; for phase scores that are sums of weighted scores for issues; and similar also for threats, SCIs and area. In all cases, the scores correspond to a given resilience level, as indicated to the right in Figure 6.

From the overall result for an area, we can go backwards (“drill down”) through the levels 2 to 6 for detailed results, which can be used in Step 10, together with the overall result. We do not have “just one number.”

Drilldown means that we provide information of what contributes most to, say a RIL=B and a score=3.06, on area level. What is the resilience level and score on the individual SCIs, and further down to the contributions

---

6 The calculations according to the methodology are now fully implemented in the SmartResilience tool ([http://www.smartresilience2.eu-vri.eu/RunningApp/ Ridb/SCIDashboard.aspx](http://www.smartresilience2.eu-vri.eu/RunningApp/Ridb/SCIDashboard.aspx)) and can be found there under the menu item “assessments.”
from the individual threats, phases, issues and finally, the individual indicators? The drilldown is illustrated for an example application in Section 2.5.

### 2.3.4 Use the results and make decisions

#### 2.3.4.1 Step 10. Provide status, trends, strength and weaknesses, improvement needs, benchmarking, etc.

There are many possibilities for use of the results. Some examples are:

1. Following up own development over time (trending) and analysing current resilience status
2. Providing overview of strengths and weaknesses and pointing at improvement needs
3. Comparing with others (benchmarking)

#### 1. Following up own development over time (trending) and analysing current resilience status

It is reasonable to aim for continuous improvement in overall resilience over time, i.e. that the trend shows a development in the direction of increased resilience. This is what the overall RIL can show. It shows both the status at this point in time, when the last resilience assessment was performed, and how it has developed from the previous assessments.

We can also compare the status at the different levels, e.g. compare the status of the different SCIs (and thus the contribution to the overall area score/RIL) and compare status/contribution from the different threats to the SCIs score/RIL. Further, we may compare the contributions from the phases to the threat with the lowest score/RIL, the contributions from the issues to the phase with the lowest score/RIL, and finally the indicators contributing to the issue with the lowest score/RIL.

Trending, i.e. comparing with oneself from time period to time period, is particularly useful in the sense that the user has full control over the “fairness” of the comparison. The exact same indicators can be used in the exact same way in every assessment, making the assessments fully comparable. The entire “model” (all issues and indicators, the range of values, the data providing input to the indicators, etc.) can be perfectly customized to a specific user, according to the user’s own requirements.

#### 2. Providing overview of strengths and weaknesses and pointing at improvement needs

Overviews of strengths and weaknesses can be presented at different levels using the status in terms of score or RIL and based on this identify improvement needs. This is partly treated in point 1 above, showing some of the contributors to high or low resilience, i.e. strengths and weaknesses. However, also complete

---

**Figure 6: Scoring process**
lists of all indicators and all issues (or "top ten" or "top five" lists) can be provided, sorted according to their score values and/or RILs.

The status information can also be used to answer specific questions such as:

- Which critical infrastructure is the most vulnerable (lowest score/RIL)?
- Which threat is the most challenging (lowest score/RIL)?
- What is the "weakest" phase (lowest score/RIL)?
- Which issues contributes the most to low score/RIL in the "weakest" phase?
- Which issues contributes most to low score/RIL (overall)?

With the help of other parts of the methodology (see Chapter 4), it may also be possible to answer questions such as:

- What is the single most optimal improvement measure?
- What are the ten most optimal improvement measures?
- What is the optimal set of improvement measures (among different sets)?
- What are the most optimal improvement measures within each phase?
- Given a certain budget for resilience improvement; what is the most optimal use of the budget?
- How much will it cost to improve the overall RIL from B to A?

3. Comparing with others (benchmarking)

Comparing resilience assessment results with others is useful. It provides an opportunity to see where the differences are by comparing RILs and scores on every level, and one can learn from each other in order to improve. Benchmark results showing that one performs poorly compared to others can also be used as arguments for increasing budgets for measures that can increase the resilience.

The challenge with benchmarking is the degree of comparability. If the "model" (issues and indicators, etc.) is adapted by a user, then the results become less comparable with other users. On the other hand, if there is little flexibility in adapting or customizing the issues and indicators, then the users may consider the resilience assessment as less relevant and not providing a realistic picture of their status.

In SmartResilience, we attempt to satisfy both customization and benchmarking through the use of common generic issues in a so-called "Core DCL," see Section 2.4.

2.4 Conclusion

The purpose of assessing resilience is to obtain a quantitative measure of how resilient a city or an individual SCI are against severe threats such as terror attacks, cyber-attacks and extreme weather. Assessing RIL provides a baseline assessment of resilience that gives insight on status and improvement needs to increase or maintain a high level of resilience. This is illustrated in Figure 7.

A RIL assessment goes beyond traditional risk assessments, e.g. by focusing on the unknown and unforeseen, and it captures the time dimension through (five) distinct phases. A RIL assessment is not a substitute for risk assessment, in fact risk assessments provide valuable input specially to phase I "Understanding risks". The RIL assessment is complementary by providing a broader perspective and focusing on rare events.

Some specific topics have been included in the analysis framework, described in Step 3 and 5. The topics are:

1. Dependencies and interdependencies
2. Cascading effects
3. Interoperability
4. Smartness opportunities and vulnerabilities

We strive for a good balance between the comprehensiveness of the analysis framework and the simplicity of understanding and using the framework. Thus, the specific topics have been addressed explicitly, but rather simplistic. The topics have been considered from an individual SCI point of view, whereas a comprehensive assessment goes beyond the single SCIs and should consider a network of SCIs.
Dependencies, interdependencies and cascading effects are treated comprehensively in SmartResilience deliverable D2.3 [45], and smartness is treated in D2.1 [44]. See also Chapter 5.

The resilience level assessment method can facilitate both a tailor-made assessment and a possibility to benchmark the results. The selection of issues and indicators used in an assessment is referred to as a dynamic checklist (DCL), since it can be adapted to each user "dynamically"; however, a part of the DCL consists of generic issues (Core DCL) relevant for all users, which facilitates benchmarking across SCIs. The resilience level assessment method can be used by both internal resources (self-assessment) and third parties (external assessors).

The same issue can, and will easily, be measured with different indicators by different users, as illustrated in Figure 5. One user may use three indicators, whereas another user uses two indicators. Thus, for two different users, the same issue may be measured using different sets of indicators. This makes it difficult to identify a core list of indicators common for all users (the "Core DCL"). Instead, the "Core DCL" consist of common issues. Although the indicators and thereby the coverage may be different, it can be defended to compare (benchmark) the score provided on the issue, if a user is not deliberately selecting only indicators that he/she knows will provide a high score.

In this chapter, we have described how to perform a RIL assessment without use of the SmartResilience web-based tool. In Chapter 6, it is described how to perform a RIL assessment using the tool, including the creation of DCLs. The advantages of using the tool are e.g. the access to existing DCLs and the database of issues and indicators, calculations performed by the tool, and visualization of the results.

The RIL assessment is an indirect assessment using a broad range of indicators, which is independent on the occurrence of events. Most SCIs around the world have never, and will never, experience an extreme event. Still it is possible to assess the RIL, i.e. the level of risk understanding, anticipation and preparation, the
capability to absorb and withstand, to respond and recover, and the abilities to learn and adapt. With a high RIL, it is less likely to experience an extreme event, and should it occur, then the severity and duration of disruptions are likely to be reduced.

2.5 Application examples
The ECHO case is used as example throughout all the steps of the methodology, whereas DELTA, FOXTROT and HOTEL are used as partial examples in the first three steps.

2.5.1.1 Step 1. Select the area (Level 1)
- DELTA: Budapest airport, Hungary
- ECHO: Southern Industrial Zone in city of Pančevo (part of the city), Serbia
- FOXTROT: Stockholm region, Sweden
- HOTEL: City of Helsinki, Finland

2.5.1.2 Step 2. Select the relevant SCIs (Level 2)
- DELTA: Transport – Air traffic – Airport
- ECHO: Chemical industry – Production and storage/processing of chemical substances
- FOXTROT: Water – Provision of drinking water & Control of water quality
- HOTEL: Energy – Underground fuel storage and energy supply (added as a new subsector)

2.5.1.3 Step 3. Select the relevant threats for the SCIs (Level 3)
- DELTA: Terrorist attack, Cyber attack and Extreme weather
- ECHO: Terrorist attack, Natural threats and New technology related threats
- FOXTROT: Terrorist attack, Natural threats and Contamination of water
- HOTEL: Natural threats, New technology related threats and Interruption in critical supply

An example of scenarios defined through the steps 1 to 3 is illustrated in Figure 8, i.e. the first three levels in the model are defined. The example used is ECHO.

---

**Figure 8: Example of scenario definition (area – SCIs – threats)**
### 2.5.1.4 Step 4. Consider each phase for each threat (Level 4)

Issues and indicators must be included in each of the five phases (see Steps 5 and 6).

### 2.5.1.5 Step 5. Define the issues for each phase (Level 5)

Examples of issues (based on the ECHO case using sources no. 2 or 3, cf. Section 2.2.2.2):

- Safety risk registry
- Register of accidents/incidents
- Emergency exercises

In Figure 9, the location of the issues in the hierarchical model is illustrated for terrorist attack (threat no. 1), and in Figure 10, the issues are illustrated for natural threats (threat no. 2). In this case, the example issues happen to be similar for both threats (as seen in the figures), and they are also the same for the third threat (new technology related threats).
The two first issues are relevant for the first phase, whereas the third issue is relevant for the second phase. Which dimensions the issues belong to are not important to establish; thus, the rows in the resilience matrix are removed. (It may be assigned in the SmartResilience tool to see the coverage of various dimensions, cf. Chapter 6).

2.5.1.6 Step 6. Search for appropriate indicators for each issue (Level 6)

Examples of indicators for selected issues (based on the ECHO case using source no. 3, cf. Section 2.2.2.3):

- Safety risk registry
  - Does a safety risk register exist with clear classification of the risk level?
  - Is the registry used in decision making?
  - Is a frequency for updating the registry defined?
- Register of accidents/incidents
  - Does an accident/incident register exist?
  - Frequency of communication about incidents from the register with operator
  - Percentage of employees informed about incidents from this register
- Emergency exercises
  - Does an emergency exercise plan exist?
  - Percentage of exercises completed according to schedule
  - Percentage of emergency responders who have completed the scheduled training

In Figure 11, the location of the indicators in the hierarchical model is illustrated for the first issue (for threat no. 1). All three example indicators belong to the same phase as the issue, i.e. the first phase, even if the boxes are stretched across several phases (for readability).

2.5.1.7 Step 7. Determine the range of values for each indicator (and optionally weights)

Examples of assignment of ranges of values for each indicator is provided in Table 11 (based on the ECHO case).
Table 11: Determining ranges of values for each indicator - examples

<table>
<thead>
<tr>
<th>Indicator values, score values and resilience levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indicator values</strong></td>
</tr>
<tr>
<td><strong>Indicator value range label:</strong></td>
</tr>
<tr>
<td><strong>LL</strong></td>
</tr>
<tr>
<td>I.3.1 Does an accident/incident register exist?</td>
</tr>
<tr>
<td>I.3.2 Frequency of communication about incidents [per month]</td>
</tr>
<tr>
<td>I.3.3 % of employees informed about incidents from this register</td>
</tr>
</tbody>
</table>

The first indicator is a Yes/No question, and the two last are non-linear quantitative indicators.

If direct scoring is applied, then ranges of values are not strictly needed. The last question could be rephrased to: "On a scale from 0 to 5, how well are the employees informed about the incidents in the risk register?"

It will of course be beneficial to have some indication of what a score of 0 or 5 means, in order to have similar scoring by different persons (increasing the indicator reliability).

2.5.1.8 Step 8. Assign values to the indicators

Examples of assigning real values to the indicators are shown for the indicators related to issue I.3 (Register of accidents/incidents).

I.3 Register of accidents/incidents

I.3.1 Does an accident/incident register exist?     Yes
I.3.2 Frequency of communication about incidents from the register with operator 1/6mth
I.3.3 Percentage of employees informed about incidents from this register 80%

I.e. the register exists, new entries are communicated with the operators every 6 months and 80% of the employees have been informed about incidents in the register.

2.5.1.9 Step 9. Perform the calculations (i.e. calculate scores and resilience levels)

Calculations on indicator level (level 6)

An example of calculations on the indicator level (level 6) is provided for the indicators related to issue I.3 (Register of accidents/incidents).

First, the indicator score values are obtained using Table 9 and Table 11, i.e. 5.0, 1.5 and 3.5:

I.3.1 Does an accident/incident register exist?     Yes 5.0 (A)
I.3.2 Frequency of comm. about incidents from the register with operator 1/6mth 1.5 (D)
I.3.3 Percentage of employees informed about incidents from this register 80% 3.5 (B)

Alternatively, the score values could have been provided by "direct scoring" on a scale between 0 and 5, without predefined ranges of values for each indicator.

The indicator score values also correspond directly to an indicator resilience level, i.e. A, D and B (cf. Table 9).

Equal weights for indicators

Using equal weights would yield a weight for each of the three indicators of 1/n = 1/3. The indicator weighted scores are then obtained by multiplying the indicator scores with the indicator weights, i.e.:

I.3.1 5.0 • 1/3 = 1.67
I.3.2 1.5 • 1/3 = 0.50
I.3.3 3.5 • 1/3 = 1.17

Unequal weights for indicators

An example of assigning unequal weights is shown for issues below following the procedure described in Section 2.2.3.1. It is performed in exactly the same way at all levels (indicators, issues, phases, etc.).
**Calculations on issue level (level 5)**

An example of calculations on the issue level (level 5) is provided for the issues related to phase I (Understand risks).

The issue scores are obtained (calculated) as the sum of the weighted scores for the underlying indicators, i.e. for issue I.3 this is (see above): 1.67 + 0.50 + 1.17 = 3.33. In a similar way, we obtain the scores for issue I.1 and issue I.2. The scores for each of the three issues in phase I (and corresponding resilience levels) are as follows:

- I.1 Safety risk registry 3.33 (B)
- I.2 Management of change (MoC) 0.00 (E)
- I.3 Register of accidents/incidents 3.33 (B)

The score for issue I.1 happens to be the same as for issue I.3.

**Equal weights for issues**

For equal weights, we proceed in the same manner as for indicators.

**Unequal weights for issues**

We use the method explained in Section 2.2.3.1. Here we assign weights to issues instead of indicators (assume now that RI means Resilience Issue, instead of Resilience Indicator).

Q1: Most important Resilience Issue? Answer: Safety risk registry (RI₁ = RI*).
Q2: Relative importance? Answer: See third column in Table 12 below.

<table>
<thead>
<tr>
<th>Issue (RI)</th>
<th>Q1: Most important RI?</th>
<th>Q2: Relative importance?</th>
<th>Inverted importance</th>
<th>Weight (wᵢ)</th>
<th>Weight [%] ( wᵢ \times 100 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>RI₁ (Risk registry)</td>
<td>RI*</td>
<td>1</td>
<td>1/1</td>
<td>0.50</td>
<td>50</td>
</tr>
<tr>
<td>RI₂ (MoC)</td>
<td>3</td>
<td>1/3</td>
<td>0.17</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>RI₃ (Accident reg)</td>
<td>1.5</td>
<td>2/3</td>
<td>0.33</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>SUM</td>
<td>2</td>
<td>1.0</td>
<td></td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Thus, we have now obtained the scores 0.50, 0.17 and 0.33 (instead of 0.33 for all with equal weights). The issue weighted scores are then obtained by multiplying the issue scores with the issue weights, i.e.:

- I.1 3.33 · 0.50 = 1.67
- I.2 0.00 · 0.17 = 0.00
- I.3 3.33 · 0.33 = 1.11

**Calculations on phase level (level 4)**

The Phase I (Understanding risks) score is obtained (calculated) as the sum of the weighted scores for the underlying issues, i.e.: 1.67 + 0.00 + 1.11 = 2.78. With equal weights of the issues, the Phase I score would have been 2.22. In both cases, the resilience level of Phase I is RIL=C, since the score is between 2 and 3.

In some cases, it may be equally appropriate to assign the weights directly, e.g. I.1=0.5, I.2=0.2 and I.3=0.3. Using the method above with relative importance may easily provide very exact weights with an implied precision which may not be justifiable (e.g. 0.353 as shown in Table 10).

**Calculations on threat, SCI and area levels (levels 3, 2 and 1)**

The calculations proceed in the exact same manner for all the levels until we reach level 1 (area level). It is less relevant to use unequal weights for phases, threats and SCIs, as discussed in Section 2.3.3.1.

The details are shown in D3.8 [52]. There it is shown that the overall score is 3.06 and a RIL=B (for both area and SCI, since there is only one SCI included).
2.5.1.10  Step 10. Provide status, trends, strength and weaknesses, improvement needs, benchmarking, etc.

Examples of use of the results are provided for:

1. Following up own development over time (trending) and analysing current resilience status
2. Providing overview of strengths and weaknesses and pointing at improvement needs

1. Following up own development over time (trending) and analysing current resilience status

Trending

From the calculations in Step 9, we have obtained an overall score of 3.06 and a RIL=B, which represents the overall results at a given point in time (when performing the assessment). We now assume that this resilience level assessment is repeated at regular intervals, typically yearly, and that the current assessment is the fifth assessment, i.e. at time T5. We further assume that the previous assessment resulted in RIL=C. Thus, the overall resilience level has developed from C "average" at time T4, to B "good" at time T5 (the current status). This is illustrated in Figure 12, providing a trend line.

![Figure 12: Trending of overall resilience level - example](image)

The overall RIL on area level, as shown in Figure 12, or the corresponding overall score (which is 3.06 in this example), just represents one aggregated character or value, which gives limited information. To see what lays behind and contributes to the overall development, we need to "drill down." Similar presentations as in Figure 12, showing the trend on overall area level, can be made at each of the lower levels.

Status

Figure 13 provides information about scores and RILs at different levels. (The area level and the SCI level are assumed to be the same in this case). It shows typical information from a "drilldown."

The overall "good" status shown in Figure 12 is primarily due to a "good" resilience against Threat 3 – New technology related threats with a score of 3.90 (upper left part of Figure 13).

The contributions to the worst threat (Threat 1 – Terrorist attack with a score 2.64, which is equal with Threat 2 – Natural threats) show that Phase I – Understand risks provides a score 2.22, which is the lowest phase score (upper right part of Figure 13).

This phase with the lowest score consists of three issues, of which two are assessed as "good" and one is "critical" (lower left part of Figure 13). The reason for the latter result is that this issue simply consists of one Yes/No indicator, and the answer was "No"; thus, a score equal zero.

The third issue consists of three indicators (lower right part of Figure 13); one scoring 5.0 – "excellent," one scoring 1.5 – "poor" and one scoring 3.5 – "good."

