Chapter

Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach

Aleksandar S. Jovanovic, Somik Chakravarty and Marjan Jelic

Abstract

The paper proposes a concept enabling quantitative assessment of resilience in critical entities developed in the European projects SmartResilience and InfraStress. The concept aims at combining simple communication-related advantages of simplified assessments results (such as "resilience very high" or "resilience very low") with the advantages of the in-depth assessments (e.g. analysis of multiple sensor data). The paper describes the main elements of the innovative, indicator-based concept, starting with the "resilience cube" at the top, and continuing with the multi-level, hierarchical, indicator-based assessment methodology. The concept allows analyzing and assessing different aspects of practical resilience management. One can assess the resilience level of an entity at a given point in time, monitor their resilience level over time and benchmark it. One can also model and analyze the functionality of a system during a particular (threat) scenario, as well as stress-test it. The same methodology allows to optimize investment in improving resilience (e.g. in further training, in equipment, etc.), in a transparent and intuitive way. A resilience indicator database (over 4,000 indicators available) and a suite of tools (primarily developed within SmartResilience and InfraStress projects) and a repository of over 20 application cases and 300 scenarios, support application of the methodology. The concept has been discussed and agreed with over 50 different organizational stakeholders and is being embedded into the new ISO 31050 standard currently under development. Its "life-after-the-project" will be ensured by the dedicated "resilience rating initiative (ERRA)". Although the concept and the tool in the form of the "ResilienceTool" were developed primarily for the resilience assessment of critical infrastructure (the "smart" ones in particular), they can be used for resilience assessment of other systems and through the extension of the, already initiated, implementation of AI techniques (machine learning) to make the ResilienceTool even more versatile and easier to use in the future.

Keywords: resilience, risk assessment, critical infrastructure, resilience indicators, risk and resilience

1. Introduction: using indicators to assess and manage resilience of critical infrastructures in SmartResilience and InfraStress projects

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 behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making an existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Which aspect of resilience of a critical infrastructure will be affected the most? Its ability to anticipate, to prepare for, to adapt and withstand, respond to, or to recover? What are the resilience indicators (RIs) which one has to look at? These are the main questions tackled by the SmartResilience project [1] to which a methodology based on resilience indicators was developed, complete with the supporting "ResilienceTool" to handle both existing ("conventional") indicators suitable for assessing the resilience of critical infrastructure as well as new "smart" resilience indicators, e.g. those from Big Data (over 5,000 available in mid-2020). In the InfraStress project [2], the concept and the tools are developed further and integrated with the concept of situational awareness system (focus of the InfraStress project).

2. Resilience as "one number", ResilienceCube and the main concept

2.1 Resilience and resilience matrix

The definition of resilience, standing in the background of the concept presented in this paper, has evolved along with the work on the development of the concept. It started with the definition of the resilience as *"The ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption".* The main amendment proposed afterward was the inclusion of the ability to understand risks (current and emerging), leading to the definition of *"Resilience as the ability to understand risks, anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruption"* [3]. In the final stage, the project adopted the elaborated definition of the resilience of an infrastructure is given below [4].

"*Resilience of an infrastructure is the ability to understand and anticipate the risks – including new/emerging risks – threatening the critical functionality of the infrastructure, prepare for anticipated or unexpected disruptive events, optimally absorb/withstand their impacts, respond and recover from them, and adapt/transform the infrastructure or its operation based on lessons learned, thus improving the infrastructure anti-fragility*."

This definition enabled the following main advantages:

- Including emerging risks and a natural link to risk assessment
- Including the goals of optimization, adaptation and transformation and
- Including the improvement of anti-fragility, the concept of increased importance for all smart systems, including smart infrastructures, and
- Enabling inclusion of the 5 phases of the resilience cycle and the indicator-based approach within the resilience matrix.

The definition allows analyzing the behavior of an infrastructure exposed to an adverse event over a "scenario timeline" and simultaneously assessing the functionality of an infrastructure over the "resilience cycle" as shown in **Figure 1**. While the decomposition over the time-axis, i.e., defining the "phases" of the resilience cycle, may be trivial, decomposition over the functionality axis is non-trivial as functionality might have different "dimensions" (see chapter 2.3). The SmartResilience concept proposes the decomposition over a 5 × 5 resilience matrix, defining 5 phases and 5 "dimensions".

The approach allows to represent the overall resilience cycle, and focus on single relevant issues. The issues, in turn, can be described by means of indicators and these can have values, thus, providing the possibility to quantitatively describe each "cell" of the resilience matrix (**Figure 2**).

Phase I, understand risks, is applicable prior to an adverse event. It emphasizes emerging risks and includes their early identification and monitoring; e.g. what could the "adverse event" be? This is followed by.

Phase II, anticipate/prepare, also applicable before the occurrence of an adverse event. It includes planning and proactive adaptation strategies, possibly also "smartness in preparation" [5].

Phase III, absorb/withstand, comes into action during the initial phase of the event and shall include the vulnerability analysis and the possible cascading/ripple effects; e.g. "how steep" is the absorption curve, and "how deep" down will it go?

Phase IV, respond/ recover, is related to getting the adverse event under control as soon as possible, influencing the "how long" will it last, question. Further, it

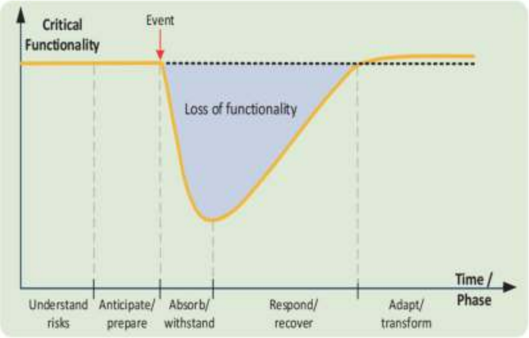


Figure 1.
The 5 × 5 resilience matrix, mapping the critical infrastructure system functionality over 5 phases of the resilience cycle.

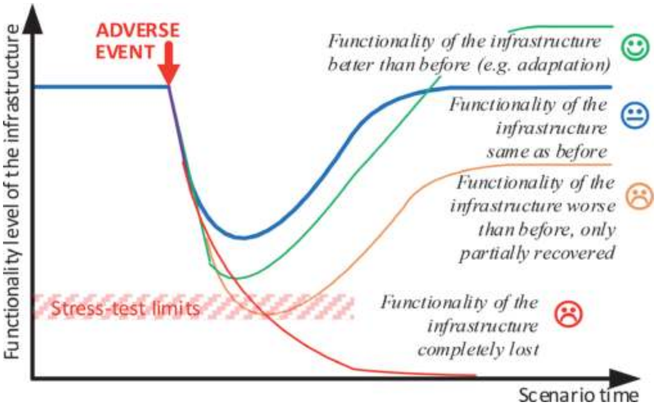

Functionality level of the infrastructure
ADVERSE EVENT
Functionality of the infrastructure better than before (e.g. adaptation)
Functionality of the infrastructure same as before
Functionality of the infrastructure worse than before, only partially recovered
Stress-test limits
Functionality of the infrastructure completely lost
Scenario time

Figure 2.
Possible outcomes of case of an infrastructure exposed to an adverse event: Between improvement and complete failure.

includes the post event recovery; e.g. "how steep up" is the recovery curve for normalization of the functionality? It is followed by.

Phase V, adapt/learn, which encompass all kinds of improvements made on the infrastructure and its environment; e.g. affecting "how well" the infrastructure is adapted after the event, and whether it is more resilient and "sustainable". The activities in this phase also lead to preparation for future events and hence, this resilience curve also exhibits a reoccurring cycle [5].

The dimensions help in categorizing the indicators. The system/physical dimension includes technological aspects, as well as the physical/technical networks being part of a given infrastructure, and the interconnectedness with other infrastructures and systems. The information/data dimension is related to the technical systems. The organizational/business dimension covers business-related aspects, financial and HR aspects as well as different types of respective organizational networks. The societal/political dimension encompasses broader societal and social contexts. Finally, the cognitive/decision-making dimension, accounts for perception aspects (e.g. perceptions of threats and vulnerabilities) [6].

2.2 Difference and relationship between a risk matrix and a resilience matrix

One should distinguish well between the risk matrix and the resilience matrix. Although similar in shape and appearance, their basic purpose and principles are different. The main purpose of a risk matrix is to show the position of a given risk (defined through its scenario) on a 2-dimensional "map", depicting the likelihood/probability of a given risk and its possible impact/consequences. Risk is then, for a given scenario, calculated as the product of the two. The higher the probability/likelihood, the higher the impacts/consequences – the higher the risk.