These results show e.g. that there is a need to improve the "frequency of communication about incidents from the accident register with operators" and the issue "management of change."
D3.6 Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures (SCIs)

2. Providing overview of strengths and weaknesses and pointing at improvement needs

The status information can also be used to answer specific questions such as:

- Which critical infrastructure is the most vulnerable (lowest score/RIL)?
- Which threat is the most challenging (lowest score/RIL)?
- What is the "weakest" phase (lowest score/RIL)?
- Which issues contributes the most to low score/RIL in the "weakest" phase?
- Which issues contributes most to low score/RIL (overall)?

Table 13 shows "top five" and "bottom five" lists of issues based on the ECHO case (using one of the threats). The "bottom five" list points to improvement needs; however, to choose optimal improvement measures need to take more than just the score or RIL into account. This is treated in Chapter 4.

Table 13: "Top five" and "bottom five" issues - example

<table>
<thead>
<tr>
<th>Top five issues</th>
<th>Score</th>
<th>RIL</th>
<th>Bottom five issues</th>
<th>Score</th>
<th>RIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Events at the site</td>
<td>4.00</td>
<td>A</td>
<td>1. Management of change – MoC</td>
<td>0.00</td>
<td>E</td>
</tr>
<tr>
<td>2. Hi Hi alarm</td>
<td>3.50</td>
<td>B</td>
<td>2. Start ups and shut downs</td>
<td>1.50</td>
<td>D</td>
</tr>
<tr>
<td>2. Safety equipment</td>
<td>3.50</td>
<td>B</td>
<td>3. Inspection visits measures</td>
<td>1.63</td>
<td>D</td>
</tr>
<tr>
<td>5. Safety risk registry</td>
<td>3.33</td>
<td>C</td>
<td>5. Fire fighters present at the site</td>
<td>1.83</td>
<td>D</td>
</tr>
</tbody>
</table>
Answers to the five questions raised above for the ECHO case are:

- There is only one SCI in the ECHO case, which is Chemical industry
- The most challenging threats are Terrorist attack and Natural threats (equal); S=2.64 and RIL=C
- The “weakest” phase is Phase I: Understand risks; S=2.22 and RIL=C
- The issue Management of change – MoC contributes most to low score/RIL; S=0.00 and RIL=E in the weakest phase
- The issue Management of change – MoC also contributes most to low score/RIL; S=0.00 and RIL=E overall, as shown in Table 13.
3 Resilience modelling – functionality assessment and stress-testing

3.1 Introduction and purpose

With reference to the resilience curve in Figure 1 (in Chapter 1), it was stated that resilience is measured in two different ways in the SmartResilience project. The first was presented in the previous chapter and is an indirect measurement of the level of resilience using indicators. It does not consider the shape of the resilience curve.

The second way to measure resilience is explained in this chapter. It measures the loss of critical functionality directly, considering resilience as inversely proportional to the loss of critical functionality, i.e. the less critical functionality that is lost, the more resilient the SCI. In this case, the shape of the resilience curve is modeled, either the complete curve or some characteristics of the curve through so-called macro-indicators. This is illustrated in Figure 14 [48].

![Critical functionality curve and its characteristics](image)

The two core variables are the critical functionality level (FL) and the points in time (t), which define the FL-t curve. The curve typically starts from 100% FL, with a certain % loss of functionality during the absorb/withstand phase and the respond/recover phase. It may have a permanent loss or improvement in the adapt/transform phase. This curve is obtained through a 10-step FL assessment method.

The FL assessment four-level model/structure behind the 10-step method is illustrated in Figure 15, where the four levels are:

- Level 1. Functionality level (FL) of the city (or area)
- Level 2. Functionality level (FL) of the infrastructure (SCIs)
- Level 3. Functionality elements (FEs)
- Level 4. Functionality indicators (FIs)
3.2 Basic concepts and terms

3.2.1 Concepts of functionality level, elements, and indicators

The functionality of an 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. Functionality elements (FEs) 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 resilience level assessment methodology, cf. Chapter 2). Functionality indicators (FIs) are quantifiable units used to measure the functionality elements. As in the resilience level assessment methodology (cf. Chapter 2), indicators are used for this assessment. Functionality, functionality elements, and functionality indicators are further described in Figure 16.

3.2.2 Characteristics of the critical functionality curve – macro-indicators

The following macro-indicators are proposed for modeling the impact of the disruption:

- Robustness
- Absorption time
- Downtime
- Loss of functionality
Robustness is defined as the capacity of the SCI to endure the effects of a negative event and thereby absorb its impact. 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 also undergoing a decrease in functionality level. As illustrated in Figure 14, it is measured as the difference between \( t_2 \) and \( t_1 \).

\[
\text{Absorption time} = t_2 - t_1
\]

Downtime is defined as the time duration for which the system is not functional, which is the time period where the functionality level of the infrastructure remains below the threshold level of functionality [8]. It can be measured as the difference in time between \( t_3 \) and \( t_2 \) (see Figure 14).

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

Note: This calculation is conducted when the threshold level of functionality is defined. (Here it is assumed that the threshold level is \( FL_{t_2} (=FL_{t_3}) \)).

Loss of functionality is functionality of the SCI lost in a given threat situation. It is measured by the area of the curve between the time when SCI starts to lose its functionality \( (t_1) \) to the time when it reaches the initial state \( (t_4) \) (see Figure 14). An approximation can be made for the area above the curve using a well-defined shape e.g. a triangle. The output would be the percentage of loss of functionality in time [41], e.g. losing 10% in 10 hours.

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

Recovery time is defined as the time at which the SCI recovers from the disruptive event and gains its initial or desired functionality [62]. It can be measured as the time taken to recover the functionality level, i.e. the time between \( t_3 \) 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 the start of the scenario, the recovery time may have to be measured at a new steady state level [39].

Recovery rate is defined as the rate at which the SCI recovers from a disruptive event and gets back to its initial functionality level [62]. It characterizes the recovery trajectories of the SCI from the point it starts recovering of the scenario to the final recovery. It is measured as the ratio of change in functionality level between time \( t_3 \) and \( t_4 \).

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

Disruption time is defined as the 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 [62]. In the 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 14).

\[
\text{Disruption time} = t_4 - t_1
\]
Improvement/adaptation/transformation: Final recovery of the FL of an SCI could be equal to, better than, or worse than the original FL [61]. Hence, the model allows to calculate the “Improvement/adaptation/transformation.” It 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 [44]), see Figure 14. It is measured as the ratio of change in FL during and after the event over the initial FL.

\[
\text{Improvement/adaptation/transformation} = \frac{FL_{t=5} - FL_{t=0}}{FL_{t=0}} \times 100\%
\]

3.2.3 Concept of stress-testing

Stress-testing is about testing of the system/structure under abnormal (exceptional) conditions [1]. A more elaborated definition is [10]:

A simulation test to determine how a given institution, system, etc., would perform under greater than usual stresses or pressures: the government’s stress test for big banks; mandatory stress tests for nuclear plants; a website stress test that simulates peak traffic.

In the SmartResilience project, the critical functionality curve, FL-t curve (or resilience curve), is used as basis for stress-testing, as illustrated in Figure 17.

![Image of Stress-testing SCIs using the resilience curve (based on [29])](image)

In the case illustrated in Figure 17, it is strictly only the thick purple curve (“FL: as before”) that passes the stress-test, all other curves fail since they cross the stress-test limit line. For more information on stress-testing, see D5.2 [56].

3.3 Method description – functionality level assessment

The functionality level assessment is performed in 10 steps, as listed in Table 14. Similar to issues and indicators in the RIL assessment (cf. Chapter 2), the functionality elements and functionality indicators are selected by the user and included in a list – a Dynamic Checklist (DCL). The creation of DCLs is supported by the SmartResilience integrated tool. The DCL setup consists of four steps, which are included in the 10 FL assessment method steps, i.e. the FL assessment method description assumes the use of the SmartResilience tool. In principle, the FL assessment could be performed without using the SmartResilience tool (similar as for the RIL assessment).
### Table 14: Steps for functionality level assessment

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the SCI(s) to be assessed</td>
</tr>
<tr>
<td>2</td>
<td>Identify relevant threats for each SCI and initiate respective DCLs</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>

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

In the SmartResilience project, an SCI is a critical infrastructure whose functionality is enhanced using smart (i.e., intelligent) systems and technologies [44]. In Step 1, the SCI owner/operator selects the SCI(s) to be assessed.

#### 3.3.1.2 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 7 (in Chapter 2). Afterwards, the user must initiate a DCL for the selected SCI(s) and threat(s) in the SmartResilience dashboard, as well as provide basic information on the scenario (e.g., scenario name, description, DCL name, type of SCI, threats, and DCL description).

If the FL assessment is going to be used for stress-testing, then the stress-test scenario should be described, including threshold values.

#### 3.3.1.3 Step 3: Identify interdependencies between the selected SCIs

Smart cities are comprised of several 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 SCIs is also affected. These can be considered in evaluation of the FL of the SCI. See Chapter 5 for more on identification of interdependencies.

#### 3.3.1.4 Step 4: Define functionality elements (FEs) for each DCL

For each DCL, the user must 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 18 provides some examples of FEs.

#### 3.3.1.5 Step 5: Define appropriate functionality indicators (FIs) for each FE in each DCL

In Step 5, appropriate FIs for each FE are defined. Figure 18 provides some examples of FIs.

#### 3.3.1.6 Step 6: Assign maximum, minimum, and target/best values to all FIs (optionally assign weights)

Assign maximum, minimum, and target/best values to the functionality indicators. These values should be assigned in terms of measurable units such as percentages, numbers, etc. Minimum, maximum, and target/best values can be used to define the current FL of the infrastructure as a percentage, if it is not assigned directly as a percentage (i.e., number, frequency, etc.). The target/best values are used to decide on the direction of the measurement, i.e., dependent on whether the minimum value is assigned as the target/best value or if the maximum is assigned as the target/best value.
The indicator values are normalized to a corresponding percentage using the following equations, depending on whether the target/best value is the minimum or the maximum value:

- If the target/best value is the minimum (as a percentage):
  \[
  F_{Inorm} = \frac{\max(F_i) - F_i}{\max(F_i) - \min(F_i)} \times 100
  \]

- If the target/best value is the maximum (as a percentage):
  \[
  F_{Inorm} = 1 - \frac{\max(F_i) - F_i}{\max(F_i) - \min(F_i)} \times 100
  \]

where: \( F_{Inorm} \) is the normalized assessment of \( F_i \).

These equations simply transform non-percentage values to percentage values. As an example, assume that the maximum value is 15 (a number) and the minimum value is 0. Further assume that the maximum value is the target/best value (which means that the second equation applies). If we have an indicator value of 6 (actually assigned in Step 8 below), we then calculate (actually performed in Step 9 below):

\[
F_{Inorm} = [1 - (15-6)/(15-0)] \cdot 100 = (1-9/15) \cdot 100 = 40\%
\]

In other words, the indicator value of 9 (as a number) is transformed to an indicator percentage value of 40%.

This is done for all time points (assigned in Step 7 below). Normally, the nominal value for the indicator at \( t_0 \) is 100% (i.e. a value of 15 in the example above).
For simplicity, the default weights are equal. However, the user may choose to assign different weights. This can be done in a similar manner as for resilience level assessment (see Section 2.2.3.3), and the FL is calculated as the weighted sum of the FIs according to the following equation:

$$FL = \sum_{i=1}^{n} F_{i}^{\text{norm}} \cdot w_{i}, \text{where } w_{i} > 0 \text{ for all } i = 1, ..., n \text{ and } \sum_{i=1}^{n} w_{i} = 1$$

where: FL is the functionality level, $w_{i}$ is the weight concerning the $F_{i}$, and $n$ is the number of functionality indicators.

As an example, assume three FIs with (normalized) values 100%, 80% and 60%, and with corresponding weights 0.1, 0.2 and 0.7. Then we calculate (actually performed in Step 9 below):

$$FL = F_{1} \cdot w_{1} + F_{2} \cdot w_{2} + F_{3} \cdot w_{3} = 100 \cdot 0.1 + 80 \cdot 0.2 + 60 \cdot 0.7 = 10 + 16 + 42 = 68\%$$

I.e. the weighted value is 68%, since the third value (60%) is assigned a high weight. Using default equal weights would have resulted in FL = 80%.

This calculation is supported in the SmartResilience tool; however, it should be noted that the weighted sum is applied for all FIs across all FEs, meaning that an FE with many indicators will obtain a higher weight. Alternatively, the FE should be calculated first, and then provide weights for the FEs in a second step. This is similar to the way indicators and issues (and even higher levels) are provided weights separately in the resilience level assessment, cf. Chapter 2.

### 3.3.1.7 Step 7: Assign time values for the scenario

The user must provide values for the time points that characterize the FL-t curve of the possible disruptive event, i.e. where the curve changes the gradient. These time points can be broadly categorized as follows:

- $t_{0}$: time before the event or starting point of the scenario
- $t_{1}$: time at which the event occurs
- $t_{2}$: time at which the infrastructure reaches the minimum functionality level
- $t_{3}$: time at which the infrastructure starts to recover
- $t_{4}$: time at which the infrastructure reaches the initial functionality level or starting point of a new steady state level
- $t_{5}$: 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 point values. 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 (default if time values are not assigned or are unknown)
- Relative time (from $t_{0}$)
- Calendar time

### 3.3.1.8 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 (e.g. like the number of 9 in the example in Step 6). In this case, the user should also have assigned maximum, minimum, and target/best values (in Step 6). Based on these values, the SmartResilience dashboard will calculate the functionality level as a percentage between 0 to 100 using the equations presented in Step 6. The user could also choose to use percentage for each FI directly. In this case, the SmartResilience dashboard will only apply the last equation in Step 6 (with equal or unequal weights) and 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/nominal functionality level, and the FL levels for the other points in time would be defined relative to $t_{0}$.
3.3.1.9 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 (if relative time or calendar time have been assigned), as illustrated in Figure 14:

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

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

The main purpose of the functionality level assessment is to provide understanding of how a disruptive event affects the critical functionality of an infrastructure. This is obtained by modelling the FL-t curve, including the absorb and recover capacity, and the curve can be characterized by the macro-indicators. The results can be used for purposes including:

1. Improving resilience, including the absorb and recover capacity
2. Benchmarking (comparing with others)
3. Stress-testing

1. Improving resilience including the absorb and recover capacity

Based on the FL-t curve, either from a real event or a simulated event, improvements may be deemed necessary. For example, this can include better absorb capacity, shorter downtime, faster recovery, less loss of functionality, and better adaptive capacity (or improvement in any other macro-indicator). The improvements can be assessed and visualized by a new FL-t curve for a similar event, as illustrated in Figure 19.

![Figure 19: Improving resilience](image)

For a new/different event, a new FL assessment is performed modelling the behavior of the infrastructure, which then constitutes a basis for new improvements.

2. Benchmarking (comparing with others)

The methodology proposed for functionality assessment can be used for benchmarking, i.e. comparing the functionality of different SCIs, as illustrated in Figure 20. 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.

It could also be a direct comparison of the measured resilience, i.e. the inverse of the loss of functionality, or just comparing the loss of functionality directly, i.e. "the area under the curve." The lesser the area under the curve, the better.

Comparisons can also be made for each of the other macro-indicators.

3. Stress-testing

Full-scale stress-testing will be treated as a separate method in the next section (see Section 3.4). However, partial stress-testing can also be performed, focusing on, for example, only the downtime, the recovery time, or the disruption time. It can even be just parts of these, e.g. evacuation time tested during an emergency exercise.

The evacuation time can then be compared to a target time for evacuation.

3.4 Method description – stress-testing

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 prescribed limits. The FL-t curve(s) obtained in the FL assessment are compared with the stress-test criteria and limits 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\text{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 21 (similar to the situation illustrated in Figure 17).
Time ("horizontal loss")

When subjected to a threat/event, an 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. 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 occurs until 90% of the functionality is restored, or some combination of various criteria. This is illustrated in Figure 22.
**Cumulative loss of functionality (area)**

As explained in Section 3.2.2, loss of functionality is the functionality of the SCI that is lost in a given threat situation. In Figure 23, 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 23.

![Figure 23: Loss of functionality surface as stress-test limit](image)

The example of a stress-test in Figure 24 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 21 (not to time or surface/area).

![Figure 24: 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 recover 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 24 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 22)
or if the surface for "loss of functionality" is used (as shown in Figure 23), then it is also necessary to assign/log the values for the time points \( t_0, t_1, t_2, t_3, t_4, t_5 \) in addition to the corresponding FL values.

### 3.5 Conclusion

The main purpose of the functionality level assessment is to provide understanding of how a disruptive event affects the critical functionality of an infrastructure. This is obtained by modelling the FL-t curve, including the absorb and recover capacity, and the curve can be characterized by the macro-indicators: robustness, disruption time, absorption time, downtime, recovery time, recovery rate, improvement/adaptation/ transformation, and loss of functionality.

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 case, following 10 main steps.

The results can be used for purposes including:

1. Improving resilience, including the absorb and recover capacity
2. Benchmarking (comparing with others)
3. Stress-testing

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 contribute to resilience assessment by analysis of loss of functionality.

### 3.6 Application example

An example is provided using the ECHO case. For some steps, the description refers to how the steps are performed using the SmartResilience tool. More information about how to support the functionality level assessment using the SmartResilience tool is presented in Chapter 6.

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

The Southern Industrial Zone in city of Pančevo, Serbia, 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 SCI or SCIs.

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

This example focuses 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, that 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 [55].

A Dynamic Checklist (DCL) is setup in the SmartResilience tool for the selected SCI(s) and threat(s), as well as providing basic information on the scenario (e.g. scenario name, description, DCL name, type of SCI, threats, and DCL description).

#### 3.6.1.3 Step 3: Identify interdependencies between the selected SCIs

In this case/scenario, other SCIs’ effects on the oil refinery are not relevant for consideration.

#### 3.6.1.4 Step 4 and 5: Define functionality elements (FEs) and indicators (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, one of the functionality elements (FEs) is production performance (FE1), and FIs are defined to measure this. FE1 and sample FIs (FI1.1 and FI1.3) are listed below in Table 15.

Table 15: Sample FEs and FIs in the ECHO case [48]

<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 (FE1)</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</td>
<td>Source: GRI G4 (2013)</td>
</tr>
<tr>
<td>Indicator</td>
<td>Domestic gas production (FI1.1)</td>
<td>Level of the production measured in million m³/day</td>
<td>Source: GRI G4 (2013) Predefined values: &lt;High&gt;: x ≥ 80; &lt;Medium&gt;: 80 &gt; x ≥ 70; &lt;Average&gt;: 70 &gt; x ≥ 50; &lt;Low&gt;: 50 &gt; x ≥ 30; &lt;Very low&gt;: x ≤ 30 [million m³/day]</td>
</tr>
<tr>
<td>Indicator</td>
<td>Overall Equipment Effectiveness (OEE) (FI1.3)</td>
<td>This indicator is used as an operational measure to monitor production performance</td>
<td>Source: Anderson, C., Bellgran, M. (2015) OEE = (TotalAvailableTime- (PlannedDowntime+Breakdown+Setup+Adjustments+Idling+MinorStoppages+ReducedSpeed+QualityLosses)) / (TotalAvailableTime-PlannedDowntime)*100</td>
</tr>
</tbody>
</table>

The complete list of FEs and FIs that are assigned to the case’s DCL are shown in Figure 25.
3.6.1.5 **Step 6: Assign maximum, minimum, and target values to all FIs (optionally assign weights)**

In this case, the user assigned indicator values directly as percentages, i.e. there was no transformation of non-percentage values using maximum, minimum, and target/best values. In addition, default equal weights were used.