Risk-oriented standards (e.g. EN 16991:2018[1] [7]) provide detailed examples of how to use a risk matrix in given areas. Using a risk matrix (sometimes referred as "risk map"), one can easily compare e.g. two risks – provided that the likelihood/probabilities and impact/consequences can be assessed.

The resilience matrix, on the other hand, serves to map the resilience of a system (e.g. a critical infrastructure such as a large power plant) during an adverse event (e.g. crisis, accident, cyber-attack, etc.). The time of the event is then usually subdivided into phases (**Figure 3(a)**), usually 4 or 5, of the event, from the time before the very event to the time after the event (the "resilience cycle"). The time of the event/scenario (see also **Figure 4**) is thus, the first and the main dimension of the resilience matrix. As the adverse event, in a general case, will affect different areas of activities, e.g. business, society, information, management, etc. the event is usually looked at for each of them in terms of their own indicators. These areas are often (e.g. in EU projects such as InfraStress [2] or SmartResilience [1, 8–12]), called dimensions, and their number is usually chosen as equal to the number of phases. The result is then a matrix (the "resilience matrix", **Figure 3(a)**), mapping the resilience of the given system – e.g. suggesting the communication "dimension" in the response "phase" of the crisis management of COVID (e.g. in the UK[2]) was "poor" (**Figure 3(b)**).

In the approach presented here, we propose that the qualifier "poor" is linked to the measurable indicators (resilience indicators) such as e.g. reliability of numbers communicated to the public, statistic/sentiment in social media, survey results, etc. In such a case, the label "poor" is supported also by quantitative indicators and can be given an aggregated value (e.g. acc. to the value × weight formula).

[1] https://www.cen.eu/news/brief-news/pages/news-2018-011.aspx (Convener A. Jovanovic).

[2] https://reutersinstitute.politics.ox.ac.uk/communications-coronavirus-crisis-lessons-second-wave

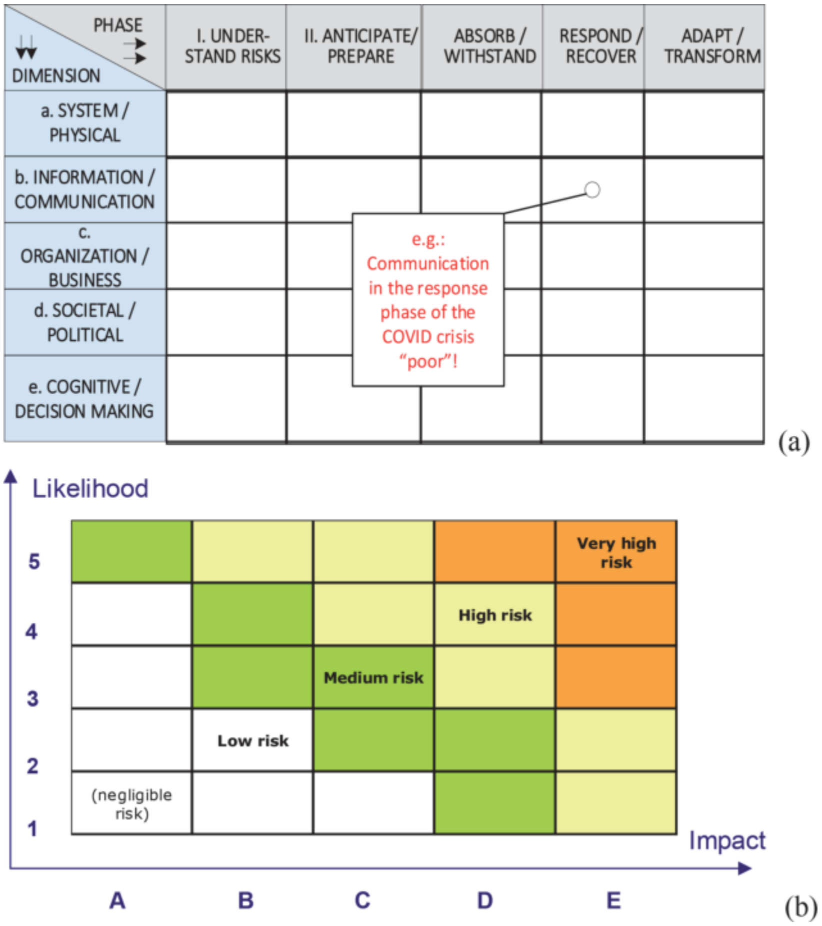


Figure 3.
Example of a 5x5 resilience matrix (a) as compared to a risk matrix (b).

Generally, the aggregation process for indicators in the method and the tool described (see **Figure 5**) here offer the following main aggregation options:

1. The simple aggregation of the indicators put on the common 0–5 scale

2. The weighted aggregation as an extension of the simple method

3. The JRC composite indicators and scoreboard (COIN) methodology[3]

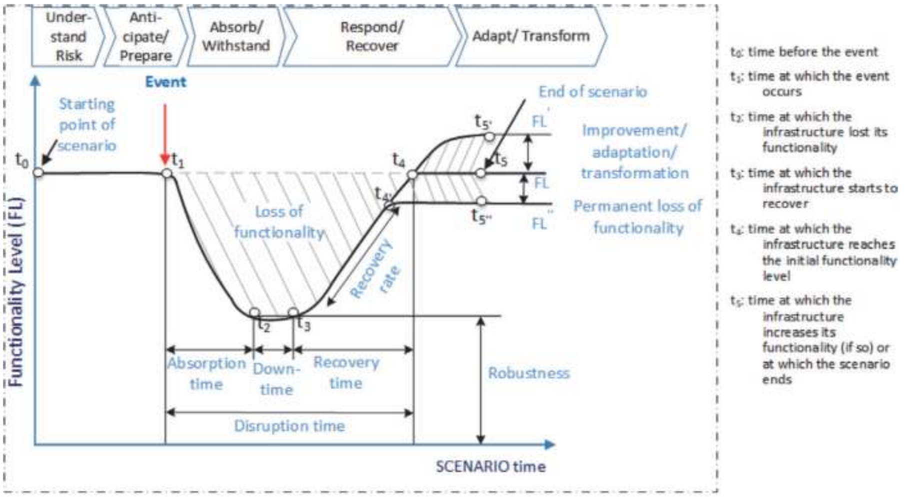
4. The Fuzzy-AHP based weight determination [13]

5. The ranking-based weight determination [11]

2.3 "Measuring" resilience by means of issues and indicators

In the concept, an "issue" is a general term referring to anything important in order to be resilient against severe threats such as terror attacks, cyber threats and extreme weather. It is telling what is important, e.g., it can be "training" performed in the anticipate/prepare phase. Obviously, the more indicators one chooses, the better the "coverage" of an issue is going to be (**Figure 5**), but it is also obvious that

[3] https://ec.europa.eu/jrc/en/publication/coin-tool-user-guide


Under-stand Risk
Anti-cipate/ Prepare
Absorb/ Withstand
Respond/ Recover
Adapt/ Transform
Event
Starting point of scenario
End of scenario
t_0
t_1
t_2
t_3
t_4
t_4'
t_5'
t_5
t_5''
FL
FL
FL
Improvement/ adaptation/ transformation
Permanent loss of functionality
Loss of functionality
Recovery rate
Absorption time
Down-time
Recovery time
Robustness
Disruption time
Functionality Level (FL)
SCENARIO time
t_0: time before the event
t_1: time at which the event occurs
t_2: time at which the infrastructure lost its functionality
t_3: time at which the infrastructure starts to recover
t_4: time at which the infrastructure reaches the initial functionality level
t_5: time at which the infrastructure increases its functionality (if so) or at which the scenario ends

Robustness (%)	$= \frac{FL_{t2}}{FL_{t0}} \times 100\%$	Recovery Time (t)	$= t_4 - t_3$
Absorption Time (t)	$= t_2 - t_1$	Recovery rate (%/t)	$= \frac{(FL_4 - FL_3)}{(t_4 - t_3)}$
Downtime (t)	$= t_3 - t_2$	Disruption time (t)	$= t_4 - t_1$
Loss of functionality (%*t)	$= \int_{t_1}^{t_4} [FL_{t_1} - FL(t)]dt$	Improvement/adaptation/ transformation (%)	$= \frac{FL_{t5} - FL_{t0}}{FL_{t0}} \times 100\%$

Figure 4.
Functionality level of the smart critical infrastructure over scenario time – The value of the FL at a particular time is calculated by aggregating the relevant indicators scores starting from FL at t_o = 100%.

the larger the number of indicators, the more complex their handling is going to be. The "way out" has two components and these would be:

- finding the "right number" of indicators acc. to the resilience problem tackled (in the usual engineering practice, managed by humans, 120–150 indicators are usually a maximum – the more critical the situation, the smaller the number; in absolute emergency situations humans can hardly look at more than 3 indicators), and

- allowing to "drill-down" in cases when one or more indicators need further explanation.