3.6.1.6 **Step 7: Assign time values for the scenario**

Based on the scenario, the case’s time points are defined as follows (and assigned values are shown in Figure 26):

- **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
- **t4**: time at which the refinery reaches the initial functionality level or starting point of a new steady state level
- **t5**: time at which the refinery increases its functionality through learning and adapting, or at which the scenario ends

![Figure 26: ECHO case time series for BLEVE scenario](image)

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

Values are assigned for the FIs at each point in time. The FL at **t0** is considered as a normal functionality level, and the FL levels for the other points in time are defined relative to **t0**. Figure 27 shows the top part of the DCL where the values are entered (as percentages).

![Figure 27: Assigned FI values in the ECHO case](image)
3.6.1.8 Step 9: Generate and evaluate the FL-t curve that models the impact of disruption through macro-indicators

The results for the assessment are presented both as a plotted functionality over time (FL-t) curve and as a table showing all values and calculations. This is illustrated in Figure 28.

![FL-t curve and results table for the ECHO case](image-url)
If calendar time or relative time are provided and used, then calculations of the macro-indicators are presented as results, in addition to the FL-t curve and the results table. This is shown in Figure 29.

![Figure 29: Calculated values of the macro-indicators for the ECHO case](image)

As an example, the robustness is calculated as: \( \frac{FL_{t2}}{FL_{t0}} \cdot 100\% = \frac{46.92}{92.31} \cdot 100\% = 50.8\% \approx 51\% \).

(The values for \( FL_{t0} \) and \( FL_{t2} \) are found in the table in Figure 28. Also note that the "t" in the unit column means hours).

### 3.6.1.9 Step 10: Use the result of the functionality level assessment

The results can be used for purposes including:

1. Improving resilience, including the absorb and recover capacity
2. Benchmarking (comparing with others)
3. Stress-testing

This was discussed in Section 3.3.1.10. The main aim of this particular case was to obtain the results described in Step 9. The results were not used for improvement, benchmarking, or stress-testing in this case.

As an example, recovery time could have been used for stress-testing with a stress-test limit of 14 days (equal to 336 hours). The calculations show that the recovery time in this scenario was 264 hours, i.e. below the limit, thus passing the stress-test.

**Advice – consider splitting the FEs/FIs in several curves**

It may be beneficial to split the FL-t curve (in Figure 28) into several curves, either for each FE or even each FI, especially for stress-testing purposes. The single curves will then reflect a certain property for which it is easier/possible to establish thresholds/stress-test limits.
4 Resilience monitoring and optimization

4.1 Introduction and purpose
Resilience monitoring is about capturing changes in resilience over time, and resilience optimization is about choosing optimal solutions or measures to improve resilience. Both use the results from the resilience level assessment, described in Chapter 2, as a baseline.

The resilience level assessment provides an overall trend in resilience level for a critical infrastructure when the resilience level is assessed regularly/repeatedly. In addition to the overall trend, resilience monitoring provides detailed information of the changes in resilience over time.

If the resilience level assessment reveals weaknesses, implementation of improvement measures may be considered. Which improvement measure(s) will be the optimal to choose? Given a set of alternatives/options, various criteria need to be weighed against each other to obtain an overall ranking. The criteria could typically include the effect on resilience (e.g. change in RIL), and costs and time to implement the measure(s), but other criteria may also be relevant. The methods used in SmartResilience to decide on optimal improvement measures considering multiple criteria are Multi Criteria Decision Making (MCDM) methods.

The purpose of resilience monitoring is to track the progress of resilience over time to confirm continuous resilience improvement or reveal weaknesses. The purpose of resilience optimization is to decide on optimal measures to improve the resilience of SCIs. The reason for choosing MCDM for resilience optimization is that MCDM methods are preferred over other alternative decision-making frameworks because MCDM methods have “the potential capacity of improving the transparency, analytic rigor, auditability and conflict resolution of decision-makers.” [28]

4.2 Method description – resilience monitoring
Resilience monitoring in SmartResilience is largely related to repeated assessments of the resilience level, as described in Chapter 2. It can also be related to changes in macro-indicators as reflected in Figure 19, based on functionality level assessments (described in Chapter 3).

In SmartResilience, an interactive visualization methodology has been developed using TreeMap diagrams (D3.5 [50]), which provide detailed information of the resilience status at a given point in time, i.e. the underlying information for each of the red circles in Figure 12 (in Chapter 2) is visualized for all levels in the resilience level assessment method (threats, phases, issues and indicators) in one picture.

The changes in resilience between each point in time, e.g. an increase from average (yellow) at T4 to good (light green) at T5, can be monitored for all the levels (threats, phases, issues and indicators) interactively by use of a slider next to the TreeMap diagram.

Monitoring is implemented in the SmartResilience tool and described in Chapter 6 (Section 6.2.2.4).

4.3 Method description – resilience optimization (MCDM)
A step-by-step MCDM methodology is proposed in SmartResilience consisting of the following steps:

- Step 1. Define the resilience-related decision problem
- Step 2. Define optimization alternatives
Step 3. Define decision criteria
Step 4. Set criteria weights
Step 5. Set up analysis, provide input data, and perform the calculations
Step 6. Choose the best alternative amongst the options

The method steps are briefly described below, and an example using the SmartResilience tool is provided in Chapter 6 using the HOTEL case. Details about the method can be found in D3.4 [49], including an example using the ECHO case.

4.3.1.1 Step 1: Define the resilience-related decision problem

This is related to the use of the results of the resilience level assessment (see Chapter 2), where the following questions were raised:

- What is the single most optimal improvement measure?
- What are the ten most optimal improvement measures?
- What is the optimal set of improvement measures (among different sets)?
- What are the most optimal improvement measures within each phase?
- Given a certain budget for resilience improvement, what is the most optimal use of the budget?
- How much will it cost to improve the overall RIL from B to A?

The first five questions are all optimization problems. Here, we will focus on the third question/decision problem, where a set of improvement measures (consisting of one or more single improvement measures) is compared with other sets. This means that we aim at choosing the optimal set of improvement measures among a number of sets (two or more). These sets, the alternatives, are defined up front, and are not necessarily optimal. Thus, we may not obtain the overall optimal set of improvement measures; only the optimal one of those sets being considered.

This step includes providing required analysis information in the SmartResilience tool, such as name, description, when it was created, and by whom.

4.3.1.2 Step 2: Define optimization alternatives

This is the sets of optimization alternatives, consisting of one or more single improvement measures each. Examples of three Optimization Alternatives (OpAs) are presented in Table 16.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1  | OpA 1| OpA 1 consists of the following solutions:  
- Increase Big Data Analyst availability (increase indicator value from 2 to 5)  
- Increase the frequency of simulator training for operating personnel (increase indicator value from 1 to 5)  
- Operational agreement with entities (other than emergency responders) for support in the phase of facility functionality restoration (increase indicator value from 2 to 4) |
| 2  | OpA 2| OpA 2 consists of the following solutions:  
- Online analysis of the end-product (increase indicator value from 2 to 5)  
- Increase frequency of the maintenance of the equipment (increase indicator value from 2 to 5)  
- Operational agreement with entities (other than emergency responders) for support in the phase of facility functionality restoration (increase indicator value from 2 to 5) |
| 3  | OpA 3| OpA 3 consists of the following solutions:  
- Increase Big Data Analyst availability (increase indicator value from 2 to 4)  
- Increase review of resilience-related standard operating procedures (increase indicator value from 3 to 5)  
- Allocate extra budget for damage repair after the event (increase indicator value from 2 to 5)  
- Increase the frequency of simulator training for operating personnel (increase indicator value from 1 to 5) |
As seen from the table, three of the single improvement measures are proposed in two of the three alternatives.

In addition, "alternative groups" are defined in this step. This means that the optimization need not include all alternatives. "All" alternatives are the default choice, but another group could be only OpA 1 and OpA 2. Thus, separate MCDM analyses may be performed for each alternative group.

### 4.3.1.3 Step 3: Define decision criteria

Decision criteria are the factors that the decision-maker wants to include in the optimization process: these are the factors that will influence the decision. Criteria may be categorized into two main groups: costs and benefits. While costs are considered features for minimization, with the smaller the better, benefits are considered features for maximization, so the larger the better. Examples are presented in Table 17.

Table 17: Examples of (multiple) criteria for decision-making for optimizing resilience of SCIs

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
<th>Higher Ranking when closer to</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cost</td>
<td>The monetary cost of implementing a particular OpA</td>
<td>Minimum</td>
</tr>
<tr>
<td>2</td>
<td>Time</td>
<td>The time to implement a particular OpA</td>
<td>Minimum</td>
</tr>
<tr>
<td>3</td>
<td>ΔRL</td>
<td>Improvement in Resilience Level</td>
<td>Maximum</td>
</tr>
<tr>
<td>4</td>
<td>PR</td>
<td>The cost to public relations due to implementation</td>
<td>Minimum</td>
</tr>
</tbody>
</table>

The criteria can be quantitative or qualitative, and they can be of various types: crisp, linguistic-crisp, linguistic-fuzzy, fuzzy, or distributions.

**Crisp** criteria are strictly quantitative, i.e. require meaningful numerical inputs (e.g. cost). **Linguistic-crisp** are similar to crisp, but values are grouped into ranges which are then assigned a meaningful linguistic term. For example: 0 None or negligible, 1-20 Very low, 21-40 Low, 41-60 Medium, 61-80 High, 81-100 Extreme.

In the **Linguistic-fuzzy** criteria type, rules are applied. A rule is written as *If* situation, *Then* conclusion, and each fuzzy set corresponds to a linguistic concept, e.g. Very low, Low, Average, High, Very High. Linguistic-fuzzy is quite a good alternative to linguistic crisp, since the end-user can say something such as "I think it is something between 1 and 2, but it might also extend to 0.5 and 2.5." **Fuzzy** criteria are similar to linguistic fuzzy, but end-users must manually input the individual values as numbers corresponding to every statement.

**Distribution** criteria use probability through distributions such as normal, exponential, log normal, t-Student, etc. Distribution criteria can be used only if the end-user knows the individual distribution of a single criterion for each alternative. This can be very useful for cases when the end-users need to do a simulation, e.g. running a Monte-Carlo sampling in the background while the end-user conducts the ranking.

For each decision criterion, the value ranges (minimum and maximum) must be defined.

For decision criteria (as for alternatives), groups – "criteria groups" – may be defined. "All" is the default choice, but other groups may be defined, facilitating different analyses. The most common criteria used in SmartResilience are the three first in Table 17; thus, a criteria group called "common" could be defined for these three criteria.

### 4.3.1.4 Step 4: Set criteria weights

The different decision criteria, e.g. the four in Table 17, are by default given equal weights (i.e. 0.25 in this case). However, non-equal weights may also be assigned, e.g. 0.3, 0.1, 0.4 and 0.2, to the criteria in Table 17. This second set of weights is then a separate weight group, making it possible to choose different sets of weights in different analyses (as was the case for decision alternatives and decision criteria as well).

A similar approach for determining non-equal weights as described in Chapter 2 may be used. Another alternative is to use the analytic hierarchy process (AHP) [40], for those familiar with this method.

### 4.3.1.5 Step 5: Set up analysis, provide input data, and perform the calculations

Setting up the analysis includes defining the analysis (name, description, etc.) and selecting the combinations of groups (optimization alternative group, decision criteria group and decision weight group) to be used.
Input data must be provided, with values within the ranges defined in Step 3. This is perhaps the most challenging part of the optimization analysis, especially defining the change in resilience. Usually, an already performed resilience level assessment is used as a baseline, and then new RIL assessments are performed for each optimization alternative to obtain the difference. This may seem straightforward, but the challenge lies in determining which issues and indicators are affected by a given improvement measure and how much they are affected.

Alternatively, some other measures of resilience may be applied, e.g. the macro-indicators described in Chapter 3, followed by assessing the change in the value of one or more macro-indicators (e.g. robustness). Once the input data are provided, the calculations can be performed to provide the ranking of all the optimization alternatives. For most users, this will be carried out in the SmartResilience tool by selecting "Ranking results" in the menu. Details of the mathematics behind this can be found in D3.4 [49].

4.3.1.6 Step 6: Choose the best alternative amongst the options
The rational choice is to select the alternative with the highest ranking. This represents the optimal decision.

4.4 Conclusion
The purpose of resilience monitoring is to track the progress of resilience over time to confirm continuous resilience improvement or reveal weaknesses. This is achieved, for example, using TreeMap diagrams.

The purpose of resilience optimization is to decide on optimal measures to improve the resilience of SCIs. A step-by-step MCDM methodology has been proposed to reach such an optimal decision, i.e. to choose the optimal alternative (highest ranking) based on selected decision criteria. The methodology is implemented in the SmartResilience tool and for most users will be a prerequisite for performing the analysis.

4.5 Application example
Resilience monitoring by TreeMap diagrams is illustrated in Chapter 6.

An application example for resilience optimization using the ECHO case is provided in D3.4 [49]. However, this is very similar to the example presented in Chapter 6, since both are based on using the SmartResilience tool. Thus, we refer to the example described in Chapter 6 (using the HOTEL case).
5  Dependency analyses – interdependencies and cascading effects

5.1  Introduction and purpose

Critical infrastructure systems do not operate isolated from each other; they are highly interconnected. For instance, telecommunication systems require a supply of energy to operate. These interconnections can go in one direction or be mutual. For example, energy systems, in turn, require a functioning telecommunication infrastructure to be operated efficiently. It follows that many infrastructure properties, including resilience, their efficiency, operational state, etc., are not only a function of the state of the given infrastructure itself, but also of all other critical infrastructure systems where interdependencies exist. A direct consequence of this is that a shock or adverse event that impacts one critical infrastructure can result in cascading failures and ripple effects at various scales that can impact larger systems.

The basis of the SmartResilience methodology to assess resilience is shown in Figure 3 (in Chapter 2). Another way of illustrating this is shown in Figure 30. Here the "area" or "city" (level 1) is viewed as "infrastructure of CIs."

![Figure 30: Assessing interdependencies of critical infrastructures in SmartResilience](image)

The first step is to define a scenario (given by a specific infrastructure and a threat, e.g., hospital and flooding) that is to be considered within five different time phases (understand risks, anticipate/prepare, absorb/witherstand, respond/recover, adapt/transform). Within these phases, one considers different issues (e.g., capacity at the hospital, and accessibility of the hospital) which in turn are measured using indicators (e.g., number of available beds in the emergency ward at the hospital, and number of roads accessing the hospital). Within this framework, interdependencies enter on two different levels: as issues and as scenarios.
First, interdependencies are issues to be dealt with in the assessment by means of indicators (e.g., in the example given above there is a dependence for the hospital on the transportation infrastructure that determines its accessibility, which could be measured with specific indicators). This is illustrated with the arrows down to the right in Figure 30 and is described in Section 5.2.

The second way (and substantially more resource-intensive one) to address interdependence in the SmartResilience methodology is to define a scenario in which a threat targets not one but several infrastructures—infrastructures-of-infrastructure (e.g., a joint assessment of the transportation and health infrastructure in the case of a specific threat). In this case, one would need to address not only issues related to the individual infrastructures, but also those that relate to cascading (or indirect) effects that arise due to their interdependencies. This is illustrated with the arrow up to the left in Figure 30 and described in Section 5.3. More information on both the issue approach (empirical approach) and the infrastructures-of-infrastructure approach (agent-based approach), and other approaches, can be found in D2.3 [45].

In addition to these two approaches, cascading effects can also be treated as threats for each single SCI, as described in Chapter 2. E.g. an explosion at a refinery may cause a toxic cloud threatening a nearby airport. In this case the airport can decide to include a toxic cloud as a threat in their resilience assessment (not only focusing on the economic cascading effects). Such cascading and ripple effects between SCIs can also be analyzed through a tabletop exercise as described in Section 5.5.

5.2 Method description – interdependency identification

The presence of (inter-)dependencies in critical infrastructures can be dealt with as issues in their resilience assessment, meaning that corresponding indicators should be formulated or identified. Here we will show how an existing methodology, the CascEff approach from the EU CascEff project, can be used to identify whether a given type of dependence between infrastructures should be considered as an issue or not.

The purpose of the CascEff project was to generate knowledge about cascading effects that can be used to inform decisions that are made in the response phase of an emergency based on existing empirical data (written accounts) of past events [31].

The method was adopted from [38]. As shown in Figure 31, the model involves a sequence triggered by an initiating event that affects one or several originating systems, from which there is an impact on dependent systems, taking into account the characteristics of the systems, conditions of the systems and impacts on the dependent systems and overall system [31]. By considering these elements, the conceptual model accounts for the past events to gain deeper insights of cascading effects which can be useful for decision making and support modelling and simulation efforts in the area of critical infrastructure. Also, this analysis can be used for predicting present and future crisis evolution [31].
The potential past events were selected to study the aim of obtaining a wide variety of cascading effects by considering the following characteristics: a) Types of initiating events, b) Spatial extent of Initiating Event, c) Spatial extent of cascading effects, d) Geographical location, e) Duration, f) Impacted systems and g) Dependency types involved [31].

To analyze these, selected documents covering the aspects such as well-elaborated events, cascading effect and social consequences are used. The analysis yields a variety of information about the events, including the number of infrastructures dependent on the other infrastructures as shown in Figure 32; see also [31]. A circle in a given row (originating system) and column (depending system) indicates that a corresponding interdependence has been identified for a particular initiating event. The size of the circle indicates the order of the event (the larger the circle, the more direct the impact, whereas smaller circles indicate less-relevant interdependencies).

![Figure 32: Dependencies and interdependencies between infrastructures [27]](image)

One of the focuses of the SmartResilience project is in the assessment of the resilience of the system in the presence of interdependencies and cascading effects. In this context, the analysis done using the CascEff method could serve as a basis for identifying potential issues between different types of infrastructures. That is, a circle between two different infrastructures in Figure 32 indicates that an issue has been reported that potentially involved a dependence of the column-infrastructure on the row-infrastructure.

Thus, each SCI operator can use Figure 32 directly for the identification of which other SCIs they depend on (at least as a starting-point) and include these as issues in the resilience assessment. For a more in-depth study, the CascEff documents and/or the CascEff approach could be consulted. Once identified, knowledge of such dependency issues serves as a starting point to identify suitable indicators.
As seen from Figure 32, most infrastructures are dependent on power supply, so what is important for these dependent infrastructures to be resilient given this dependency, i.e. what is the issue? One issue could be to have redundancy of power supply and another would be back-up systems, e.g. having your own diesel generators and/or battery banks. Indicators, i.e. how you measure the issues, could then be e.g. number of independent power supply systems, or duration of back-up systems.

5.3 Method description – cascading effects loss estimation

To assess the full impact of interdependencies and cascading (indirect) effects, it is necessary to consider “infrastructures-of-infrastructures.” In SmartResilience, we use an agent-based model, coupled with an environmental damage scenario generator. The model is calibrated using extensive datasets on a one-to-one scale, i.e., each natural person or legal entity is represented by an agent. As a particular use case we consider infrastructures in flooding events of different sizes. We show how this model (and its slimmed-down version) can be used to define indicators that can be generically used in the resilience assessment of other infrastructures, without the need to implement the model as such.

Agent-based models (ABMs) originated in the 1980s as computational tools to study certain types of phenomena on a conceptual level [6]. They were particularly useful in cases where one is interested in phenomena that result from multiple types of interactions between very heterogeneous actors. For this reason, ABMs have soon been used as one of the standard tools to quantitatively assess the impact of disasters or other adverse events on critical infrastructures and their interdependencies, usually involving some level of aggregation of the agents or of stripping away certain sets of actors [59],[4],[5],[32],[33]. Recent developments—the advent of big data and ever-increasing computational resources—have changed the capabilities of what ABMs can do dramatically. Using detailed large-scale datasets from business information, national accounts, census data, etc., it has now become possible to simulate millions of agents that represent each natural person or legal entity in an entire national economy in a way that the properties of the agents are calibrated to the data. It is further possible to move beyond the state-of-the-art by coupling such an ABM with catastrophe models to link environmental and economic processes.

The ABM was developed based on related previous efforts, in particular the ABM platform developed in the FP7-ICT project CRISIS served as point of departure. A schematic overview of the ABM is shown in Figure 33.

Figure 33: Schematic overview of the ABM [36]

The model depicts the economy of a small nation at a one-to-one scale and includes about 10 million agents. There are four institutional sectors, namely (i) non-financial corporations (firms), (ii) financial corporations...
banks), (iii) the government and (iv) households. This national economy interacts with the rest of the world through imports and exports. Each sector is populated by a number of heterogeneous agents representing natural persons or legal entities. The main interactions in the model can be summarized as follows. Firms pay dividends to their owners and wages (financed through income and loans from banks) to workers. Households consume goods produced by these firms. Households and firms deposit their money with banks that in turn grant loans to the firms. The government levies taxes and redistributes social contributions in order to provide social services to the citizens, next to consuming on the retail market.

The ABM provides estimates on a firm-level for several measures that can be used as the basis to formulate resilience indicators, including sectoral price indexes, supply, unit labor costs, unit material costs, unit capital costs, unit net taxes/subsidies, target unit operating surplus, consumer price index, productivity, desired investments (in capital stock and replacements), material stock of unit intermediate inputs, employments, labor vacancies, wages, financing gaps, as well as all net cash flow items.

Despite recent advances in computational power, the implementation of a sophisticated one-to-one scale simulation model coupled with a spatially fine-grained damage scenario generator is still resource-intensive in terms of computation time. To bypass potential limitations in applications of such simulation models, we propose to use a slimmed-down version of the ABM that produces lookup tables of indicators that can be conveniently loaded into the SCI dashboard of the SmartResilience tool. In brief, the slimmed-down model uses the well-established concept of representative agents.

The slimmed-down ABM is a model akin to so-called inoperability input output (IIO) models. This type of analysis has been developed by Wassily Leontief [30] and is currently the standard method to address economic interdependencies. IIO models attempt to predict the resulting economic losses and inoperability suffered by a company that result from a disruption in a different company (or set of companies) in the same or different sectors. IIO models address all kinds of threats that physically damage infrastructure, e.g., loss due to flooding, other forms of extreme weather, shutdowns due to cyber-attacks (for instance, the recent WannaCry attack that triggered substantial disruptions in the UK health sector). The main contagion channel by which this initial event affects other infrastructures is due to the supply and use of intermediate goods and the exchange of services.

The output of the models described here is linked to the overall SmartResilience framework by providing indicators. That is, the observable model parameters are directly related to one or several economic resilience indicators. To "load" these indicators with values that have been generated, for instance, by the ABM described here, the SCI Dashboard provides a data upload service, which is briefly described in Chapter 6 and in detail in D4.2 [54]. The entry in the SCI Dashboard is shown in Figure 34.

In fact, the web-based data analytics background service applies for any big data indicators, not only those related to dependencies. The general workflow is shown in Figure 35 (from D4.2 [54]).
The first step for the user is to login to the SmartResilience member-only area and go to the SCI dashboard. Then the scenario needs to be designed and the DCL needs to be created. Therefore, the user selects the SCI, threat, phase, issues, indicators, and assigns values to the indicators whenever this input is available. To utilize the data analytics background service, the next step is to select those indicators in which the value should be derived from the ABM approach, or the network analysis approaches, which are all included as existing indicators. This leads to the next step, where the corresponding templates can be downloaded (Excel templates that contain instructions on the expected data format). Once the user has inserted his or her data into this template, it can be uploaded again, and the analysis is run with the click of a button. This provides access to libraries (DLL files) that execute the computations. These DLL files can, for instance, consist of deployed Matlab solutions that expose certain functions that compute the indicators based on the input data, i.e., functions that extract the relevant networks and compute performance measures. For the user, these computations take place entirely in the background. The output that the user receives are assessments (of functionality or resilience) based on big data and/or conventional indicators.

5.4 Conclusion

Two ways of analyzing interdependencies in the SmartResilience framework have been presented in this chapter. The first approach describes interdependencies within an assessment on the level of issues or indicators. Therefore, one proceeds in the following steps.

1. For a specific scenario (infrastructure and threat) in a given phase, identify issues that may arise because of a dependence of the assessed infrastructure on another one using an approach of your choice, such as the matrix in Figure 32 or the CascEff approach itself, described in Section 5.2.
2. Identify **indicators** related to this **issue**. Often the type of dependence identified in step 1 suggests which indicators might be appropriate. Otherwise, sources of indicators described in Chapter 2 may be used.

3. Include the resulting indicators in the DCL for the considered scenario and perform the resilience assessment, i.e. follow the method description in Chapter 2.

Going beyond the interdependencies-as-issues/indicators approach outlined above, it was presented in Section 5.3 how to assess interdependencies on the level of “infrastructures-of-infrastructures”—a far more ambitious approach. On this level, the scenario is not defined by one but by several infrastructures that are affected by the same incident that may or may not cause cascading effects. We provided an in-depth description of how an analysis of interdependencies can be made on such a level using an ABM that was coupled with an environmental damage scenario generator. The ABM models a national economy on a scale of one-to-one (each natural person, household, firm, bank, etc., is represented as an agent in the model) and can be calibrated using extensive datasets from national accounts, business demographics, and statistical offices. We showed how this ABM allows one to assess indirect and cascading effects of flooding events in the presence of physical, geographic, regulatory, and economic interdependencies. The results of the model can be uploaded into specific indicators using a web service provided by the SCI dashboard, therefore providing full integration with such complex modelling efforts with the overall SmartResilience framework.

### 5.5 Application example

Interdependency identification, based on the results from the CascEff project, is exemplified at the end of Section 5.2. It should be noted that missing interdependencies in the matrix in Figure 32 does not mean that there are no interdependencies between these infrastructures; it simply means that such interdependencies were not documented in the cascading events analyzed in the CascEff project.

Cascading effects loss estimation results are rather advanced, and the description of these results are found in D2.3 [45]. The uploading of economic resilience indicators based on the ABM model, and other big data indicators, are described in Section 6.2.4.

Finally, a somewhat different approach to the analysis of cascading effects, applied in the SmartResilience project, is a tabletop exercise of a cascading scenario involving several SCIs. This case study, combining all the SCIs in the project, was labelled INDIA in the SmartResilience project. Although interdependencies and cascading effects are foreseen at the onset of the exercise, more detailed information about interdependencies can be revealed during such a tabletop exercise. More information about this tabletop exercise can be found in D5.11 [57].
6 Integrated tool

6.1 Introduction and purpose
The SmartResilience integrated tool supports the main methodologies of the project, but it also consists of many additional features. It is not the aim of this guideline to cover all features or the advanced use of the tool. Rather, this description of the tool is limited to inform the user of the main methodologies regarding how to use the tool to perform the assessments. For extended description of the tool, we refer to D3.7 [51].

Using the tool will, in some cases for some parts of the methodologies, make the assessments more efficient; in some cases, the background calculations are so complex that using the tool is practically a prerequisite.

The tool description provided here is based on the current version of the tool (October 2018). As the tool is still under development, both content and layout may change.

6.2 Tool description
The tool is accessed through http://www.smartresilience2.eu-vri.eu/RunningApp/RIdb/SCIDashboard.aspx and requires login with username and password. This opens the main menu at the left side of the screen as shown in Figure 36. It also shows the SCI Dashboard overview on the right side (not shown in Figure 36).

As already mentioned, we will not cover all features of the tool. The only tabs in the main menu we will describe are tabs 4, 5 and 6, i.e. "Manage & Setup," "Assessment and monitoring" and "Resilience optimization." These are the tabs required when using the main methodologies.

The arrow signs to the right on each tab indicate sub-menus.
The links between the methodologies and the relevant parts of the tool are shown in Figure 37 (red arrows).

In Figure 37, the relevant sub-menus are opened for "Assessment and monitoring" down to the left and "Manage & Setup" down to the right.

Red solid arrows show where to perform the assessments in the tool, whereas yellow boxes show where to perform necessary setups for the assessments. Red dotted arrows indicate outputs of assessments (issues from interdependency identification and indicators from cascading effect loss estimation) that provide input for other assessments (resilience level assessment and functionality level assessment).

### 6.2.1 Manage & Setup

The "core twins" of the methodologies are issues (or elements) and indicators, i.e. what is important for resilience and how to measure it. Selected issues and corresponding indicators are included in a checklist (structured according to the five phases), termed a dynamic checklist (DCL) since it can be dynamically adjusted to each user, i.e. each user can select the most relevant issues and indicators for her/him.

However, before creating the DCL, which is the basis for the assessments, the use case/case study and scenarios must be described. Each use case (e.g. a city/area or a specific critical infrastructure) may consider different scenarios (e.g. the specific critical infrastructure and a specific threat, such as cyber-attack). A DCL is made for each scenario and all scenarios are linked to the use case/case study in question.
6.2.1.1 Case Studies
In the Case Studies screen, you click on "Add New Case Study" on the top of the page and provide a case study name and a description. Examples of existing case studies are shown in Figure 38 (menu not shown).

![Figure 38: Providing case study name and description](image)

6.2.1.2 Scenarios
In the Scenarios screen, you click on "Add New Scenario" on the top of the page and provide information on:

- Scenario Name
- Scenario Description
- Case Study (select from drop-down menu)
- Type of CI(s)
- Other CI(s) possibly affected
- Type of Threat(s)
- MCDM Analysis
- Attachments
- Linked DCLs
- Threat(s) tackled in linked DCLs

Examples of existing scenarios are shown in the scenario overview screen in Figure 39 (menu not shown).

![Figure 39: Adding a new scenario and examples of existing scenarios](image)

6.2.1.3 Dynamic Checklists
Now the user can start creating the DCL, for which there are several options. However, first the user must decide on the type of assessment: resilience level or functionality level assessment.

The user can, for either of the two types of assessments:
1. Select/copy an existing DCL and use this as it is
2. Select/copy an existing DCL and adjust it by removing and/or adding issues and indicators from the database and/or by defining new issues and/or indicators

page 70
3. Create a new DCL with issues and indicators from the database
4. Create a new DCL with issues and indicators both from the database and defining new issues and/or indicators

In case there is a need for defining new issues or indicators, the items in the lower yellow box of the "Manage & Setup" tab in Figure 37 are used. We will come back to how this is done in the next section.

Selection/copying of an existing DCL or creation of a new DCL is made from the Dynamic Checklists screen as shown in Figure 40 (menu not shown).

Selection/copying of an existing DCL or creation of a new DCL is made from the Dynamic Checklists screen as shown in Figure 40 (menu not shown).

In case there is a need for defining new issues or indicators, the items in the lower yellow box of the "Manage & Setup" tab in Figure 37 are used. We will come back to how this is done in the next section.

A list of existing DCLs can be chosen from All DCLs, Core DCLs, Recommended DCLs, Completed DCLs, or User’s DCLs, and they can be filtered to selected case studies. In Figure 40, the selected case study is the ECHO case study in the SmartResilience project, for which there are 12 DCLs. These DCLs have been sorted according to their ID number, and the first three are shown in the figure.

A refinery (same type of critical infrastructure) may choose to use one of the DCLs as used in the ECHO case by copying the chosen DCL (third column from the right). The copied DCL can be used as it is (option 1 above), or it can be modified/edited (option 2). Creating a new DCL (options 3 and 4) is started by clicking on either "Add New Resilience Index Level" or "Add New Functionality Level."

Figure 40: Selecting an existing or creating a new DCL

Whether an existing DCL is copied or a new one is being created, the user enters the "Dynamic Checklist – Setup" screen consisting of four steps, as shown in Figure 41. (Only the top of the screen is shown; the lower part depends on the step chosen). These steps are described below.

![Dynamic Checklist - Setup](image)

**Figure 41: DCL setup**

**Step 1: Basic Information**

The basic information includes:

- Scenario (select from drop-down menu)
- Scenario Description and Other CI(s) possibly affected
- DCL Name
- Created on
- Type of CI(s)/Threat(s)
- DCL Description
- Type of assessment
Step 2: Issues

Step 2 is accessed by clicking on the “Step 2: Issues” arrow (or the "Next" button). The top part of the screen is shown in Figure 42.

The right part of the screen shows the selected issues structured according to the five phases. The left part is used for search and selection, and issues to be included are dragged (by pressing the six dots to the left) and dropped into the correct phase on the right side (directly on the phase name). More information about an issue is obtained by clicking on the information symbol to the left of the ID number. Issues are removed by marking the issue (in the right pane) and pressing the “Delete selection” button at the bottom of the screen (not shown in Figure 42).

Step 3: Indicators

Step 3 is accessed by clicking on the "Step 3: Indicators" arrow (or the "Next" button). The top part of the screen is shown in Figure 43.

The indicator screen is very similar to the issue screen. The right part of the screen shows the selected indicators for each issue structured according to the five phases. The left part is used for search and selection, and indicators to be included are dragged (by pressing the six dots to the left) and dropped into the correct issue on the right side (directly on the issue name). More information about an indicator is obtained by clicking on the information symbol to the left of the ID number. Indicators are removed by marking the indicator (in the right pane) and pressing the "Delete selection" button at the bottom of the screen (not shown in Figure 43).
Step 4: Preview

By clicking on the "Step 4: Preview" arrow (or the "Next" button), a total overview of the DCL is shown, i.e. the selected issues with corresponding selected indicators structured according to the five phases. The top part of the screen is shown in Figure 44. A DCL for resilience level assessment, as is shown here, should typically consist of several (5-8) issues per phase, and one or more indicator for each issue.

Figure 43: Indicators in DCL

Figure 44: Preview of the complete DCL
The names are listed to the left with corresponding descriptions to the right. The DCL can be exported to Excel and/or Word using the buttons up to the right. Examples are provided in Annex 2.

The DCL is now ready for use in the various assessments.

6.2.1.4 Elements, Indicators & Issues

Before proceeding to the assessments, let us see how to include elements, issues, and/or indicators that are not already part of the SmartResilience database. New elements, issues, or indicators must be defined and entered into the database before they can be included in a DCL.

First, it must be checked if identical or similar elements/issues/indicators are already in the database. This is done in the entry page when selecting the "Elements, Indicators & Issues" item in the menu. A search term, e.g. "emergency," may be entered with filtering based on type (issue, elements or indicator), CI(s), Threat(s), Phase(s), and Other (provider, rating and approved). The search page is shown in Figure 45, without the left menu pane.

An example of a search is shown in Figure 46. Here, the search term "emergency" is used for the type "issue" for Industrial Production Systems, considering all threats, all phases and all providers as relevant. This search resulted in 26 records found (two of them shown in Figure 46). They apply to either Industrial Production Systems specifically or to any CI.

If a user wants to include an issue related to emergency planning or emergency preparedness, he or she can check the 26 records and see if any of these records match perfectly (and use this), match somewhat (and adjust this), or do not provide a good match at all (thus, implying the need to create a new issue).

This is carried out in the DCL, in Step 2 and Step 3 as described in Section 6.2.1.3 above, by clicking on the information symbol to the left of the ID number (see Figure 42 and Figure 43). In the top right corner in the new window that appears, the user can choose between "Save As" (if adjusting the existing issue or indicator), "Edit" (if adjusting your own issue or indicator), and "New" (if creating a new issue or indicator). The template shown in the window must be filled in with the required information and saved.
6.2.1.5 Approvals

When all required information is provided, you as the "owner" should verify this by approving the issue or indicator (via the "Approvals" item in the menu).

6.2.2 Assessment and monitoring

6.2.2.1 Resilience Level Assessment

The sub-menus for the resilience level assessment are shown in Figure 47.

"Create new DCL" is the same as was described in Section 6.2.1.3. It was then entered through "Add New Resilience Index Level" in the Dynamic Checklists menu (see Figure 40).

The sub-menu "Go to assessments" opens the window shown in Figure 48 (menu not shown).
DCLs with performed resilience level assessments

The basis for an assessment is the DCL. Each row in Figure 48 describes one specific DCL, including its ID number. The number in the first column (in brackets) shows how many assessments are carried out using the particular DCL, e.g., three assessments for the DCL with ID 12. To make a new assessment based on a specific DCL, click on the plus sign in the last column. This will provide a screen as shown in Figure 49.

Assessment - Resilience Level

Now the values of the indicators can be entered. In the method in Chapter 2, it is described how the real measurement values provide indicator scores based on predefined ranges of indicator values (worst and best values). Alternatively, the scores (0-5) can be provided directly.

In the tool, the ranges of indicator values can be assigned using minimum, maximum and target values; however, there is no calculation of the score based on the real indicator value in the tool. The user must calculate the corresponding score value, or assign the score directly, and enter it in the tool (in the last
column in Figure 49). The aggregated calculations of scores and resilience levels (RILs) on all the levels above the indicator level, i.e. issues, phases, threat, SCI and area, are performed by the tool.

Each issue can be assigned a corresponding dimension (a-e), although this is not affecting the aggregation calculations. It provides additional information about the issue/indicator coverage of the resilience matrix.

By expanding the rows of resilience level assessments (see Figure 48), information is provided on the status of each assessment for the given DCL. This is shown in Figure 50 for the first row in Figure 48 (DCL ID 12).

Figure 50: Status/completeness of resilience level assessments

All three assessments are almost complete (only missing the assignment of dimensions). The results of the first of the three assessments, i.e. the assessment with ID 12 (coincidentally the same ID number as the DCL), are obtained by clicking on the "Show Results" sign. Parts of the results are shown in Figure 51 (split in two parts).
The overall result is a score of 2.51, corresponding to a RIL=C (average). The lower part of Figure 51 shows the detailed results/scores and RILs (indicated with colors and labels) for the last phases.