In order to organize the analysis and enable drilling down to the base assessment elements, the selected scenario is segmented into six levels [1]. This practice is based on several previous methods, notably the ANL/Argonne method [14], the Leading Indicators of Organizational Health (LIOH) method [15–17], the US-DHS method [18], and the Resilience-based Early Warning Indicator (REWI) method [19]. The ANL/Argonne method for assessing a resilience index (RI) is structured in 5 levels, providing indicators on the lowest level and a similar hierarchy is used in the SmartResilience and InfraStress projects for assessing resilience levels, entering the indicators on level six.

The "resilience indicators" are mainly taken from current practices (standards, guidelines, reports, etc.) within safety and risk management, emergency preparedness, business continuity, etc. and in most cases, they exist already as safety indicators, risk indicators, or similar (e.g. those proposed by OECD, GRI, API, HSE, IAEA and other organizations). Collecting the indicators and applying the approach, the theoretical framework for variable selection, weighting, and aggregation must be defined [20] and the basis for this is the context of the assessment, or scenario. An example of a "resilience indicator data sheet" is given Appendix 1.

The values of indicators, often for one and the same indicators, can come from experts (e.g. as qualifiers – "high", "very low"", etc.), from measured or monitored

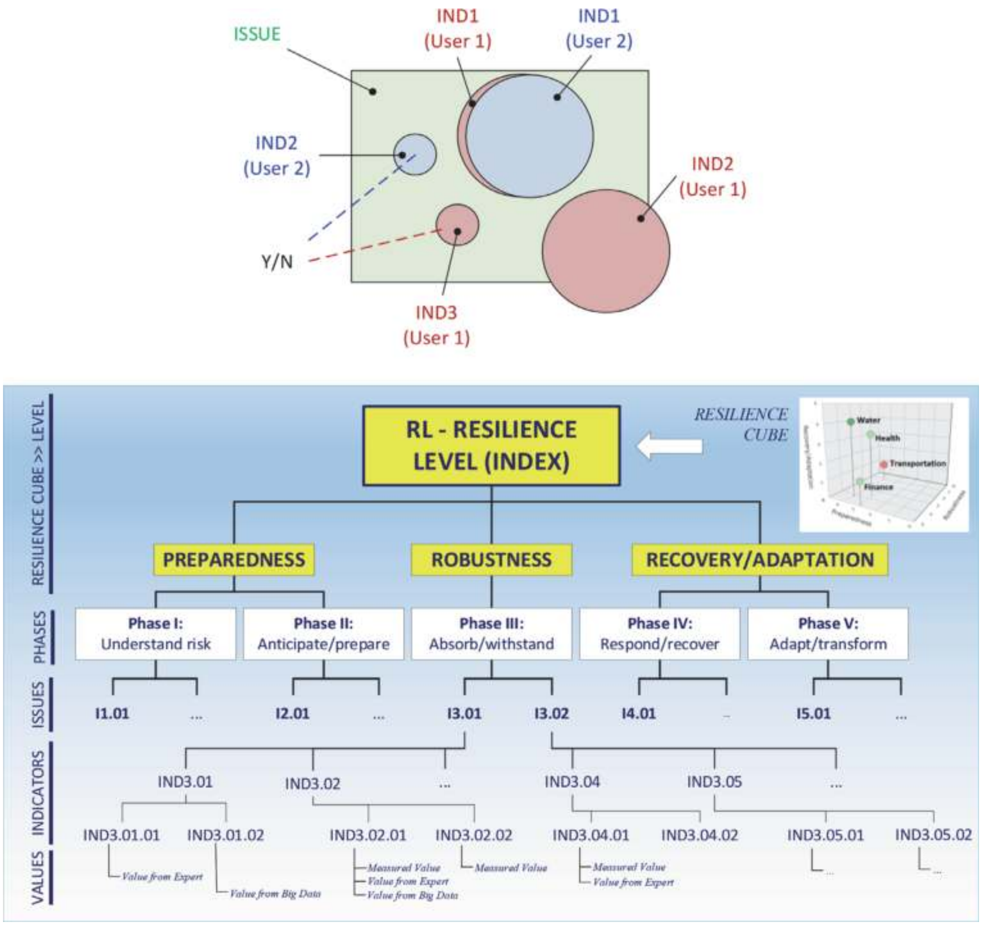


Figure 5.
Issues measured by indicators (above), allow to make the bridge between a given, e.g. measured value of an indicator, and the overall, final resilience index & ResilienceCube (below).

values (e.g. numbers of accidents), or from big data analysis. Single, real values, from any of the above sources, in the methodology, can be yes/no questions, numbers, percentages, fuzzy numbers, or some other type. Once in the model, for the communication with the end-user, they are, in a general case, transferred into the score, on a scale 0 to 5.

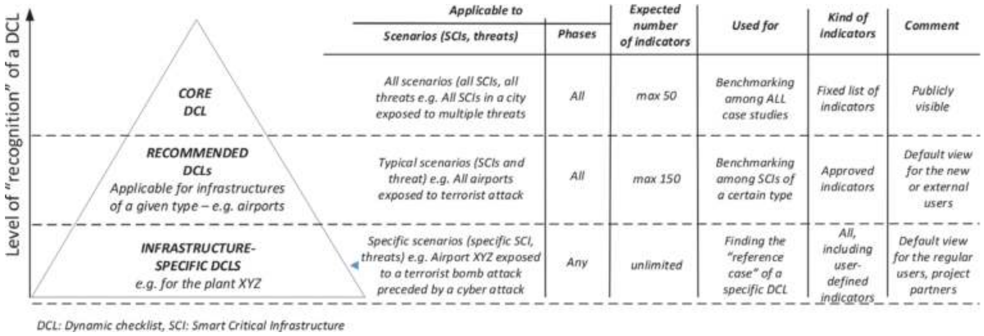
2.4 Dynamic checklists of resilience issues and indicators

One of the ways to use resilience issues and indicators practically [21], is to put them into "lists" (checklist) and in the concept it is done in a dynamic way, allowing to dynamically create checklist appropriate for a given case using available indicators or adding new ones to the list. In order to make the creation/drafting of these dynamic checklists (DCLs) easier and allow for comparison and benchmarking of results, the user is encouraged to use the list suggested by the concept, namely (**Figure 6**):

- The CORE DCLs, containing the indicators suggested for virtually all infrastructures,

- The RECOMMENDED DCLs, containing indicators suggested for the particular type of infrastructures and

- The USER's DCL, containing indicators specific for a particular infrastructure.



	Applicable to		Expected number of indicators	Used for	Kind of indicators	Comment
	Scenarios (SCIs, threats)	Phases				
CORE DCL	All scenarios (all SCIs, all threats e.g. All SCIs in a city exposed to multiple threats	All	max 50	Benchmarking among ALL case studies	Fixed list of indicators	Publicly visible
RECOMMENDED DCLs Applicable for infrastructures of a given type – e.g. airports	Typical scenarios (SCIs and threat) e.g. All airports exposed to terrorist attack	All	max 150	Benchmarking among SCIs of a certain type	Approved indicators	Default view for the new or external users
INFRASTRUCTURE-SPECIFIC DCLS e.g. for the plant XYZ	Specific scenarios (specific SCI, threats) e.g. Airport XYZ exposed to a terrorist bomb attack preceded by a cyber attack	Any	unlimited	Finding the "reference case" of a specific DCL	All, including user-defined indicators	Default view for the regular users, project partners

DCL: Dynamic checklist, SCI: Smart Critical Infrastructure

Figure 6.
Hierarchical structure of the checklist in the concept.