There are various other ways of presenting the results in the tool, including comparison (through the "Comparison" sub-menu), but we will not provide further details about the assessment results in this guideline.

### 6.2.2.2 Functionality Level Assessment

The sub-menus for the resilience level assessment are shown in Figure 52.

"Create new DCL" is the same as was described in Section 6.2.1.3. In that section, this tab was entered through the "Add New Functionality Level" option in the Dynamic Checklists menu (see Figure 40). The sub-menu "Go to assessments" opens the window shown in Figure 53 (menu not shown).

As for the resilience level assessment, the basis for a functionality level assessment is the DCL. Each row in Figure 53 describes one specific DCL, including its ID number. The number in the first column (in brackets) shows how many assessments are carried out using the particular DCL, e.g. two assessments for the DCL with ID 109.
A DCL for functionality level assessment is quite different from a DCL for resilience level assessment. A DCL for resilience level assessment consists of issues and indicators that need to be distributed to all five phases of the resilience cycle and provide reasonable coverage in terms of the number of issues and indicators. A DCL for functionality level assessment consists of (functionality) elements and (functionality) indicators, and phases need not be considered explicitly. It can consist of one or very few elements and one or a few indicators per element.

Figure 54 shows an example for the DCL with ID 109 (accessed by clicking on the preview symbol in the second last column in Figure 53). It focuses on the critical functionality for the society (one element and two indicators). In addition, it is possible to include functionalities for the CI in terms of its own "business continuity."

To make a new assessment based on a specific DCL, click on the plus sign in the last column in Figure 53. This will provide a screen as shown in Figure 55.

Now the values of the indicators can be entered, i.e. the percentages at times $t_0$ to $t_5$, thus describing the critical functionality curve (resilience curve). Note that "Points," i.e. number of time points, is selected as 6, which is the default number. However, this can be increased.
Assessment - Functionality Level

By expanding the row of DCL ID 109 in Figure 53 in the same way as for resilience level assessment DCLs (see Figure 50), the user can click on "Show Results" and obtain the results as shown in Figure 56 and Figure 57.

Dynamic Checklist Assessment Results

Figure 56 shows the upper part of the results, providing the basic information of the assessment. Figure 57 shows the lower part of the results, i.e. the critical functionality curve and a table with the exact percentages used for the indicators. The curve is an average of the two indicators. Note that 9 points have been used in the time series (increased from 6 to 9).
In addition to "Equidistant time," "Calendar time" or "Relative time" can also be selected. However, this requires values on the time points. These can be entered by clicking on the "Setup Time Series" button (see Figure 55) and a pop-up window as shown in Figure 58 will appear. Here, "Real Time" and/or "Relative Time" may be entered.

By using real time or relative time, the distances between the time points will not be equal as is shown in Figure 57, where the absorb phase/time is seemingly equal to the respond time and the recovery time.

The last sub-menu under "Functionality level" is "Compare FLs in time". Here, different FL assessments can be compared by displaying them in the same FL-t diagram. Relative time should be used.
6.2.2.3 Stress-testing

The critical functionality curve, such as the one in Figure 57, provides the basis for stress-testing, if we assume that the threat considered is the "stress-test event." However, the curve or line that represents the threshold, which the critical functionality curve is compared against, is currently not implemented in the tool. For example, it could be a horizontal line in Figure 57 at 60%, in which case the stress-test is approved (always above 60%). The different forms of threshold are discussed in Chapter 3.

6.2.2.4 Monitoring

Monitoring is about capturing changes over time, either short-term or long-term. It is typically reflected by Figure 7 and Figure 12 in Chapter 2, showing the overall trend in resilience level for a particular critical infrastructure when the resilience level is assessed regularly/repeatedly.

In the tool, monitoring is illustrated a bit differently. When clicking on the "Monitoring" sub-menu under "Assessment and monitoring," the screen shown in Figure 59 appears.

![Monitoring entry screen in the tool](image)

This screen consists of three panes (and a forth below these panes for results). In the left pane, case studies, DCLs, and assessments are listed. By selecting/clicking on a case study, the assessments for that case study are listed in the middle pane, from where they can be dragged and dropped into the right pane. When assessments are dropped in the right pane, results are visualized in the result pane below these three panes (not shown in Figure 59).

An example of a selection of an assessment for visualization is shown in Figure 60.

![Selection of assessment for visualization of results – example (ID 12)](image)
First, the case study is selected in the first pane resulting in a listing of the nine assessments in the middle pane. Assessment ID 12 is then dragged from the middle pane and dropped to the right pane, providing the results shown in Figure 61 (legends and detailed information have been moved below the figure).

![Figure 61: Visualization of results of assessment ID 12](image)

When selecting only one assessment, the result shows detailed information of the status at a specific point in time, i.e. it does not show changes over time. If there have been repeated assessments over time, like the plots shown in Figure 12 (in Chapter 2), then a form of monitoring over time can be illustrated.
The visualization shown in Figure 61 is a TreeMap structured according to the six levels in the RIL method, as presented in Figure 3 (in Chapter 2). Compared to the trend line in Figure 12 (in Chapter 2), this provides much more detailed information, and it also provides more information than was illustrated in Figure 13 (in Chapter 2) using bar charts. Level 1 (area) covers the entire rectangle and is located farthest back in the picture. Since level 2 (CI) and level 3 (threat) are "all/any CIs" and "all/any threats," correspondingly, they also cover the entire rectangle, one on top of the other, and they have the same score and resilience level as the area (yellow, i.e. RIL=C). Phases (level 4) are divided in five different rectangles covering the entire area together. Issues (level 5) are also separated, and they consist of the indicators (level 6). The sizes of the rectangles indicate weights. The TreeMap visualization is explained in more detail in D3.5 [50].

The visualization is a kind of "heat map" showing where the resilience is poor (pink) or even critical (red). In this example, some indicators and even issues are red, i.e. critical, and one entire phase is poor (pink), which is Phase II: Anticipate/prepare. This phase is strongly in need of improvement.

More details are obtained by mouse over, indicated by the arrow and the magnifier glass in Figure 61. The detailed information is provided in the upper right corner (note that in Figure 61, we have moved this information and the legends below the figure for readability). In the example in Figure 61, the mouse was held over Phase I: Understanding risks, indicating that the score was 3.29 for this phase. This is more detailed information than the colors provide; a light green color only indicates a score between 3 and 4.

When two or more assessments are included in the right pane, the resulting visualization (TreeMap) has a slider on the right side, which is moved to see the changes in colors in the TreeMap.

6.2.3 Resilience optimization

If the resilience level assessment reveals weaknesses, either isolated or in comparison (benchmarking), or the functionality assessment and/or stress-testing show unacceptable loss of functionality, implementation of improvement measures will be required. Which improvement measure(s) will be optimal to choose? Given a set of alternatives/options, various criteria need to be weighed against each other. This could typically include the effect on resilience (e.g. change in RIL), costs, and time to implement the measure(s), but other criteria may also be relevant. The method used to decide on optimal improvement measures is a Multi Criteria Decision Making (MCDM) method.

The tool provides a means to rank the various alternatives/options by entering the necessary information in a series of steps. When clicking on "Resilience optimization" in the main menu (see Figure 36), the screen shown in Figure 62 appears with only two items in the menu (not shown): "Manage MCDM analysis" and "Analysis results". The screen gives an overview of the existing MCDM analyses - those that have already been performed. Clicking in the menu on "Manage MCDM analysis" provides the same entry screen as seen in Figure 62.
Opening "Analysis results" in the menu provides the results of a selected MCDM analysis, i.e. an analysis must be selected/marked first.

New MCDM analysis – Analysis information

If a new MCDM analysis shall be performed, click on the "Add New MCDM Analysis" at the top of the screen. This will provide the entry page shown in Figure 63. This figure uses one of the existing analyses (MCDM ID 15) as an example (in reality, the fields are of course empty when first opened). The menu to the left shows all the steps that must be performed as part of the MCDM analysis. We will go through each of the steps.

Figure 63: MCDM analysis – example (ID 15)

In order to make the screenshots larger and more readable, the left menu is excluded in the figures below (as was also done in the previous sections).

Alternative definition

Opening "Alternative definition" in the menu for the example analysis gives the screen as shown in Figure 64.

Figure 64: Overview of alternative improvement options defined

Here the different alternatives/options for improvement are described/defined, and new alternatives can be added using the "Add New Alternative" button. This provides a pop-up window as shown in Figure 65 (which shows the already filled out alternative OpA2 from the example case).
The results as visualized in Figure 61 could be used as inputs to define improvement measures/alternatives/options. This figure shows the "hot spots" where improvements are most needed. Figure 37 also indicates (with dotted arrows) that improvements may be discovered through FL assessment, stress-testing, and/or monitoring and that cascading effects ideally should be considered in MCDM analyses, as described in Chapter 3.

![Figure 65: Defining an alternative improvement option](image)

**Alternative group**

The default option is that all the alternatives for improvement are considered in the MCDM analysis, i.e. all are ranked. The selection of only some of the alternatives can be done by creating new alternative groups. This is obtained by clicking on the "Add New Alternative Group" button in the "Alternative group" screen.

**Criteria definition**

As mentioned above, criteria could typically include the effect on resilience (e.g. change in RIL), costs and time to implement the measure(s). In the example case (ID 15), only changes in resilience level and costs are considered, as shown in the criteria definition overview page in Figure 66.

![Figure 66: Overview of criteria defined](image)

New criteria can be added using the "Add New Criteria" button. This provides a pop-up window as shown in Figure 67 (here showing the already filled out cost criterion from the example case).

**Criteria group**

As for alternative improvement measures, all criteria are chosen by default in the MCDM analysis; however, it is possible to make different groups of the criteria, e.g. to have one group with change in RIL, costs and time for implementation, and another group consisting of only change in RIL and costs (as in the example...
case in Figure 66). To add a new criteria group, click on the "Add New Criteria Group" button in the "Criteria group" screen.

**Figure 67:** Defining a criterion – example

**Criteria weight**

The different criteria must be weighed against each other in the MCDM analysis. The default is equal weights, e.g. that change in RIL and costs are equally important, i.e. both with a weight 0.5. This may be changed by adding new "weight groups," where the user defines the weight of each criteria (adding up to 1.0, of course). This was done in the example case, as shown in Figure 68.

**Figure 68:** Overview of different weights provided between the criteria – example

Figure 69 shows that the costs count 70% and change in resilience level counts 30% in the example case (this screen is opened by editing the user defined weight group (ID 19) in Figure 68).
Analysis setup

Since there can be different groups of alternatives, criteria, and criteria weights, the groups need to be selected for each analysis, i.e. there can be different analyses with different combinations of the three groups. This is illustrated in Figure 70 for the example case.

In the example case, the first analysis (ID 20) is the default setup, i.e. all alternatives and all criteria are included, and the criteria have equal weights. In the second analysis (ID 21), a different alternative group is used, and the criteria are given user defined weights.

The definition/selection window for the second analysis (ID 21) is shown in Figure 71. The window is opened by editing the analysis ID 21 (from screen shown in Figure 70).
Input data

Input data for each of the analyses are entered as shown in Figure 72.

<table>
<thead>
<tr>
<th>Alternatives</th>
<th>Cost / Euros / [1,000,000.00 - 8,000,000.00]</th>
<th>Change in Resilience level / RL improvement / [0.01 - 1.00]</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpA1 (remain same)</td>
<td>1,000,000.00</td>
<td>0.01</td>
</tr>
<tr>
<td>OpA2 - One new gas fired heating plant added</td>
<td>3,500,000.00</td>
<td>0.02</td>
</tr>
<tr>
<td>OpA3 - One new biomass plant added</td>
<td>6,000,000.00</td>
<td>0.06</td>
</tr>
<tr>
<td>OpA4 - One electrical heating plant added</td>
<td>8,000,000.00</td>
<td>0.10</td>
</tr>
</tbody>
</table>

Values are provided within the ranges defined in the criteria definition step (see Figure 67). A main challenge is to obtain the change in resilience level. Each of the alternatives need to be compared with the baseline resilience level assessment, by performing the RIL assessment for each of the alternatives and compare the results.
Ranking results

Selecting the "Ranking results" item in the menu opens the window shown in Figure 73, where the calculations have been performed and the results presented.

OpA1 has the highest rank and is the optimal option.

6.2.4 Dependency analysis and Big data uploader

Dependency analysis through interdependency identification and cascading effects loss estimation was presented in Chapter 5. In Figure 37, it is indicated that interdependency identification primarily provides input to the resilience level assessment, i.e. interdependencies that should be considered in the RIL assessment. It is also indicated with a red dotted arrow that the main connection to the tool is that these interdependencies should be included as issues. The case is the same for the cascading effect loss estimation, where these advanced analyses provide suggestions for economic resilience indicators. In addition, these economic resilience indicators, and other big data driven indicators get their values through the "Big data uploader," as illustrated in Figure 34 and described in Chapter 5.

For more advanced analyses of issues and indicators, including potential interdependencies through a "dynamically learning" system, we refer to D2.3 Section 4 [45] and D3.7 [51].

Big data uploader

The four steps to use the Big data uploader are:

1. Choose your indicator from the existing Dynamic Checklist
2. Upload XLS file with your input data
3. Run background analysis
4. Check your outputs

Step 1 was shown in Figure 34 and is the step where the (big data) indicator is selected from the relevant DCL.
Step 2 is illustrated in Figure 74 (as it looks in the tool). Here an XLS file with input data must be uploaded. The user must first download the template (see blue text in Figure 74) and follow the instructions for entering input data into the XLS file.

![Figure 74: Uploading input data to big data indicator](image)

The downloaded template consists of three sheets: a Data sheet, a "How to" sheet, and an Example sheet. The Data sheet is shown in Figure 75.

![Figure 75: Data sheet for big data uploader](image)

As the notice says, only the data sheet must be included in the XLS file when uploaded in the tool. The "How to" sheet is shown in Figure 76.

![Figure 76: "How to" (instruction) sheet for big data uploader](image)

The Example sheet is shown in Figure 77.
Step 3, running the background analysis, is shown in Figure 78.

Step 4, checking outputs, is shown in Figure 79.
7 Advice on legislation, organizational factors and ethics

7.1 Introduction

This chapter provides a description of some contextual factors that should be considered when conducting an assessment as described in the previous chapters. It includes legal issues, organizational requirements, as well as ethical considerations. Note specifically the checklist in Table 18 and recommendations in Table 19.

The compatibility of the resilience approach and the existing legal and regulatory regimes has been discussed by resilience researchers (e.g. [3]), as also elaborated in the framework of the H2020 EU project RESILIENS [9]. It has e.g. been found that characteristics related to “persistence” (compliance) are quite well addressed by legal systems, while others such as adaptability or transformation are not accounted for in many cases [3], [9]. Reasons for this include that many laws neither sufficiently consider local differences, nor allow for reactions to changing circumstances [9].

While it is beyond the scope of this guideline to further investigate possibilities to enhance the integration of resilience in the legal and regulatory framework, an overview is provided on existing legal acts that oblige stakeholders to assess resilience and to maintain a certain level of resilience of smart critical infrastructure, which is further described in [46]. These legal acts can (directly or indirectly) be the trigger for conducting a resilience assessment. However, since not all actors are aware of each legal act, some most relevant legal acts are summarized in this chapter.

Legal acts not only play a role because they oblige stakeholders to address resilience. They can also influence the success of actions to assess or to increase resilience (“external influencing factors”). In this context, especially the data protection legal framework is important.

The success of resilience measurement also highly depends on organizational preconditions ("internal influencing factors"), which are also described.

Finally, the chapter addresses the issue of ethics. Specifically, what are possible unintentional consequences that the development and use of indicators can have? And how can this be addressed beforehand, and possible negative results mitigated?

7.2 Consider legal obligations

Obligations to assess and maintain a certain level of resilience are manifested in legal acts on different levels, most importantly on EU and on national level. More elaborated lists and descriptions of these can be found in D3.1 [46].

On EU level, the “strongest” types of legal acts are regulations, directives, and decisions, which the EU defines as follows [24]:

**Regulations**

A "regulation" is a binding legislative act. It must be applied in its entirety across the EU. For example, when the EU wanted to make sure that there are common safeguards on goods imported from outside the EU, the Council adopted a regulation.

**Directives**

A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the EU consumer rights directive, which strengthens rights for consumers across the EU, for example by eliminating hidden
charges and costs on the internet and extending the period under which consumers can withdraw from a sales contract.

**Decisions**

A "decision" is binding on those to whom it is addressed (e.g. an EU country or an individual company) and is directly applicable. For example, the Commission issued a decision on the EU participating in the work of various counter-terrorism organisations. The decision relates to these organisations only [20].

The European Programme for European Critical Infrastructure Protection (EPCIP) provides an overall frame for critical infrastructure protection (energy, transportation, and finance) in the EU. It focuses on the identification and assessment of critical infrastructure in the EU (established in Directive 2008/114/EC [14], see below), the Critical Infrastructure Warning Information Network (CIWIN), the funding for over 100 critical infrastructure protection projects, as well as international cooperation [19].

Relevant EU Directives, including obligations for stakeholders to conduct resilience assessments or to maintain a certain level of resilience, include the following five directives:

1. **Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection**

   Directive 2008/114/EC [14] establishes a procedure for the identification and designation of European critical infrastructures (ECIs), and a common approach to the assessment of the need to improve the protection of such infrastructures to contribute to the protection of people. The Directive applies to the energy and transport sectors. Member States (MSs) must regularly review the identification of ECIs, and each ECI must have an "operator security plan" in place. MSs must conduct threat assessments and report the types of risks, threats and vulnerabilities every 2 years. Thus, it constitutes one of the basic legal acts in the context of resilience assessment.

2. **Directive 2013/40/EU – on attacks against information systems**

   Directive 2013/40/EU [21] is relevant especially due to the “smart” character of CIs addressed in SmartResilience. It establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to tackle such offences and to improve cooperation between judicial and other relevant authorities. The Directive introduces new rules harmonizing criminalization and penalties for a number of offences directed against information systems. It also calls for EU countries to use the same contact points used by the Council of Europe and the G8 to react rapidly to threats involving advanced technology. The main types of criminal offences covered by this Directive are attacks against information systems, ranging from denial of service attacks designed to bring down a server to interception of data and botnet attacks.


   Also, the “NIS Directive” [22] seems most relevant in the context of SmartResilience considering the “smart” component of the project. It prescribes measures to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market. It also sets out obligations to all MSs to adopt a national strategy on these matters. The Directive creates a cooperation group as well as a computer security incident response network. Requirements for operators about security and notification are established. The Directive further lays down obligations for MSs to designate national authorities.


   Directive 2007/60/EC [13] establishes a framework for the assessment and management of flood risks, which aims to reduce their adverse consequences for human health, the environment, cultural heritage and economic activity within affected communities. It is thus relevant for all CIs that are prone to flood events. The Directive prescribes a three-step procedure consisting of a preliminary flood risk assessment, a risk
assessment and flood risk management plans. The flood risk management plans are not formally binding, but measures are proposed to manage the risks and focus on prevention, protection and preparedness.