2.5 Assessing resilience an infrastructure during an adverse event: Functionality level (FL)

The indicator-based approach is proposed by the SmartResilience and InfraStress projects also for modeling of the behavior of the infrastructure during a particular disruptive event (scenario). In this case, the (critical) functionality of an infrastructure is analyzed during scenario time (**Figure 2**). No matter how intuitively one might say that the critical functionality of an infrastructure is easy to define, in practice, especially quantitative terms, it is not. E.g., the functionality of an airport is to "keep the air traffic going" or that the critical functionality of a refinery is "to produce the gasoline", but these are often difficult to measure. E.g., in the air traffic, one can look at the number of passengers boarding and/or on cargo throughput, but should at the same time look at the compliance with, e.g., safety and environmental norms, because not satisfying the latter could also be a loss of critical functionality. In the concept, these are considered to be

- The ELEMENTS of the functionality (corresponding to the "issues"), and for this one can define

- The (FUNCTIONALITY) INDICATORS, just as in the case of resilience level assessment.

Defining the functionality in the above way enables to precisely and quantitatively define the resilience curve in scenario time, e.g. for the main characteristic points in time [22]:

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.

Based on the resilience curve (or functionality curve), it is then possible to define the resulting macro-indicators, as illustrated in the notional diagram in **Figure 4**, such as:

- Robustness [%]

- Absorption time [h]

- Downtime [h]
- Loss of functionality [% over h]
- Recovery time [h]
- Recovery rate [%]
- Disruption time [h]
- Improvement/adaptation/transformation [%]

It should be noted that these are the RESULTING macro-indicators, and not the INPUT indicators as the resilience indicators and functional indicators mentioned above. These macro-indicators can also be used for "stress-testing", in which case these can be compared with the critical thresholds (e.g. for the maximum loss of functionality, duration or a combination of these, etc.).

Robustness characterizes the absorbing capacity of the smart critical infrastructure [23]. NL uses robustness as defined by the National Infrastructure Advisory Council (NIAC) [24], i.e. "the ability to maintain critical operations and functions in the face of crisis" [25]. It can be seen as the protection and preparation of a system facing a specific danger. The objective of the robustness component is to identify measures that can help the system withstand or adapt to a hazard. It emphasizes the ability of an infrastructure to withstand the incident if the protective measures fail. It also integrates the capacity of the infrastructure to function in a degraded state. The importance of robustness is not necessarily defined by how the infrastructure continues to function in the face of an incident but rather by how it is able to continue to accomplish its mission and to provide its products and services through preventative measures, mitigation, or absorption capabilities [25]. Robustness is defined as the capacity of the smart critical infrastructure to endure the effects of a negative event and thereby absorb its impact. As shown in **Figure 4**, 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.

$$\text{Robustness} = \frac{FL_{t2}}{FL_{t0}} \times 100\% \tag{1}$$

Absorption time is defined as the time during which the smart critical infrastructure absorbs a disruptive event while the smart critical infrastructure undergoes a decrease in its functionality level. As illustrated in **Figure 4**, it is measured as the difference between t_2 and t_1.

$$\text{Absorption time} = t_2 - t_1 \tag{2}$$

Loss of functionality is the functionality of the smart critical infrastructure lost in a given threat situation. It is measured by the area of the curve (an approximation) between the time when the smart critical infrastructure starts to lose its functionality (t_1) to the time when it reaches the initial state (t_4) (see **Figure 4**). The approximation is done for the area above the curve to a well-defined shape, e.g. a triangle. The output would be the percentage loss of functionality in time [26, 27], e.g. losing 10% in 10 hours.

$$\text{Loss of functionality} = \int_{t_1}^{t_4} [FL_{t_1} - FL(t)]dt \tag{3}$$

FL in all the formulae (incl. Eq. (3), is calculated as the aggregated score on indicators, in the particular case of FL, as functionality indicators, such as those presented in the sample list in **Figure** 7).

Next in the scenario is the **recovery** state of the smart critical infrastructure. The concept of recovery explains the passage of an infrastructure's functionality from a degraded state to one of acceptable operation. This concept builds on the concept of robustness in that, if measures of robustness fail to fully prevent, mitigate, or allow the asset to absorb the damage event, recovery constrains the impacts of the event to keep the CI functional. For the purpose of modeling the impact of a disruptive event, **recovery** refers to the ability to not only return to acceptable operating levels but also to recover fully from the effects of an event [25] in the maximum allowable/acceptable recovery time (as described in the stress test methodology [12, 28]).

Downtime is defined as the time duration for which the system is not functional. In Ref. to critical infrastructures, this could apply if the CI stops functioning. In this case, the functionality level of the infrastructure remains below the **threshold level** of functionality [25]. It can be measured as the difference in time between t_3 and t_2 (see **Figure 4**).

$$\text{Downtime} = t_3 - t_2 \qquad (4)$$

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

Recovery time is defined as the time at which the smart critical infrastructure recovers from the disruptive event and gains its initial or desired functionality [23]. It can be measured as the time taken to recover the functionality level, i.e. the time between time t_3 and t_4.

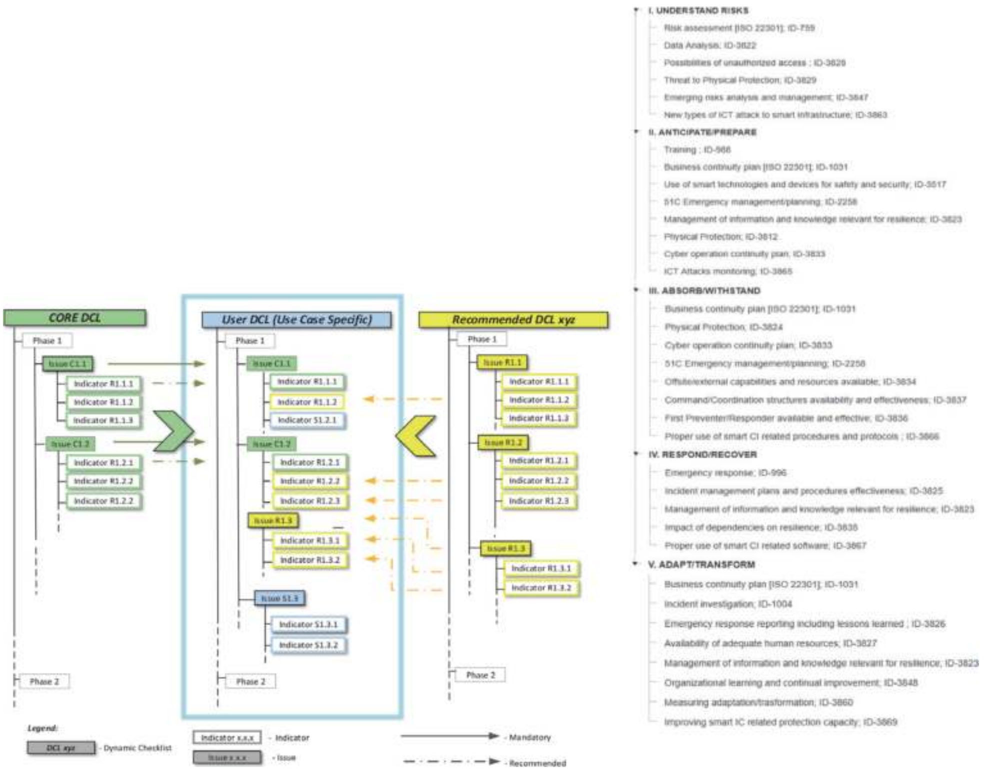

I. UNDERSTAND RISKS
Risk assessment [ISO 22301]; ID-755
Data Analysis; ID-3822
Possibilities of unauthorized access ; ID-3828
Threat to Physical Protection; ID-3829
Emerging risks analysis and management; ID-3847
New types of ICT attack to smart infrastructure; ID-3863
II. ANTICIPATE/PREPARE
Training ; ID-988
Business continuity plan [ISO 22301]; ID-1031
Use of smart technologies and devices for safety and security; ID-3817
51C Emergency management/planning; ID-2258
Management of information and knowledge relevant for resilience; ID-3823
Physical Protection; ID-3812
Cyber operation continuity plan; ID-3833
ICT Attacks monitoring; ID-3865
III. ABSORB/WITHSTAND
Business continuity plan [ISO 22301]; ID-1031
Physical Protection; ID-3824
Cyber operation continuity plan; ID-3833
51C Emergency management/planning; ID-2258
Offsite/external capabilities and resources available; ID-3834
Command/Coordination structures availability and effectiveness; ID-3837
First Preventer/Responder available and effective; ID-3836
Proper use of smart CI related procedures and protocols ; ID-3866
IV. RESPOND/RECOVER
Emergency response; ID-996
Incident management plans and procedures effectiveness; ID-3825
Management of information and knowledge relevant for resilience; ID-3823
Impact of dependencies on resilience; ID-3838
Proper use of smart CI related software; ID-3867
V. ADAPT/TRANSFORM
Business continuity plan [ISO 22301]; ID-1031
Incident investigation; ID-1004
Emergency response reporting including lessons learned ; ID-3826
Availability of adequate human resources; ID-3827
Management of information and knowledge relevant for resilience; ID-3823
Organizational learning and continual improvement; ID-3848
Measuring adaptation/trasformation; ID-3860
Improving smart IC related protection capacity; ID-3869
CORE DCL
User DCL (Use Case Specific)
Recommended DCL xyz
Phase 1
Issue C1.1
Indicator R1.1.1
Indicator R1.1.2
Indicator R1.1.3
Issue C1.2
Indicator R1.2.1
Indicator R1.2.2
Indicator R1.2.2
Phase 2
Issue C1.1
Indicator R1.1.1
Indicator R1.1.2
Indicator S1.2.1
Issue C1.2
Indicator R1.2.1
Indicator R1.2.2
Indicator R1.2.3
Issue R1.3
Indicator R1.3.1
Indicator R1.3.2
Issue S1.3
Indicator S1.3.1
Indicator S1.3.2
Issue R1.1
Indicator R1.1.1
Indicator R1.1.2
Indicator R1.1.3
Issue R1.2
Indicator R1.2.1
Indicator R1.2.2
Indicator R1.2.3
Issue R1.3
Indicator R1.3.1
Indicator R1.3.2
Legend:
DCL xyz - Dynamic Checklist
Indicator x.x.x - Indicator
Issue x.x.x - Issue
- Mandatory
- Recommended

Figure 7.
Example of creating a DCL by combining generic (CORE DCL), typical (RECOMMENDED DCL) and specific issues/indicators into the final DCL.

$$\text{Recovery time} = t_4 - t_3 \tag{5}$$

Note: Since the functionality level at the end of the scenario may be different from at the start of the scenario, the recovery time may have to be measured at a new steady-state level [28].

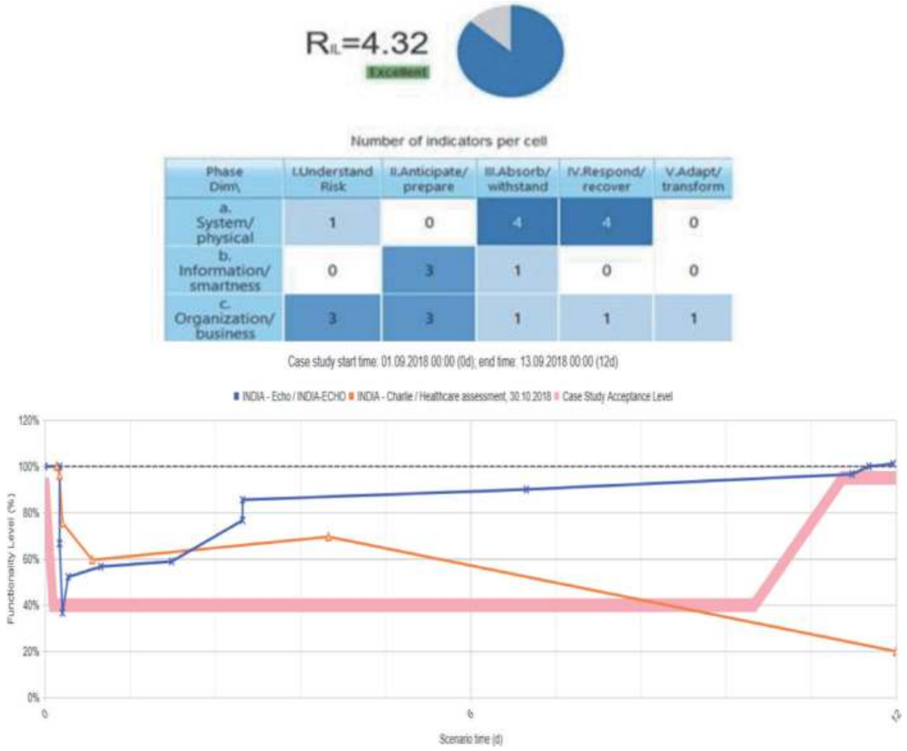
Recovery rate is defined as the rate at which the smart critical infrastructure recovers from a disruptive event and gets back to its initial functionality level [23]. It characterizes the recovery trajectories of the smart critical infrastructure from the point it starts recovering from the scenario to the final recovery. It is measured as the ratio of change in functionality level between time t_3 and t_4.

$$\text{Recovery rate} = \frac{(FL_4 - FL_3)}{(t_4 - t_3)} \tag{6}$$

Another measure considered for modeling the impact is **disruption time**. The disruption time is defined as the total time taken by the CI to recover. It is also seen as a measure for recover capacity of the smart critical infrastructure to return to the desired functionality level [23]**.** In the functionality level over time (FL-t) curve, it is the time between when the event occurs, i.e. at time t_1, and time when the smart critical infrastructure has fully recovered, i.e. t_4 (see **Figure 4**).

$$\text{Disruption time} = t_4 - t_1 \tag{7}$$

Improvement/adaptation/transformation: Final recovery of the FL of a smart critical infrastructure could be equal to, better than, or worse than the original FL [29]. Hence, the model allows for the calculation of the "improvement/adaptation/



R_{IL}=4.32

Excellent

Number of indicators per cell

Phase Dim\	I.Understand Risk	II.Anticipate/ prepare	III.Absorb/ withstand	IV.Respond/ recover	V.Adapt/ transform
a. System/ physical	1	0	4	4	0
b. Information/ smartness	0	3	1	0	0
c. Organization/ business	3	3	1	1	1

Case study start time: 01.09.2018 00:00 (0d); end time: 13.09.2018 00:00 (12d)

Figure 8.
An example of a report of one of the resilience assessments – FL curve comparing the response of FL with scenario time for case studies ECHO and CHARLIE, including the comparison of the FL curves with the acceptance level (shown in pink, can be used for stress-testing, too).

Macro Indicator	Values for ECHO	Values for CHARLIE
Robustness [%]	42	20
Absorption time [h]	1	284
Downtime [h]	2	−192
Loss of functionality [% over h]	58% in 282 h	80% in 284 h
Recovery time [h]	279	192
Recovery rate [%]	17	−26
Disruption time [h]	0	284

Table 1.
The macro indicator values for the cases in ***Figure 8*** *- the macro indicators calculated from the FL curve provide a quantitative way of comparing alternatives of system recovery supporting decision making and optimization [1].*

transformation." This is the capacity of the smart critical infrastructure to learn from a disruptive event (e.g. a revision of plans, modification of procedures, introduction of new tools and technologies [10]) (see **Figure 4**). It is measured as the ratio of change in FL during and after the event over the initial FL.

$$\text{Improvement/adaptation/transformation} = \frac{FL_{t5} - FL_{t0}}{FL_{t0}} \times 100\% \qquad (8)$$

Such macro indicators are ideal for comparing the FL responses for multiple case studies, infrastructure, entities etc. They allow an objective evaluation of not only how the functionality level of a system might react to an event but also how and when it can recover. Using a theoretical acceptance level, a stress-test can also be performed. An illustrative example comparing the FL response for two SmartResilience case studies (ECHO and CHARLIE) is shown in **Figure 8** and **Table 1**.