The “Seveso III Directive” [15] is based on a preventive principle that aims to anticipate possible (probable) negative effects from events involving dangerous substances and uses various instruments to avoid the occurrence of damage. It is achieved by focusing on ways to avoid transboundary pollution, prevent pollution at source, reduce environmental damage and reduce the risk of harm. The Directive covers facilities where dangerous substances may be present (e.g. during processing or storage) in quantities above a certain threshold. Operators of the infrastructures are obliged to take all necessary measures to prevent major accidents and to limit their impact on human health and the environment. The requirements include [15]:

- Notification of all concerned establishments (Article 7);
- Deploying a major accident prevention policy (Article 8);
- Gathering information about the domino effects (Article 9);
- Producing a safety report for upper tier establishments (Article 10). This article specifically, focuses on indicators for monitoring performance;
- Producing internal emergency plans for upper tier establishments (Article 12);
- Providing information in case of accidents (Article 16).

A more comprehensive overview can be found in D3.1 [46].

EUR-Lex8, which includes amongst others all types of EU law, related actions and summaries reflecting the policy context, also allows to check how member states have incorporated an EU legal act into national law (as communicated by the member states)9.

To exemplify national legislation that obliges stakeholders to assess and/or maintain a certain level of critical infrastructure resilience, important legal acts in Germany in the field of energy supply, and important legal acts in Sweden in the field of drinking water supply are described in D3.1 [46].

D3.1 further includes chapters on “guidelines and support,” which in part are directly related to specific legal acts.

7.3 Consider external and internal influencing factors

7.3.1 External (legal) factors

When assessing resilience, or when conducting measures to increase resilience, specific legal acts can influence the success of these actions. An important issue to be considered is data protection, which becomes relevant in many cases when collecting data – the basis for any resilience assessments using indicators.

On EU level, current legal framework of data protection is manifested in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [16].

Directive 95/46/EC [16] seeks a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the EU. The full text (as well as a summary) is available on the EU’s official website.

---

8 http://eur-lex.europa.eu/homepage.html
The EU legal framework of data protection is currently within a process of change: A comprehensive reform of data protection rules in the EU was proposed in January 2012 by the European Commission. It comprises a Regulation (Regulation (EU) 2016/679 – protection of natural persons with regard to the processing of personal data and the free movement of such data [23]) and a Directive (Directive (EU) 2016/680 – protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data [18]), which entered into force in May 2016, while the Regulation entered into force in May 2018, before which the Directive had to be transposed into national law by the EU Member States. These new legal acts are a response to challenges from the digital age. They shall strengthen citizens’ control over their personal data and simplify the regulatory environment for business – and thus support the Digital Single Market Strategy, which the European Commission has prioritised [20].

A detailed description of the legal framework of data protection on EU level is included in D3.1 [46], complemented by an example for data protection legislation on national level, using the German data protection law [25]. Further, checklists exist that can be used to evaluate the compliance with the national data protection law. D3.1 [46] includes the example of the German “Checkliste Technische und organisatorische Maßnahmen nach §9 BDSG, Annexe 1-3 – TOM,” which includes checklists on e.g. physical access control and entry control.

Besides the collection of data, also limited possibilities to share data in terms of assessment results and respective exchange with other stakeholders is seen as hindering for resilience-related actions10.

While environmental legislation [17] can implicate obligations regarding the resilience of specific critical infrastructure (cf. Section 7.2), it can also hinder actions intended to enhance resilience of specific critical infrastructure. For example, an infrastructure that is not resilient can have negative impacts on the environment such as water contamination, which environmental laws try to avoid. On the other hand, actions that are actually meant to avoid negative impacts on the functioning of infrastructure, and thus to increase resilience, can also implicate negative impacts on the environment. As an example, non-renewable energy sources might be more resilient regarding a secure energy supply also during specific hazards events but do more harm to their environment. Thus, respective environmental legislation must be considered. Environmental legislation has also been mentioned by SmartResilience end-user partners11 as being a possible hurdle when implementing actions to increase resilience.

7.3.2 Internal (organizational) influencing factors

The success of resilience assessments and/or the implementation of resilience measures, strongly depend on factors and structures within an organization, which can be supportive or hindering.

The checklist in Table 18 does not claim to be exhaustive, and most useful implications of its results can only be identified on a case by case basis. However, it can help to identify factors that can be improved in order to enhance the possibilities to successfully conduct resilience assessments and/or to successfully implement measures to increase resilience.

Respective issues are partly also represented in specific resilience indicators (D4.1 [53], D4.2 [54]). However, representing required context factors for successful resilience assessment and actions, those issues that were described by practitioners are listed here. They can be grouped into topics on “staff + work process”, “tools”, “cooperation”, and “others”.

10 SmartResilience workshop April 24-26, Budapest
11 SmartResilience workshop April 24-26, Budapest
Table 18: Checklist on organizational factors

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes/ No</th>
<th>if Yes, the positive effect can be</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staff + work process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there specialised staff and/or even a dedicated unit within the organization?</td>
<td>Yes/No</td>
<td>Dedicated place for knowledge, expertise, resources, and tools can ensure that the required resources are available</td>
</tr>
<tr>
<td>Is there any training for responsible staff members on:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ How to conduct resilience assessments?</td>
<td></td>
<td>Improved abilities to conduct resilience assessments and to implement actions to enhance resilience</td>
</tr>
<tr>
<td>▪ How to report assessment results?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ How to implement actions to increase resilience?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there sufficient knowledge about realistic risks, criticality of infrastructure, and possible cascading effects?</td>
<td></td>
<td>Improved awareness</td>
</tr>
<tr>
<td>Do responsible staff members have expertise in the application of indicators?</td>
<td></td>
<td>Increased feasibility of resilience assessments</td>
</tr>
<tr>
<td>Are resilience assessments integrated into company processes / daily work?</td>
<td></td>
<td>Enhanced possibilities for assessments</td>
</tr>
<tr>
<td><strong>Tools</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a useful Decision Support System in place?</td>
<td></td>
<td>Improved abilities to implement actions to enhance resilience</td>
</tr>
<tr>
<td>Are clear, practical and easy to use methodologies for resilience assessments known and available?</td>
<td>Yes/No</td>
<td>Improved abilities to conduct resilience assessments</td>
</tr>
<tr>
<td>Are specific guidelines for specific areas known and available?</td>
<td></td>
<td>Improved abilities to implement actions to enhance resilience</td>
</tr>
<tr>
<td>Do the existing IT systems allow to efficiently extract required data for resilience assessments?</td>
<td>Yes/No</td>
<td>Feasibility to gain relevant data without using too much time and man-power</td>
</tr>
<tr>
<td><strong>Cooperation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do confidentiality rules allow to share assessment results with other stakeholders?</td>
<td>Yes/No</td>
<td>Improved possibilities of learning from each other</td>
</tr>
<tr>
<td>Is the cooperation with other relevant stakeholders (e.g. police, fire brigade, armed forces) sufficiently in place?</td>
<td>Yes/No</td>
<td>Improved motivation; improved abilities to implement actions to enhance resilience</td>
</tr>
<tr>
<td>Does any exchange of experiences with similar actors take place?</td>
<td></td>
<td>Improved sharing of knowledge + increased motivation</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can the resilience assessment be conducted without using sensitive data?</td>
<td></td>
<td>Enhanced possibilities to use available data</td>
</tr>
<tr>
<td>Is the amount of available data manageable?</td>
<td></td>
<td>Enhanced possibilities to select relevant data</td>
</tr>
</tbody>
</table>

7.4 Consider ethical aspects of indicator-based resilience assessment

Resilience assessment is obviously intended to contribute to improved resilience to the benefit of critical infrastructures and the society at large. However, even with the best of intentions, unintended consequences caused by the application of resilience indicators can occur and can be difficult to anticipate. Even so, some factors may contribute to unintended consequences and, therefore, the knowledge of these factors raises awareness. Taking into consideration the knowledge of different contributing factors and
potential problems, and having a continuous follow-up, the occurrence of unintended consequences may be reduced.

Table 19 provides an overview on recommendations aimed at minimising the potential negative implications of assessing resilience. Users of the guideline should specifically check the “application phase.”

Table 19: Overview of ethical recommendations

<table>
<thead>
<tr>
<th>Phase</th>
<th>To Do</th>
</tr>
</thead>
</table>
| Pre-research phase (all involved stakeholders) | - Check all intentions and motivations of the involved partners and supporters  
Who initiated a research project and who benefits of the research regarding resilience indicators?  
If there is any conflict, address the conflict in the project team to ensure independent research. |
| During research phase (researchers) | - Define the system of your research  
- Define and document the term “resilience,” explicit policy linked to the definition; and explicit articulate the scale and context  
- Prove carefully any generalizations  
- Check the data fundament for completeness, correctness, consistency and traceability |
| Application phase (all users of resilience indicators) | Before using resilience indicators:  
- Check chosen resilience indicators for the quality criteria as presented in the figure  
Additionally,  
- Check if there is a current need for the resilience indicator (relevance), otherwise the resilience indicator can be inaccurate.  
- Check if others cannot use a developed indicator due to a lack of understanding. Is the resilience indicator presented in a comprehensible way?  
- In a complex resilience system, data may be unavailable to execute the application of resilience indicators in such a way that the results are sufficient. Missing data may reduce the application possibilities. |
| In case of any occurring ethical conflict | - Discuss the conflict with all involved stakeholders and check the three main conditions: 1) validity, 2) objectivity and 3) reliability  
If open questions cannot be solved, the indicator should not be used for any further actions! |

The figure in Table 19 outlines a set of indicator quality attributes or requirements, which can be used to evaluate the quality of a resilience indicator. It is based on e.g. [11], [12], [57] and [60]. Further information can be found in D3.1 [46]. See also Section 2.3.2.3 about relevant indicator quality attributes.
8 Example case studies – descriptions

Four SmartResilience project case studies have been used as examples throughout the guideline. These are:

- Transportation - airport security (labelled DELTA in the project)
- Industrial production (labelled ECHO in the project)
- Drinking water supply (labelled FOXTROT in the project)
- Underground fuel storage and energy supply (labelled HOTEL in the project)

All four case studies are used as partial examples, e.g. in Chapter 2. ECHO is used as example case in the method description of RIL and FL assessment in Chapter 2 and 3, and in the tool description of DCL setup, RIL assessment and resilience monitoring in Chapter 6. HOTEL is used as example case in the tool description of FL assessment and resilience optimization (MCDM) in Chapter 6.

In this chapter, descriptions of the example cases are provided. The descriptions include a general case study description and a specific scenario description. The latter has been used for exercises, particularly related to stress-testing. The descriptions are mainly based on D5.1 [55] and D5.2 [56].

In addition, DCLs for RIL and FL assessment are included for the ECHO and HOTEL cases in Annex 2.

8.1 Transportation - airport security (DELTA)

The Budapest Liszt Ferenc International Airport (BUD) is the largest international airport of the Hungarian capital city, Budapest. The total land area of the facility is 15,050,000 square meters. The facility has both commercial (passenger, cargo) and general aviation traffic, but is also occasionally serving military airplanes (e.g. KC-130s in Balkan wars). In 2016, the commercial aviation handled more than 11.4 million passengers, more than 90,000 aircraft movements and 112,000 tons of cargo with coordinated work of approximately 10,000 people. Border traffic size: 3,677,714 people did cross the Schengen external borders at the airport in 2015. There is a 5-level security check system, covering public and national security, passenger security, border security and customs checks. Blocking of the air traffic in the main airport of a member state has a deep effect over the country and related airports. BUD T1 is a medium-size passenger terminal, at the day of the exercise it will have 1000 passengers, more or less randomly divided between airside and landside. Two threat scenarios will be played through, forcing the security personnel to perform evacuation accordingly.

Stress-test scenario case 1:
Detected Improvised Explosive Device (IED) trace threat in the middle part of the terminal (passenger security), between airside and landside, in cascade with two other unattended luggage alerts (1st at the centre, 2nd at arrival airside baggage claim area, 3rd at the mezzanine level). At the same time, Disaster Management Centre alerts the Hungarian National Police (HNP) that their Cerberus server responsible for operating the terminal’s automated extinguisher system has been cyber-attacked exploiting vulnerability.
CVE-2012-2999\textsuperscript{12}, resulting in denial of service, meaning the automated fire extinguishing system is blinded and will not be operational in case of explosion or fire.

Therefore, sealing of terminal parts with only partial evacuation of the terminal – as usual in case of unattended luggage - is not enough, operational level of the facility has dropped, as without operating Cerberus PRO fire safety system it cannot operate safely. Full evacuation has to be commenced in two directions as the location of the IED threat cuts the terminal area in two, between airside and landside.

Passengers and staff will be evacuated in two main directions, as the central of the threat separates the territory in two parts.

\textit{Stress-test scenario case 2A:}

Industrial accident near the terminal. Sulphur dioxide is released into the air. Complete evacuation is not possible. The placement of persons must be solved at the terminal. The gas is self-dispersed. The expected duration of the pollution is approx. 5-6 hours. Some terminal parts are also contaminated, passengers have to be secured at safe terminal parts. Landside and airside apron areas also have to be empty. In this case there is no “pure” evacuation based on main threats, but emergency handling of passengers and staff will provide a challenge to the local authorities and to the airport operator. People in the forefront of the terminal building and passengers at the airside have to be evacuated from the external parts into the building.

\textit{Stress-test scenario case 2B:}

Ongoing decontamination, several escape routes free and safe, terminal has to be fully evacuated. Passengers and staff will be evacuated in one main direction (towards the landside, e.g. public parking areas), as the cause of the blocked transport interferes all people within the area.

\subsection*{8.2 Industrial production (ECHO)}

City of Pančev has the so called Southern Industrial Zone located at the southeast edge of town, right next to the residential area of the city, app. 4 km away from the city centre. In addition to the compound of the HIP-Petrohemija a.d. Pančev, this zone includes the HIP Azotara Pančev a.d. and NIS Oil Refinery Pančev. The area is connected to road, rail and river circulation by means of the port on the Danube River. In this industrial zone, there is a production of petroleum products, basic chemical products, polyethylene, mineral fertilizers, calcium ammonium nitrate, carbamide and NPK fertilizers. These infrastructures are inter-connected and interdependent. The whole zone is regarded as one big CI or CIs.

\textit{Stress-test scenario:}

Within the ECHO case there is one scenario – BLEVE (Boiling liquid expanding vapour explosion) identified as the major accident with the most severe consequences based on calculation and modelling done and presented in the Safety report. From the Safety report, two worst cases have been considered for BLEVE effects.

\begin{itemize}
  \item Case 12 from the Safety report– Spillage of propylene from sphere reservoir FB-16705 (1000m\textsuperscript{3}) on the warehouse 16700.
    
    Description of the incident: Propylene spillage occurred on the first flange joint of the pipeline for decanting of propylene from the sphere FB-16705 due to propulsion of the seal of 50 mm in length and 3 mm in width.
    
    Time duration of the incident: 30 minutes.
  
  \item Case 14 from the Safety report: Incident on the FB-5001 vessel (10m\textsuperscript{3}) for hydrogen reserve.
    
    Description of the incident: Since reservoir with hydrogen is under high pressure, it may come under its total destruction physical explosion under certain conditions.
\end{itemize}

\textsuperscript{12} CVE – Common Vulnerabilities and Exposures; CVE-2012-2999, see \url{https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2999}
When a vessel containing pressurized gas breaks, as a result of that, stored energy is released. This energy may produce shock wave and flying fragments of vessels.

Time duration of the incident: 1 minute.

Besides this reservoir FB-16705 (1000m³) there are 5 more reservoirs with the same capacity, on which potentially BLEVE effect could happen. There are many causes that could provoke such an event.

One of the main causes that was analysed is leakage of liquefied petroleum gas (LPG) on the flange located next to the LPG vessel, with subsequent ignition of the LPG. Combustion of LPG on the affected valve will have direct contact with the vessel will cause heating up of LPG inside the vessel and this will result in rapid vaporization and increase pressure which will lead to explosion. The consequences of such explosion could include only very hypothetically a “domino” effect due to thermal radiation and flying debris. Such an effect could be provoked by terrorist attack or sabotage.

Hypothetically, it is also possible to get affected by cyber-attacks on ICT systems.

8.3 Drinking water supply (FOXTROT)

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

In the FOXTROT case, the focus is on the microbial contamination of water and threats to the ICT systems in the waterworks and distribution. Waterborne disease is linked to climate change and is predicted to be more frequent in the future as described in each threat description. Threats to the ICT systems is linked to the vast digitalization of industrial processes, including drinking water production, causing new challenges for the producers to prevent vulnerabilities in the systems.

**Stress-test scenario:**

The scenario takes place in a medium-sized Swedish city with 10-15,000 inhabitants. In the city there is a waterworks that supplies approximately 10,000 people with drinking water. The water is taken from a surface water source and is after the purification process distributed out to the people in the city.

It has been raining for about a week. At the beginning of the week about four to five millimetres a day, and the soil begins to get saturated, the rain does not decrease but increases and after seven days it has reached about 40-50 mm. Then the city is suffering from an intense rainfall, a so called 100-year rain, and for about 24 hours it rains intensively. A total of about 150 mm falls on an already saturated field. SMHI (Swedish and Meteorological and Hydrological Institute) goes out with warning class 3. The heavy rain is leading to floods. All low points in the area, such as road tunnels, are flooded and so are many basements.

One of the wastewater treatment plants have suffered loss of electricity and has lost its functionality and automatic controls. The surface water source is flooded. Even though there is no electricity the treatment plant still faces a risk of overflow because of the large amounts of water still coming in.

Fecal indicators are coming into the surface water with the flood. The usual treatment is precipitation in combination with chlorine treatment or UV treatment. Even diaphragm or filters can be used.

A number of waterworks pipelines have also been demolished, of which two large pipes are completely depleted. This leads to water towers empty quickly.

After a time, also the waterworks SCADA system goes down due to loss of electricity.

8.4 Underground fuel storage and energy supply (HOTEL)

The energy supply infrastructure in the city of Helsinki, mainly through the city-owned energy company Helen Oy, is producing and distributing three main products, district heating, district cooling and electricity.
Of these, electricity supply involves fair redundancies by alternative feed sources, and as the yearly mean temperature in Helsinki is +6°C and the mean for the warmest month +18°C (July, with average daily maximum of 21.5°C), cooling is less critical than heating. The main supply sources of district heating are the three major power stations, supported for peak loads by smaller heating plants and few limited connections to the adjacent systems of the neighbouring cities. The distribution piping system for district heating in Helsinki is more than 1300 km in length and runs underground to all public and most private buildings in the city. District heating can easily cope with usual and many unusual winter circumstances, as the mean daily minimum temperature (-7°C) of the coldest month (February) is well above the designed minimum temperature for the system [35]. However, the system is not designed to cover sustained load approaching the record cold in Helsinki (-34°C in 1987). In spite of the redundancies, disturbances in critical or multiple nodes of sourcing and distribution could also limit the heating function during severe cold spells. Such challenges represent threats to the heating system function, customer expectations, and in extreme cases, to public health. The relevant threats for the case are natural and new technology related threats.