3. Practical application of the ResilienceCube and the methodology for resilience assessment

The indicator-based resilience concept described above, enables practical assessment of the following aspects of resilience (**Figure 9**):

1. Resilience Index (Resilience as "one number") and the ResilienceCube (preparedness, robustness, adaptation/transformation)

2. Assessing resilience of an infrastructures over time – the Resilience Level (RL)

3. Assessing resilience of an infrastructure during an adverse event – the Functionality Level (FL)

4. Assessing resilience of "multiple infrastructures": Multi-level resilience assessment

5. Modeling interaction and dependencies, visualizing resilience

6. Comparing resilience of different infrastructures: Benchmarking

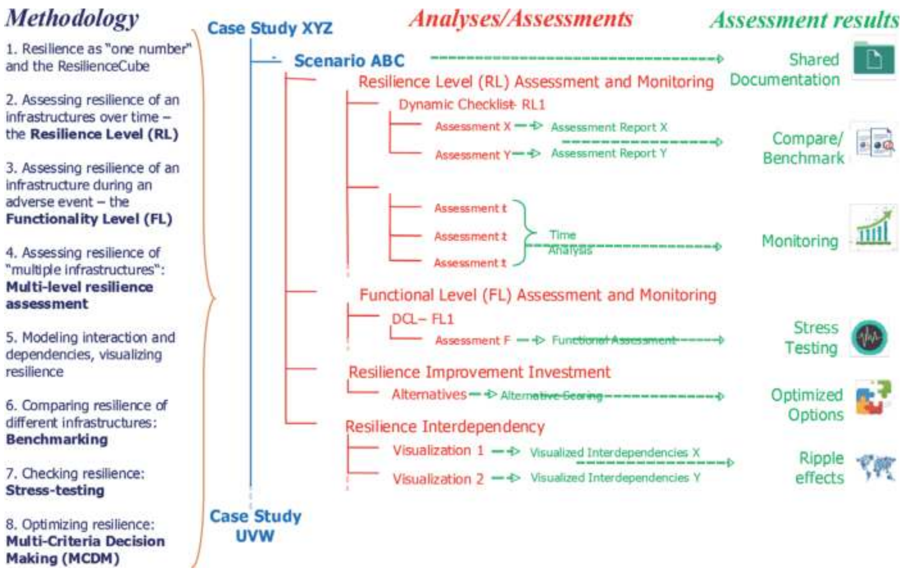

Methodology
1. Resilience as "one number" and the ResilienceCube
2. Assessing resilience of an infrastructures over time – the Resilience Level (RL)
3. Assessing resilience of an infrastructure during an adverse event – the Functionality Level (FL)
4. Assessing resilience of "multiple infrastructures": Multi-level resilience assessment
5. Modeling interaction and dependencies, visualizing resilience
6. Comparing resilience of different infrastructures: Benchmarking
7. Checking resilience: Stress-testing
8. Optimizing resilience: Multi-Criteria Decision Making (MCDM)
Case Study XYZ
Scenario ABC
Analyses/Assessments
Resilience Level (RL) Assessment and Monitoring
Dynamic Checklist- RL1
Assessment X
Assessment Report X
Assessment Y
Assessment Report Y
Assessment t
Assessment t
Assessment t
Time Analysis
Functional Level (FL) Assessment and Monitoring
DCL– FL1
Assessment F
Functional Assessment
Resilience Improvement Investment
Alternatives
Alternative Scoring
Resilience Interdependency
Visualization 1
Visualized Interdependencies X
Visualization 2
Visualized Interdependencies Y
Case Study UVW
Assessment results
Shared Documentation
Compare/ Benchmark
Monitoring
Stress Testing
Optimized Options
Ripple effects

Figure 9.
Applying the methodologies in order to assess resilience and obtain practical (quantitative) results.

7. Checking resilience: Stress-testing

8. Optimizing resilience: Multi-Criteria Decision Making (MCDM)

For its users, the methodologies are embedded into the interactive, web-based and freely available "ResilienceTool". Applied in different case studies, dealing with energy, transportation, health, smart cities, water, sensitive installations, etc., the methodology and tool provide the user with different options when using the approach and the system by showing how benchmarking can be done and the best-practice solutions can be re-used.

When applying the concept and the methodologies practically, it is important to understand that the flexibility of the concept and the methodologies necessarily demand for domain expertise in "configuring" the resilience model for a specific area/city or critical infrastructure. A fixed list of critical infrastructures for cities in Europe does not exist, and it must be up to each user of the concept, methodologies and the software tool, to decide which feature of respective infrastructures should be analyzed and how. Similarly, no fixed list of threats exists, neither on the area level nor for the single critical infrastructures. Thus, it will be up to the users to define which threats (scenarios) they consider relevant. Domain experts are needed in order to define the important issues, and how to measure these issues, i.e. identifying the indicators. They are in a way "configuring" the resilience model, which largely is a one-time effort prior to using the model for calculating the resilience levels, although some adjustments, tuning, and reconsiderations are expected. Thus, in the implementation phase, it is important to have close collaboration between the users, the method developers, and IT developers (of calculation and presentation tools).

3.1 Resilience index/cube, resilience level (RL), functionality level (FL) and multi-level resilience assessment

Per default, assessing resilience in the concept is based on scoring (other ways of upwards aggregation are possible, but used only in "expert mode"), the scores being aggregated upwards – up to the Resilience Index score. At each level, the scores can be assigned weights, as the indicators, too. When performing the resilience assessment, the indicators' real values are entered into the calculation, and the issue scores are obtained as average weighted scores of the indicator scores. It is possible to let a specific indicator overrule the effect of the other indicators, i.e. having "knock out indicators" where, in the case of a low value, the effect is not "averaged away" through an average weighted score of all the indicators. The reasoning behind the selected scales is that a scale from 0 to 5 for indicators (and issues) are sufficiently broad, especially if there are needs to perform expert judgments to provide scores for the indicators (or directly for the issues) in case of lack of data [17]. This has similarities to the use of safety integrity levels (SIL) for safety-instrumented systems [30]. In and for the cases where the issue-indicator approach is not sufficient, the concept and the tool allow using multi-level indicators (de facto composite indicators).

3.2 Modeling interaction and dependencies, visualizing resilience

SmartResilience and InfraStress projects look at interdependencies between infrastructures to understand how, in a case of a problem in one of them, the functionality of others can be impacted. The assessment is based on issues and indicators: these issues and indicators that are shared by different infrastructures indicate "lines of interconnectedness and interdependency". The infrastructures involved and the issues/indicators form thus the logical network that can analyze in order to model the propagation of influences from one infrastructure to another. Thus, the cascading and ripple effects can be modeled and the dynamic behavior of the network ("infrastructure-of-infrastructures") analyzed **Figure 10**).

The network in **Figure 10** is created as the case applied onto the indicators applicable to six types of infrastructures in SmartResilience project (health, ICT, energy, water, transportation, industry) and looking at the core, recommended and specific indicators (**Figure 6**). About 2,000 indicators were considered. The

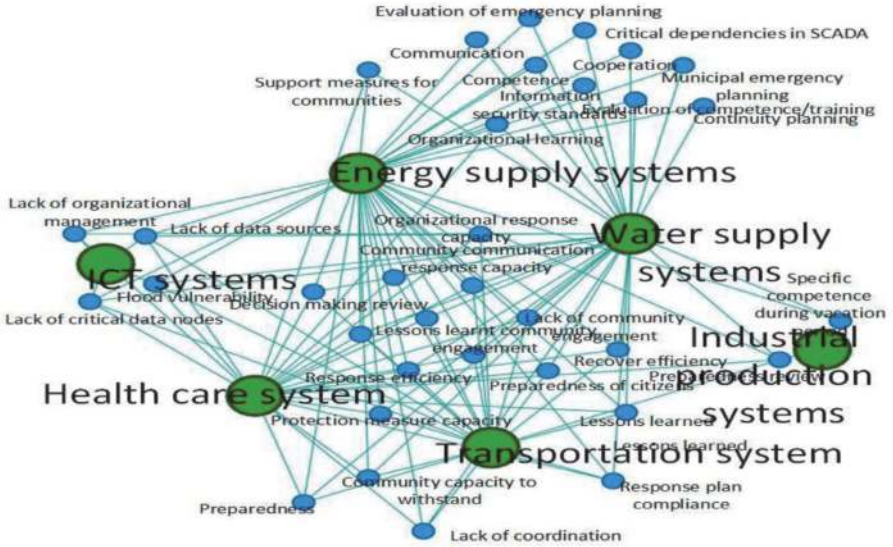

Evaluation of emergency planning
Critical dependencies in SCADA
Communication
Cooperation
Support measures for communities
Competence
Municipal emergency planning
Information security standards
Evaluation of competence/training
Continuity planning
Organizational learning
Energy supply systems
Lack of organizational management
Lack of data sources
Organizational response capacity
Community communication response capacity
Water supply systems
ICT systems
Specific competence during vacation
Flood vulnerability
Decision making review
Lack of critical data nodes
Lack of community engagement
Lessons learnt community engagement
Industrial production systems
Recover efficiency
Preparedness review
Response efficiency
Preparedness of citizens
Health care system
Protection measure capacity
Lessons learned
Lessons learned
Transportation system
Community capacity to withstand
Response plan compliance
Preparedness
Lack of coordination

Figure 10.
Interdependencies among multiple infrastructures as a network: Common indicators define the interdependencies.

analysis has included the web-semantics-based analysis of the descriptions of indicators and the statistical analysis of the values of these indicators in the case studies performed in SmartResilience project. The analysis has also served as the basis for the,more user-oriented visualization of interdependencies in a critical infrastructure.