The case focuses on a scenario that can significantly disrupt the district heating supply or distribution in Helsinki, namely fire in the underground fuel storage of a power plant (supply node for district heating). Short-term events can trigger the scenario that then will take some time to develop significance, depending on weather and functionality of other resources in the system. There is experience on the initiation and management of the scenario, as self-heating and auto-ignition in solid fuel storage is not very rare [42]. More challenges could appear with e.g. increasing share of biomass-derived solid fuels in storage.

**Stress-test scenario:**

The scenario of self-heating and auto-ignition typically involves a bed of solid fuel, where the combination of air ingress, limited heat transport and exothermal oxidation may allow for gradual heating up to the ignition of a smouldering fire, especially in cases of long storage time, sensitive fuel quality and/or warm fuel entering storage. Storing fuel in underground silos will add to the challenge by limiting access for countermeasures. Significant disruption of district heating service under high load (cold spell) would normally also require additional trouble from failing alternative fuel feed and loss of another heating plant source.

In a severe but conceivable case, auto-ignition and fire could initiate and develop as follows: a batch of fuel has entered the storage silo when warm, or with a heating and ignition-prone composition/quality or was stored for a lengthy time in the silo. During a midwinter cold spell (below -20 to -25°C) at full load of the district heating network, after ignition the thermal gradient and gaseous combustion products diffuse only slowly from the fuel bed centre. When the period between ignition and detection is not short, a relatively extensive volume of fuel will be involved in the resulting smouldering fire. The adopted extinguishing countermeasures include water and possibly nitrogen injection and directing the silo contents to boiler for removal. Nevertheless, the fire in this case will proceed to emit combustion gases also to the area surrounding the plant, annoying the residents. Public complaints in local and national media may result in untimely technical modifications. Meanwhile, heated fuel directed to combustion will result in conveyor damage so that all silos become unavailable. With no support oil fuel due to its high viscosity in a cold storage tank, the backup fuel comes by truck transport from another plant, but at a low rate meaning plant derating to 60% capacity. Then boiler failure takes a nearby heating plant out of service, and the combined deficit in production results in gradual system cooling in a part of the network. The impact becomes significant during the extended cold spell and extended period of reduced plant capacity. The following (simplified) timeline describes the scenario.

| t₀ | The network, including the Salmisaari plant, is running at 100% of the capacity |
| t₁ | Self-ignited fire is detected with delay, still the plant is running at 100% of the capacity |
| t₂ | Redirected heated fuel to combustion takes out conveyor belt and thereby all underground fuel silos. Attempts to get replacement fuel from the plant storage fail. Production of the plant falls to 60% of the capacity, relying on fuel transported from Hanasaari plant by truck. A nearby heating plant falls to 0% production, so that the district of the heating network starts to cool. |
t₃  The storage is non-functional, Salmisaari plant continues to operate at 60% capacity and the nearby heating plant remains out of service. The district of the network has cooled so that it triggers evacuation of high priority people from elderly peoples’ homes.

t₄  The conveyor belt has been repaired and the Salmisaari plant becomes functional at 100% of the capacity.

t₅  The nearby heating plant is also recovered and running at 100% of the capacity, so that the network is supplied with heating as required by the demand.
References


SmartResilience (2017). Deliverable D3.7: SCIs Dashboard containing the module on Dynamic Intelligent Checklists and the link to the RapidMiner based modules. First version. [In progress]


## A N N E X E S

<table>
<thead>
<tr>
<th>Annex</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex 1</td>
<td>Review process ..........................................................</td>
<td>109</td>
</tr>
<tr>
<td>Annex 2</td>
<td>Catalogue of resilience indicator checklists ..........</td>
<td>110</td>
</tr>
</tbody>
</table>
Annex 1  Review process

The Content of this Annex has been submitted as part of the periodic review report to the PO/EU/Reviewers.
Annex 2 Catalogue of resilience indicator checklists

The catalogue of resilience indicator checklists (Dynamic Checklists - DCLs) is included in the SmartResilience tool, see Figure 80.

As shown in the figure, there are more than 100 DCLs in the tool. They can be exported to Excel and Word. Here we only include examples of DCLs for the resilience level assessment and functionality assessment for the ECHO case and the HOTEL case. There are many DCLs for each case, so those included in this annex may differ from those used as examples for assessments in the main part of the guideline.

In addition, we include the Core DCL consisting of generic issues that should be included in all cases, even if they are measured with different indicators. This makes it possible to benchmark at least a part of the assessments, i.e. the part covered by the Core Issues, against others.

The Core DCL may (as all DCLs) be further developed in the future.
### A.2.1 DCL for Resilience Level Assessment of the ECHO case

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Understand risks</strong></td>
<td></td>
</tr>
<tr>
<td>I.1. Safety Risk registry; ID-2060</td>
<td>A Safety Risk registry is necessary to have an overview of risks within an organization and is used as a tool for making decisions, such as defining appropriate control measures and development of improvement action plans</td>
</tr>
<tr>
<td>I.1. Does the Safety Risk registry exist?; ID-2061</td>
<td>Simple existence of this registry in the organization with clear classification of the risk level (high, medium, low)</td>
</tr>
<tr>
<td>I.1.2. Using of Safety Risk registry in decision making; ID-2062</td>
<td>Is the Safety Risk registry used in decision making?</td>
</tr>
<tr>
<td>I.1.3. Frequency of revision of Safety Risk registry defined?; ID-2063</td>
<td>Considering the fact that in the production process different types of changes occur all the time, e.g. technical/organizational changes, one of the tools that has to be used is a risk registry. There should be established intervals when this risk registry should be revised and updated to consistently help in making right decisions</td>
</tr>
<tr>
<td>I.2. Management of Change - MoC; ID-2064</td>
<td>The Management of Change (MoC) helps ensure that changes to a process do not inadvertently introduce new hazards or unknowingly increase risk of existing hazards</td>
</tr>
<tr>
<td>I.2.1. Is a procedure for Management of Change established?; ID-2065</td>
<td>Establishing MoC enables the ability to ensure that changes to a process won’t give rise to new risks and to ensure that existing risks are considered</td>
</tr>
<tr>
<td>I.3. Register of accidents/incidents; ID-2071</td>
<td>Register that generates all accidents/incidents identified</td>
</tr>
<tr>
<td>I.3.1. The existence of a register of accidents/incidents; ID-2072</td>
<td>Simple existence of this register in the organization</td>
</tr>
<tr>
<td>I.3.2. Frequency of communication with units about occurred accidents; ID-2073</td>
<td>Are accidents/incidents from this register communicated with operators?</td>
</tr>
<tr>
<td><strong>II. Anticipate/Prepare</strong></td>
<td></td>
</tr>
<tr>
<td>II.1. Emergency exercises; ID-2075</td>
<td>Timely conducting exercises provide company emergency preparedness through practice and should be planned in time and updated regarding new equipment, new technologies, and new operators</td>
</tr>
<tr>
<td>II.1.1. Existence of emergency exercise plan; ID-2076</td>
<td>To cover all shifts and employees and to make proper preparations for conducting exercises, it is important to have a plan in place</td>
</tr>
<tr>
<td>II.1.2. % Emergency exercises completed according to the schedule; ID-2077</td>
<td>The entire exercise plan should be completed accordingly to the defined deadline. In order to keep track you should measure the progress. If the plan is not fulfilment, there is a risk of untrained people that will not adequately respond in case of an emergency situation</td>
</tr>
<tr>
<td>II.1.3. % of new employees provided emergency response training; ID-2078</td>
<td>All persons that are involved in emergency response must be trained, first initially, and then after some time perform refresher training</td>
</tr>
<tr>
<td>II.2. Presence of firefighters at the production site; ID-2079</td>
<td>Considering the existing risk present at production sites, according to state law, each site should have a certain number of firefighters during 24/7</td>
</tr>
<tr>
<td>II.2.1. Drills for the firefighters fulfilled according to the plan; ID-2080</td>
<td>Drills for the firefighters are mandatory. The plan should be prepared thoroughly and controlled frequently</td>
</tr>
</tbody>
</table>
### Dynamic Checklist - Resilience Level

#### Smart Industrial zone in the City of Pančevo affected by a hypothetical BLEVE

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>II.2.2. Analyses and evaluations of performed firefighter drills; ID-2081</td>
<td>Are periodic analyses and evaluations done to ensure that the firefighters are adequately trained to respond properly in emergency situations?</td>
</tr>
<tr>
<td>II.2.3. Number of deficiencies identified in firefighter drills performed; ID-2082</td>
<td>After each drill performed, it should be carried out a meeting to analyse the performed drill. All deficiencies identified must be recorded and measures defined</td>
</tr>
<tr>
<td>II.3. Maintenance plan; ID-2089</td>
<td>Plan of maintenance for relevant equipment used in production</td>
</tr>
<tr>
<td>II.3.1. Is a maintenance plan developed for each production unit?; ID-2090</td>
<td>This provides information about whether maintenance activities are planned and subsequently monitored</td>
</tr>
<tr>
<td>II.3.2. Is the maintenance plan executed?; ID-2091</td>
<td>All maintenance activities according to this plan should be executed on time</td>
</tr>
<tr>
<td>II.3.3. Is the maintenance plan based on recorded events?; ID-2092</td>
<td>In order to have a complete and adequate maintenance plan, it is necessary to take into account previous events and prevent recurrence</td>
</tr>
<tr>
<td>II.3.4. Are maintenance activities planned?; ID-1039</td>
<td>Is there a plan for maintenance activities in the facility in place?</td>
</tr>
</tbody>
</table>

#### III. Absorb/withstand

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.1. Safety equipment; ID-2100</td>
<td>This equipment is important in a case of unexpected events when it should be in service and help to prevent the undesired event</td>
</tr>
<tr>
<td>III.1.1. The number of activations of safety equipment; ID-2101</td>
<td>This is the number of times per year a certain safety equipment has been activated to prevent accidents. This indicates possible deviations in the process which should be paid attention to</td>
</tr>
<tr>
<td>III.2. Hi Hi alarm; ID-2098</td>
<td>When a Hi Hi alarm occurs in a process unit, it means that all allowable limits have been exceeded and urgent measures must be taken</td>
</tr>
<tr>
<td>III.2.1. The number of Hi Hi alarms activated; ID-2099</td>
<td>This is the number of times per period that the alarm has been activated on the specific equipment</td>
</tr>
<tr>
<td>III.3. Start-ups and shut-downs (S&amp;S); ID-2102</td>
<td>Unplanned shut-downs occur whenever some operating parameters (flow rate, temperature, pressure) greatly exceed predetermined limits in the system causing activation of emergency shut-down systems</td>
</tr>
<tr>
<td>III.3.1. The number of shut-downs; ID-2103</td>
<td>This is the number of times per period unplanned shut-downs occur</td>
</tr>
<tr>
<td>III.3.2. The number of near-misses or incidents due to S&amp;S; ID-2104</td>
<td>S&amp;S should be monitored for early identifications of deficiencies in order to timely respond and correct it</td>
</tr>
<tr>
<td>III.3.3. The number of deferred start-ups and unplanned shut-downs; ID-2105</td>
<td>This may indicate disturbances and require further analyses to determine the causes</td>
</tr>
<tr>
<td>III.3.4. % relevant personnel trained on S&amp;S prior to commencing this work; ID-2106</td>
<td>This indicator shows whether the personnel is prepared for conducting S&amp;S. This can serve as input for analyses of the training provided, if something has gone wrong during S&amp;S</td>
</tr>
<tr>
<td>III.3.5. % relevant personnel performed S&amp;S training versus plan; ID-2107</td>
<td>This indicator provides information about the commitment of personnel to be trained, as well as information about who is trained</td>
</tr>
<tr>
<td>III.4. Safety Instrumentations and Alarms (SIA); ID-2108</td>
<td>Safety alarms on the process equipment</td>
</tr>
<tr>
<td>III.4.1. Alarms per hour; ID-2109</td>
<td>This will help to track trends and to identify early warnings</td>
</tr>
</tbody>
</table>
### Dynamic Checklist - Resilience Level

**Smart Industrial zone in the City of Pančevo affected by a hypothetical BLEVE**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.4.2. Total number of SIA activations reported by operations; ID-2110</td>
<td>This can indicate weak points in the process and identify early warnings</td>
</tr>
<tr>
<td>III.4.3. Total number of SIA faults reported during tests; ID-2111</td>
<td>It serves to correctly identify, monitor and measure the damage mechanism(s), providing input in the prediction of when the degradation may occur</td>
</tr>
<tr>
<td>III.4.4. Mean time between alarm activations and operator responses; ID-2112</td>
<td>This can help to analyse available resources in terms of the time that operators need to respond</td>
</tr>
<tr>
<td>III.4.5. Number of SIA tests versus schedule; ID-2113</td>
<td>In order to be sure that Safety Instrumentations and Alarms operate accurately, necessary tests have to be carried out in a timely manner</td>
</tr>
</tbody>
</table>

**IV. Respond/recover**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV.1. Presence of firefighters at the production site; ID-2079</td>
<td>Considering the existing risk present at production sites, according to state law, each site should have a certain number of firefighters during 24/7</td>
</tr>
<tr>
<td>IV.1.1. S1E Number of firefighters per shift at site; ID-2307</td>
<td>Each shift needs to have a prescribed number of firefighters present per shift at the site</td>
</tr>
</tbody>
</table>

**V. Adapt/transform**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.1. Investigation of HSE events; ID-2114</td>
<td>Documented (written) incidents investigation procedure in place</td>
</tr>
<tr>
<td>V.1.1. Does the organization have a procedure for investigation of HSE events in place?; ID-2115</td>
<td>Is a written procedure of incidents investigation in place?</td>
</tr>
<tr>
<td>V.1.2. Investigation team qualifications; ID-2117</td>
<td>How well are members of the investigation team trained? Does the members of investigation teams have specified qualifications?</td>
</tr>
<tr>
<td>V.1.3. Percentage of application of incident investigation procedures in place; ID-2118</td>
<td>Are the incident investigations conducted according to the valid procedure?</td>
</tr>
<tr>
<td>V.1.4. Frequency of communication about the incidents to the external sites; ID-2120</td>
<td>Is there incident related communication exchange with other relevant production sites?</td>
</tr>
</tbody>
</table>

### A.2.2 DCL for Functionality Level Assessment of the ECHO case

**Dynamic Checklist - Functionality Level**

**Smart Industrial zone in the City of Pančevo affected by a hypothetical BLEVE**

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Production performance; ID-1234</td>
<td>The production out is one of the key functions of any infrastructure. In a refinery, this could be, for example, the total volumes of oil produced per day</td>
</tr>
<tr>
<td>1.1. G4-4: Domestic gas production (million m3/day); ID-1236</td>
<td>Level of the production measured in million m3/day</td>
</tr>
</tbody>
</table>
### Dynamic Checklist - Functionality Level

**Smart Industrial zone in the City of Pančevo affected by a hypothetical BLEVE**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2. G4-4: Domestic oil production (thousand tons/day); ID-2302</td>
<td>Oil production (with gasoline and light condensate) measured in tons/day</td>
</tr>
<tr>
<td>1.3. Overall Equipment Effectiveness (OEE); ID-2308</td>
<td>This indicator is used as an operational measure to monitor production performance</td>
</tr>
<tr>
<td>2. HSE: Health, Safety and Environment performance; ID-1247</td>
<td>In 2015, NIS continued the practice of recording HSE indicators from two perspectives – events that are under direct influence of the company, and those that are outside NIS’ direct influence, i.e. NIS-oriented records and contractor-oriented records. NIS top management continued quarterly theme meetings chaired by the General Manager and HSE management, ensuring safe working conditions for all employees and business partners as well as environmental protection. Also, it continued its business operations in accordance with the &quot;HSE Policy&quot; (adopted in 2013), HSE Policy Statement (November 2014) and principles of sustainable development, reduction of adverse effects of the company's activities on environment and human health, as well as constant improvement and an efficient environmental management system</td>
</tr>
<tr>
<td>2.1. G4 EN3: Energy consumption within the organization (GJ/day); ID-1249</td>
<td>Total energy consumption in joules or multiples</td>
</tr>
<tr>
<td>2.2. G4 EN21: Amount of air pollutant i.e. SO2 emitted (tons/day); ID-1255</td>
<td>The operation of process units, boilers in Power Plants of Pančevo Oil Refinery and Novi Sad Oil Refinery is primarily based on combustion of fossil fuels: petroleum products and natural gas. During these processes the formation of NOx, SO2, and particulate matter (PM) and air emissions occurs. NIS, being committed to sustainable development and meeting the requirements of legislation, seeks, through best management practices, to contribute fully to environmental protection</td>
</tr>
<tr>
<td>2.3. G4 LA6: Number of lost days/year; ID-1263</td>
<td>Lost working days due to work related injuries</td>
</tr>
<tr>
<td>2.4. Number of HSE training/year; ID-2305</td>
<td>In 2015, three main directions of improvement were referenced: improvement of the quality of investigations of events, increased participation of managers in site visits and increased communication with the employees on safe and unsafe activities, raising awareness and improving knowledge of the employees of basic risks that surround them in every day work, in order to help them perceive and recognise these risks</td>
</tr>
<tr>
<td>3. Global/ international/ interconnectedness; ID-1271</td>
<td>Global interconnectedness of the critical infrastructures implies the interdependencies between Cis in different countries</td>
</tr>
<tr>
<td>3.1. Economic inoperability between the NIS Serbia and Angola (€/day); ID-1272</td>
<td>The economic dependency of the NIS Serbia plant on Angola plant</td>
</tr>
<tr>
<td>3.2. Exports (thousand tons/day); ID-2306</td>
<td>Export of oil products sold in thousand tons</td>
</tr>
<tr>
<td>4. SOCIAL/SOCIETAL performance; ID-1281</td>
<td>The social dimension of sustainability concerns the impacts the organization has on the social systems within which it operates</td>
</tr>
<tr>
<td>4.1. Percentage of employees present per shift; ID-2309</td>
<td>Percentage of employees intended to work/actual number present per shift</td>
</tr>
<tr>
<td>5. SECURITY: Security system performance; ID-1239</td>
<td></td>
</tr>
</tbody>
</table>

*Note: BLEVE stands for “Boiling Liquid Exothermic Vapor Explosion.”*
### Dynamic Checklist - Functionality Level

**Smart Industrial zone in the City of Pančevo affected by a hypothetical BLEVE**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1. The number of activations of safety equipment; ID-2101</td>
</tr>
<tr>
<td>6. ECONOMY: Economic performance; ID-1242</td>
</tr>
<tr>
<td>6.1. Total income from all activities (€); ID-2191</td>
</tr>
<tr>
<td>6.2. Price per share; ID-2304</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the number of times per year a certain safety equipment has been activated to prevent accidents. This indicates possible deviations in the process which should be paid attention to</td>
</tr>
<tr>
<td>The economic dimension of resilience of the CI concerns the economic status of the organization. It helps in understanding not just the current state but also the impact of a disruption on the performance of the CI in the short and long-term</td>
</tr>
<tr>
<td>Total income from all activities (€)</td>
</tr>
<tr>
<td>Price of NIS j.s.c. Novi Sad per share on the Belgrade Stock Exchange [RSD]</td>
</tr>
</tbody>
</table>