3.3 Comparing resilience of different infrastructures: benchmarking

Using issues and indicators from pre-approved and standardized sources such as the CORE and Recommended DCLs allows for the additional benefit of benchmarking certain aspects of resilience management across different organizations. As the CORE issues are expected to be present in every Complete DCL, organizations can at the very least be compared based on managerial, resilience-oriented activities and processes, regardless of industry or threat. WITHIN a particular scenario (industry and threat), Complete DCLs can be benchmarked when using the Recommended issues proposed by the industry's experts.

Once the CORE DCL issues are selected, the user can make an actual resilience assessment adding the indicators under the CORE issues. Since for all of the case studies, the Recommended DCLs have been developed, one can take a look at those lists and choose which indicators from there fit into the CORE DCL. It may happen that the names of the issues from Recommended DCL are slightly different from the CORE ones. Hence, it is possible that not all the previously used indicators will fit. In this case, the user should use only the ones which match with the CORE issue. Furthermore, it may be needed that new indicators (not used in the Recommended DCL) are added in order to ensure sufficient coverage of the CORE issue.

3.4 Checking resilience: stress testing

The stress test framework is used to test whether, in a given threat situation, the smart critical infrastructure is/will be resilient enough to be able to continue functioning within the prescribed limits. The FL curve(s) obtained in the analysis is compared with the stress test criteria and limits in order to evaluate whether the smart critical infrastructure 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 (e.g.):

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

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

Time ("horizontal loss"): when subjected to a threat/event, a smart critical infrastructure 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 smart critical infrastructure 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.

3.5 Optimizing resilience: Multi-criteria decision making (MCDM)

Given that the purpose of the resilience and functionality level assessments is to reveal weaknesses, either isolated or in comparison with others (benchmarking), implementation of improvement measures is expected to 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. higher RL), 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 and given that the nature of smart critical infrastructures and the resilience issues that they evoke tend to mix both quantitative (budgeting, performance indicators, etc.) and qualitative (expectations, procedures, etc.) aspects, it has to be able to address both semantic-logic and crisp numbers. Logical Multi-criteria decision-making (MCDM) methods are also preferable over other alternative decision-making frameworks because MCDM methods have "the potential capability of improving the *transparency*, *analytic rigor*, *auditability* and *conflict resolution* of decision-makers" [31]. Correspondingly, the MCDM provides:

- Means to establish accountability and transparency behind decisions, which may otherwise have unclear rationale and motives [25] by: placing stress on clearly stating and weighting the decision criteria, thereby improving transparency, and by ensuring that decisions taken through this method are explicit, paving the way to audit past decisions and thus provide accountability [32].

- Means for conflict resolution. This becomes a crucial issue when multiple perspectives are applied to a single smart critical infrastructure management decision [20, 24].

- Path for engagement and participation. Besides aiding decisions related to engineering, scientific studies, and cost analysis, one aspect that is becoming very crucial in decision-making studies is the engagement of multi-stakeholders and participation of communities [32].

The project considered various in-depth MCDM approaches that were used in other projects such as AIRM, PROMETHEE, and ELECTRE. However, during the eight case studies included in the SmartResilience and InfraStress projects, all of which involve end-user-owners of smart critical infrastructures, it became clear that the complexity of these methods made understanding them much more difficult and, at the same time, the required processing of the data needed proving to be prohibitively time consuming and expensive. Once an analysis is prepared and assessment data is input into the model (available on the project's ResilienceTool), the different optimization alternatives are scored following the combination of the user's input with the weighted criteria to rank the alternatives.

4. Implementation of the ResilienceCube concept in the "ResilienceTool" and merging it with the situational awareness systems

To support the methodology, a complete online tool was developed in which all the aspects described above were implemented with its intended user in mind - the person within a city or area, or a specific smart critical infrastructure [13]. The tool is based on the concept and its methodologies (the Cube, **Figure 11**), on the data resulting from extremely wide use (over 5,000 issues/indicators, over 300 assessments). In addition to the tools needed to support the ResilienceCube related analysis, presented above (database, methodologies, reporting), the tool contains also the Moodle-based education platform, support for standardization, a knowledge base (e.g. glossary) and a series of own and external tools linked to the system. Currently over a dozen of subsystems, containing all the features of the full system, but operating on the respective "private" databases are available for external users opted for the use of the system.

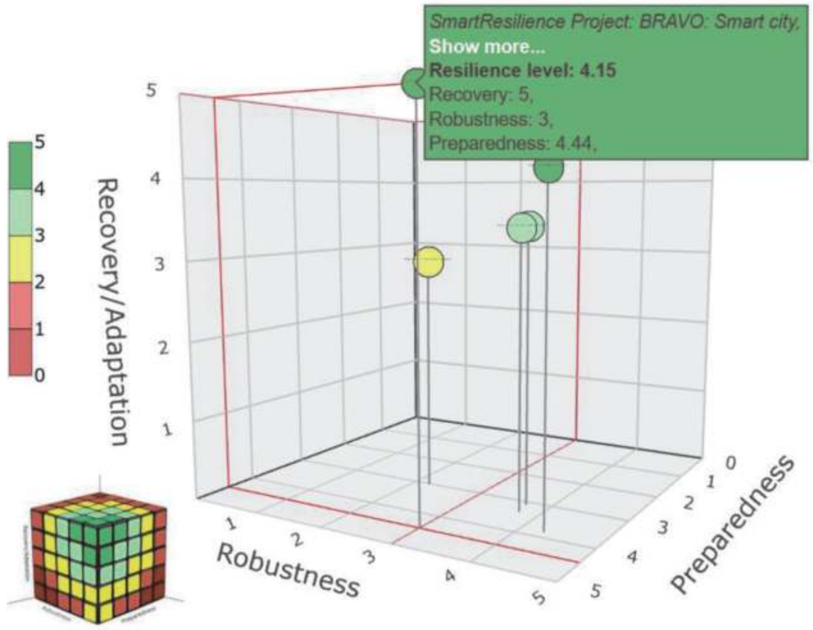


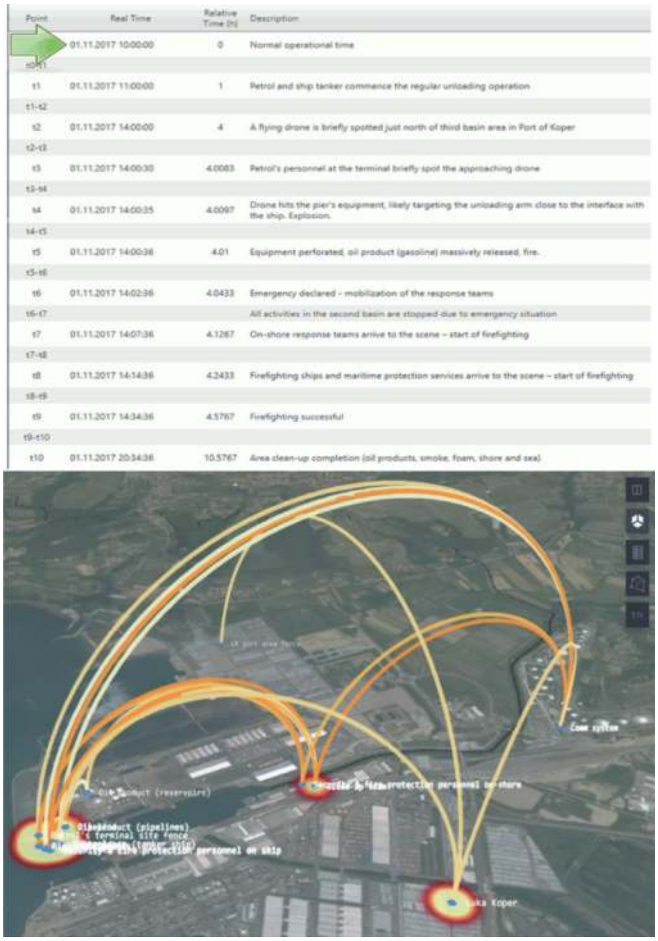
Figure 11.
ResilienceTool: The ResilienceCube.