### Dynamic Checklist - Resilience Level

**Energy supply system in Helsinki affected by fire**

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.1. Societal and political risk; ID-2331</td>
</tr>
<tr>
<td>I.2. Incident frequency; ID-2321</td>
</tr>
<tr>
<td>I.3. Fire risk assessment; ID-2322</td>
</tr>
<tr>
<td>I.4. Management review of risk assessment; ID-2323</td>
</tr>
<tr>
<td>I.5. Reports and complaints on incidents; ID-2324</td>
</tr>
<tr>
<td>I.5.1. Was the annual assessment of external reports &amp; complaints conducted?; ID-911</td>
</tr>
<tr>
<td>I.5.2. Number of external reports &amp; complaints on incidents?; ID-910</td>
</tr>
<tr>
<td>II.1. Sensitivity to ignition; ID-3490</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This issue is describing the status of societal and political risk assessment and in comparison with the last assessment</td>
</tr>
<tr>
<td>This issue describes how often the incident is or has been occurring</td>
</tr>
<tr>
<td>This issue is describing the status of conducted fire risk assessment</td>
</tr>
<tr>
<td>This issue is describing the status of conducted management review of the risk assessment</td>
</tr>
<tr>
<td>This issue gives the status of observed written or oral descriptions, opinions or complaints on the incidents, and conducted assessment of those</td>
</tr>
<tr>
<td>This indicator describes whether the annual assessment of external reports &amp; complaints on incidents</td>
</tr>
<tr>
<td>Number of external reports &amp; complaints on incidents</td>
</tr>
<tr>
<td>This issue describes the stored fuel sensitivity to self-ignition</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>II.1.1. How long was the batch stored that initiated fire?; ID-912</td>
</tr>
<tr>
<td>II.1.2. Is high fuel temperature being indicated?; ID-914</td>
</tr>
<tr>
<td>II.1.3. Is sensitive fuel quality indicated for the batch?; ID-915</td>
</tr>
<tr>
<td>II.2. Communication; ID-1046</td>
</tr>
<tr>
<td>II.2.1. Are there sufficient guidelines for internal and external communication?; ID-2366</td>
</tr>
<tr>
<td>II.2.2. Review of communication policy conducted?; ID-919</td>
</tr>
<tr>
<td>II.3. Sensor checking; ID-2329</td>
</tr>
<tr>
<td>II.3.1. Have sensors been checked and calibrated according to guidelines?; ID-916</td>
</tr>
<tr>
<td>II.4. Management review of plans and protocols; ID-2330</td>
</tr>
<tr>
<td>II.4.1. Review of contingency protocols conducted?; ID-922</td>
</tr>
<tr>
<td>II.4.2. Management review of continuity plan conducted?; ID-917</td>
</tr>
<tr>
<td>III.1. Storage time of overheated batch(es); ID-2325</td>
</tr>
<tr>
<td>III.1.1. How long was the batch stored that initiated fire?; ID-912</td>
</tr>
<tr>
<td>III.2. Odour detection; ID-2326</td>
</tr>
<tr>
<td>III.2.1. Is the operator detecting a fire odour?; ID-913</td>
</tr>
<tr>
<td>III.3. Fuel redirecting experience; ID-2364</td>
</tr>
<tr>
<td>III.3.1. Is the fuel redirecting experience satisfactory?; ID-921</td>
</tr>
<tr>
<td>III.4. Switch of fuel source; ID-2337</td>
</tr>
</tbody>
</table>
### Dynamic Checklist - Resilience Level

**Energy supply system in Helsinki affected by fire**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boilers</td>
<td></td>
</tr>
<tr>
<td>III.4.1. Number of alternative silos available; ID-2338</td>
<td>This indicator describes how many alternative coal silos are available as a source of fuel</td>
</tr>
<tr>
<td>III.4.2. Is the fuel oil storage available?; ID-2339</td>
<td>This indicator describes whether the fuel oil storage is available</td>
</tr>
<tr>
<td>III.4.3. Is fuel from the coal storage of another plant available?; ID-2340</td>
<td>This indicator describes the availability of fuel from the coal storage of another plant</td>
</tr>
<tr>
<td>III.5. Sensitivity to ignition; ID-2327</td>
<td>This issue is describing the stored fuel sensitivity to self-ignition</td>
</tr>
<tr>
<td>III.5.1. Is high fuel temperature being indicated?; ID-914</td>
<td>This indicator measures the temperature rating of the fuel being transported or residing in the storage</td>
</tr>
<tr>
<td>III.6. Redirecting heated fuel to combustion; ID-2363</td>
<td>This issue describes the frequency of fuel directing incidents</td>
</tr>
<tr>
<td>III.6.1. What is the frequency of redirecting heated fuel to combustion?; ID-920</td>
<td>Number of fuel redirecting incidents/year</td>
</tr>
</tbody>
</table>

### IV. Respond/recover

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV.1. Extinguishing efforts; ID-2355</td>
<td>This issue describes the number of fires extinguished yearly</td>
</tr>
<tr>
<td>IV.1.1. How many fires were extinguished?; ID-923</td>
<td>Number of extinguished fires/year</td>
</tr>
<tr>
<td>IV.2. Incidents requiring alternative fuel; ID-2356</td>
<td>This issue describes frequency of incidents when alternative fuel was needed</td>
</tr>
<tr>
<td>IV.2.1. How many incidents required alternative fuel?; ID-924</td>
<td>Yearly number of fire incidents that required alternative fuel, e.g. coal from another silo, oil or coal from another plant storage</td>
</tr>
<tr>
<td>IV.3. Time to extinguish fire; ID-2367</td>
<td>This issue describes how long it took to extinguish fire</td>
</tr>
<tr>
<td>IV.3.1. How long did it take to extinguish the fire?; ID-925</td>
<td>This indicator measures how long did it take to extinguish the fire</td>
</tr>
<tr>
<td>IV.4. Performance assessment of responses/recovery; ID-2358</td>
<td>This issue describes whether the status of performance assessment on responses and recovery phase</td>
</tr>
<tr>
<td>IV.4.1. Performance assessment of responses / recovery measure conducted?; ID-926</td>
<td>This indicator describes whether the performance assessment of the measure undertaken for the responses and recovery have been conducted</td>
</tr>
<tr>
<td>IV.5. System unavailability due to fire; ID-2353</td>
<td>This issue describes the level of system unavailability due to fire</td>
</tr>
<tr>
<td>IV.5.1. Percentage of system unavailability; ID-933</td>
<td>This indicator measures the yearly system unavailability due to fires</td>
</tr>
<tr>
<td>IV.6. Time to restore functionality; ID-2362</td>
<td>This issue describes the response time to restore the useful functionality</td>
</tr>
<tr>
<td>IV.6.1. Time to restore district heating; ID-3518</td>
<td>Time to restore district heating</td>
</tr>
</tbody>
</table>
A.2.4 DCL for Functionality Level Assessment of the HOTEL case

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CORE: District heat production and supply in the western district; ID-2343</td>
<td>This element describes the level of thermal production and supply for district heating in the western district, Helsinki</td>
</tr>
<tr>
<td>1.1. Supply to percent of customers in western district (experienced by customer); ID-2408</td>
<td>Percent of customers supplied with district heating in western district</td>
</tr>
<tr>
<td>1.2. Production for district heating (percentage of the full normal capacity); ID-2344</td>
<td>Percentage of the required thermal supply in western district for the district heating system</td>
</tr>
</tbody>
</table>
### A.2.5 CORE DCL consisting of generic issues recommended for all cases

<table>
<thead>
<tr>
<th>Dynamic Checklist - Resilience Level General</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>I. Understand risks</strong></td>
</tr>
<tr>
<td>I.1. Risk management; ID-3873</td>
</tr>
<tr>
<td>I.2. Future scanning and smartness related challenges; ID-3874</td>
</tr>
<tr>
<td>I.3. Threat monitoring; ID-3889</td>
</tr>
<tr>
<td><strong>II. Anticipate/prepare</strong></td>
</tr>
<tr>
<td>II.1. Site integrity; ID-3877</td>
</tr>
<tr>
<td>II.2. Use of smart technologies for safety and security; ID-3887</td>
</tr>
<tr>
<td>II.3. Threat monitoring; ID-3889</td>
</tr>
<tr>
<td>II.4. Internal and external resource planning; ID-3890</td>
</tr>
<tr>
<td>II.5. Business continuity arrangements, including cyber (CORE); ID-3898</td>
</tr>
<tr>
<td>II.6. Training (CORE); ID-3899</td>
</tr>
<tr>
<td>II.7. Emergency planning; ID-3900</td>
</tr>
<tr>
<td>Dynamic Checklist - Resilience Level</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>1. Pre-planned crisis organization, internal and external resources, emergency response functions and tasks, general instructions and procedures for each phase, action plans for defined scenarios, procedures for alert, mobilization and communication, various checklists to be used, etc.</td>
</tr>
</tbody>
</table>

### III. Absorb/withstand

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.1. Offsite/external capabilities and resources availability; ID-3834</td>
<td>Resources pre-identified, in particular, to ensure the maintenance of an organization’s essential activities. These may be provided in their entirety by an offsite physical resource or, alternatively, provision for key resources may be arranged separately. This may include, but not be limited to: water, electricity/gas, ICT networks/hardware/software, office equipment, hygiene requirements, etc.</td>
</tr>
<tr>
<td>III.2. First Preventer/Responder available and effective; ID-3836</td>
<td>An effective multi-agency response to a serious or major incident, particularly by relevant first responders (this varies by country but, in general, police, fire, health, ambulance, local authority, etc) is critical to mitigate risk, preserve life, protect property and maintain essential activities. The effectiveness of any multi-agency response is dependent on a range of capabilities, including physical communications, shared and agency protocols, mutual knowledge and understanding, etc, which are generally developed through multi-agency training and exercising.</td>
</tr>
<tr>
<td>III.3. Use of smart CI related procedures and protocols; ID-3866</td>
<td>The organization must take into consideration the connectedness of its (smart) infrastructure and maintain a set of procedures to ensure its protection in this regard. For example, ICT access control through secure protocols, verified sources/files, etc. This issue refers to the communication held between different smart infrastructures and how to monitor and prevent breaching and exploiting it.</td>
</tr>
<tr>
<td>III.4. Business continuity protocols and procedures, including cyber; ID-3878</td>
<td>The critical infrastructure shall create a business continuity plan for ensuring the infrastructure’s performance before, during and after an adverse event. It shall establish documented procedures for responding to a disruptive incident and define how it will continue and/or recover its activities within a predetermined time frame. Such procedures shall address the requirements of those who will use them.</td>
</tr>
<tr>
<td>III.5. Physical Protection, monitoring analysis; ID-3879</td>
<td>Detection, delay, and response are required functions of an effective physical protection. The total time for detection and response must be less than the time remaining (delay) for the adversary to complete his task after the first sensing. An effective PP has several specific characteristics. A well-designed system provides defence in depth, exhibits balanced protection, and minimizes the consequence of component failures. A design process based on performance criteria rather than feature criteria will select elements and procedures according to the contribution they make to overall system performance. Performance of the technology elements contributing to the functions of detection, delay, and response will vary based on numerous factors: the component design, unit to unit differences in a specific component due to manufacturing inconsistencies, installation, maintenance, environmental factors influencing component operation, the specific adversary threat, and specific tactics used by an adversary. Protection monitoring is defined as ‘systematically and regularly collecting, verifying and analysing information over an extended period of time in order to identify violations of rights and protection risks for subject of concern for the purpose of informing effective responses. The output of protection monitoring systems are: quantitative and qualitative data and information on the protection environment, protection trends over time, rights violations, and/or risks - threats, vulnerabilities, and capacities - of the affected population. Data needed for decision-making: protection risks, protection needs, capacities and coping strategies, life-saving assistance or immediate support needed, trends for what the monitoring systems.</td>
</tr>
</tbody>
</table>
### Dynamic Checklist - Resilience Level

#### General

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.6. Emergency management protocols and procedures; ID-3880</td>
<td>Emergency management protocols are to be implemented when specific site-based emergencies and/or serious disruptions arise. Emergency Response Team will need to make early judgments regarding the seriousness of a developing situation and the steps to take until assistance arrives. An emergency is a serious, unexpected, often dangerous situation that requires immediate action. The emergency procedure is a plan of actions to be conducted in a certain order or manner, in response to an emergency event.</td>
</tr>
<tr>
<td>III.7. Command and control structure validated and clearly understood; ID-3881</td>
<td>During an adverse/disruptive event, the command structures must be available and effective, throughout the resilience cycle but primarily during the absorb/recover phases.</td>
</tr>
<tr>
<td>III.8. Internal response resources fully available for the duration of the event; ID-3882</td>
<td>Are the required resources for on-site response fully available to the responders? Both immediate and long term. e.g. budget for over hours during long events.</td>
</tr>
</tbody>
</table>

#### IV. Respond/recover

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV.1. Emergency response; ID-996</td>
<td>Emergency response is needed to ensure appropriate response is undertaken during an emergency situation. The response mechanisms require various organizational measures such as planning, following procedures, designated control centres to ensure operations during an emergency, personnel assigned to contact during emergency, regular drills to improve preparedness, etc.</td>
</tr>
<tr>
<td>IV.2. Management of resilience information/knowledge, including adequate HR; ID-3823</td>
<td>Persons working under the organization’s control should have appropriate awareness aspects such related to organizational resilience and the business continuity management systems (BCMS). Such persons may include staff, contractors, partners, suppliers. They should conduct activities to create awareness about incident prevention, detection, mitigation, self-protection, evacuation, response, continuity and recovery; the importance of conformity with business continuity policy and procedures; the implications to BCM of changes in the operation of the organization including the benefits of improved business continuity management performance; to achieve conformity with the requirements of the BCMS and reporting of potential hazards or threats. Further, organizational resilience is enhanced when knowledge is widely shared and effectively communicated where appropriate and applied. Learning from experience and learning from each other is encouraged. The organization can demonstrate and enhance the exchange/sharing of information and knowledge, as well as learning.</td>
</tr>
<tr>
<td>IV.3. Impact of dependencies on resilience; ID-3835</td>
<td>The critical infrastructure should acquire knowledge about important dependencies on other infrastructures as they can be very easily impacted by the disruption in another infrastructure. Identifying dependencies and supporting resources for CI operations, including suppliers, outsource partners and other relevant interested parties is required to ensure appropriate better understanding of risk in particular while responding and recovering from an adverse event.</td>
</tr>
<tr>
<td>IV.4. Incident management plans and procedures and monitoring their effectiveness; ID-3883</td>
<td>The presence, comprehensiveness and quality of incident management plans and procedures as needed to adequately address adverse events (incidents, accidents, disasters) should be checked. Said provisions have to be maintained and updated if need be, which is why effectiveness of plans and procedures shall be monitored specifically during adverse events in order to maximize the instructional benefit from real world strain.</td>
</tr>
<tr>
<td>IV.5. Offsite/external capabilities, support activities and resource availability; ID-3884</td>
<td>Energy, water and/or other relevant resources available to first responders at offsite/external location.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>IV.6. Real-time monitoring and information sharing; ID-3885</td>
<td>Information Sharing based on ISO 22396 seeks to create mechanisms for information exchange by which a participating organization can learn from other’s experiences, mistakes and successes. It can be used to guide the maintenance of the information exchange arrangement in order to increase commitment and engagement. It provides measures that enhances the participating organizations capability to cope with disruption risk. In terms of information technology used to collect and share the data, a combination of various data types is often necessary to monitor and detect events. These sources used for monitoring (often in real-time) include social media, sensor webs and IoT, satellite data, spatial data, Lidar, mobile GPS data, as well as crowdsourcing (e.g. using citizens and their smartphones as sensors).</td>
</tr>
<tr>
<td>IV.7. Allocating sufficient recovery resources; ID-1820</td>
<td>(ID: SCADA.O)</td>
</tr>
<tr>
<td>IV.8. Cyber operation continuity plan; ID-3886</td>
<td>The critical infrastructure shall create a cyber operation continuity plan for ensuring the infrastructure’s performance before, during and after an adverse event. It shall establish documented procedures for responding to a disruptive incident and define how it will continue and/or recover its activities within a predetermined time frame. Such procedures shall address the requirements of those who will use them.</td>
</tr>
</tbody>
</table>

**V. Adapt/transform**

<p>| V.1. Incident investigation; ID-1004 | Incident investigation is crucial to understand the reasons for an incident/event. The procedures for incident investigation such as post-incident/near misses evaluation could help in better recovery and response plans. Also, providing training to the employees in incident investigation procedures could help in ensuring preparedness and ability to even anticipate the risks and vulnerability. Furthermore, the investigation results may help in learning from the incidents and adapting measures for future mitigation. |
| V.2. Emergency response reporting including lessons learned; ID-3826 | Emergency response report is an &quot;after-action&quot; report. It summarizes the system information including overview of the emergency, detailed timeline of the incident and response, evaluation of emergency situation, recommendations for improvement to emergency response planning, training and communication, timeline for making the recommended changes, updated emergency response plan and also compliance aspects. |
| V.3. Management of resilience information/knowledge, including adequate HR; ID-3823 | Persons working under the organization’s control should have appropriate awareness aspects such related to organizational resilience and the business continuity management systems (BCMS). Such persons may include staff, contractors, partners, suppliers. They should conduct activities to create awareness about incident prevention, detection, mitigation, self-protection, evacuation, response, continuity and recovery; the importance of conformity with business continuity policy and procedures; the implications to BCM of changes in the operation of the organization including the benefits of improved business continuity management performance; to achieve conformity with the requirements of the BCMS and reporting of potential hazards or threats. Further, organizational resilience is enhanced when knowledge is widely shared and effectively communicated where appropriate and applied. Learning from experience and learning from each other is encouraged. The organization can demonstrate and enhance the exchange/sharing of information and knowledge, as well as learning. |
| V.4. Improving smart CI related protection capacity; ID-3869 | |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.5. Organizational learning and continual improvement; ID-3848</td>
<td>Knowledge management and knowledge sharing at all levels of the organization. Lessons learned from past performance with implementation throughout the organization and its effective adoption monitored. Corrective actions monitoring with feedback to management planning. This issue is relevant for the ability of an organization to prevent future recurring failures and to continually improve through learning.</td>
</tr>
<tr>
<td>V.6. Business continuity arrangements, including cyber; ID-3875</td>
<td>The critical infrastructure shall create a business continuity plan for ensuring the infrastructure’s performance before, during and after an adverse event. It shall establish documented procedures for responding to a disruptive incident and define how it will continue and/or recover its activities within a predetermined time frame. Such procedures shall address the requirements of those who will use them.</td>
</tr>
</tbody>
</table>