5. Application of the concept and the tool

The project [1], covered over 30 case studies, (e.g. **Figures 8** and **12**).

6. Towards integration of resilience and situational awareness

Following the generally accepted position, that integration of all the aspects (concepts, data, tools, policies, implementation, etc.) is essential for successful risk and resilience governance, the InfraStress project of the EU [2] has developed an integrated framework (**Figure 13**).



Point	Real Time	Relative Time [h]	Description
	01.11.2017 10:00:00	0	Normal operational time
t0-t1			
t1	01.11.2017 11:00:00	1	Petrol and ship tanker commence the regular unloading operation
t1-t2			
t2	01.11.2017 14:00:00	4	A flying drone is briefly spotted just north of third basin area in Port of Koper
t2-t3			
t3	01.11.2017 14:00:30	4.0083	Petrol's personnel at the terminal briefly spot the approaching drone
t3-t4			
t4	01.11.2017 14:00:35	4.0097	Drone hits the pier's equipment, likely targeting the unloading arm close to the interface with the ship. Explosion.
t4-t5			
t5	01.11.2017 14:00:36	4.01	Equipment perforated, oil product (gasoline) massively released, fire.
t5-t6			
t6	01.11.2017 14:02:36	4.0433	Emergency declared – mobilization of the response teams
t6-t7			All activities in the second basin are stopped due to emergency situation
t7	01.11.2017 14:07:36	4.1267	On-shore response teams arrive to the scene – start of firefighting
t7-t8			
t8	01.11.2017 14:14:36	4.2433	Firefighting ships and maritime protection services arrive to the scene – start of firefighting
t8-t9			
t9	01.11.2017 14:34:36	4.5767	Firefighting successful
t9-t10			
t10	01.11.2017 20:34:36	10.5767	Area clean-up completion (oil products, smoke, foam, shore and sea)

Figure 12.
Visualization of interdependencies based on indicators: User-oriented (InfraStress project).

The approach has been implemented in its five "pilots", cases covering "sensitive industrial plants and infrastructures", exposed to cyber-physical threats. The pilots cover chemical and pharmaceutical plants, ports, industrial zones, petrochemical plants, storage plants and similar. For all the plants the resilience has been analyzed, the analysis integrated with analysis of situational awareness systems performance (e.g. anti-drone systems or cyber protection systems), and, finally embedded into a testbed stress-testing concept for different scenarios.

7. Standardizing the concept: ISO 31050

The main calling of ISO 31050 (ISO New Work Item (NWI) 31050 "Guidance for Managing Emerging Risks to Enhance Resilience"[4]), is to provide universal, yet meaningful guidance on developing new competencies and business models to create relevant and realistic recommendations in an ever-changing uncertain world. The standard itself aims to provide the much-needed foresight and insight to deal with the rapidly changing landscape of risk due to the slew of new uncertainties and new emerging risks, the management of which is essential for society. It is based on the idea that these, emerging risks, are those that can challenge the resilience of the critical infrastructures the most. It aims to integrate and align the (emerging) risk

[4] https://www.iso.org/standard/54224.html

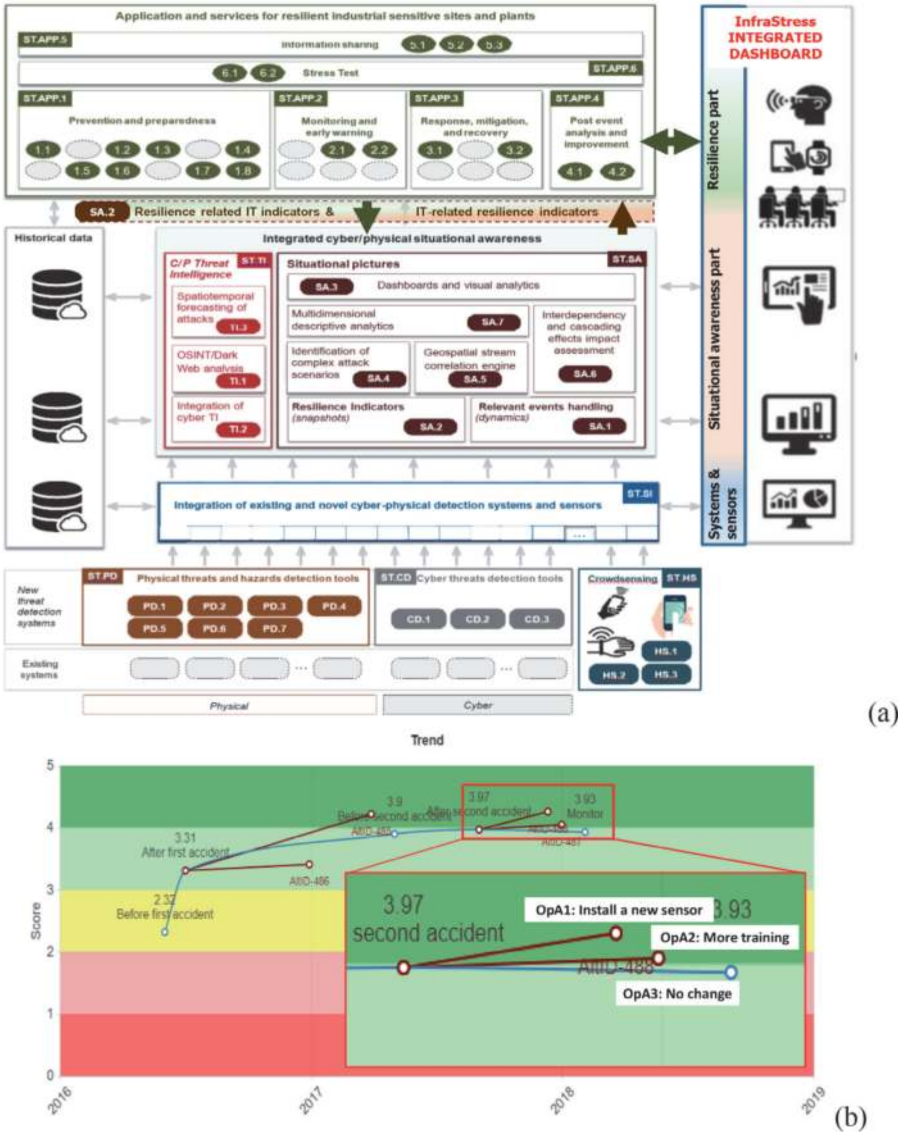

Application and services for resilient industrial sensitive sites and plants
ST.APP.5
Information sharing
5.1
5.2
5.3
6.1
6.2
Stress Test
ST.APP.6
ST.APP.1
Prevention and preparedness
1.1
1.2
1.3
1.4
1.5
1.6
1.7
1.8
ST.APP.2
Monitoring and early warning
2.1
2.2
ST.APP.3
Response, mitigation, and recovery
3.1
3.2
ST.APP.4
Post event analysis and improvement
4.1
4.2
InfraStress INTEGRATED DASHBOARD
Resilience part
Situational awareness part
Systems & sensors
SA.2
Resilience related IT indicators &
IT-related resilience indicators
Historical data
Integrated cyber/physical situational awareness
C/P Threat Intelligence
ST.TI
Spatiotemporal forecasting of attacks
TI.3
OSINT/Dark Web analysis
TI.1
Integration of cyber TI
TI.2
Situational pictures
ST.SA
SA.3
Dashboards and visual analytics
Multidimensional descriptive analytics
SA.7
Interdependency and cascading effects impact assessment
SA.6
Identification of complex attack scenarios
SA.4
Geospatial stream correlation engine
SA.5
Resilience Indicators (snapshots)
SA.2
Relevant events handling (dynamics)
SA.1
Integration of existing and novel cyber-physical detection systems and sensors
ST.SI
...
New threat detection systems
ST.PD
Physical threats and hazards detection tools
PD.1
PD.2
PD.3
PD.4
PD.5
PD.6
PD.7
ST.CD
Cyber threats detection tools
CD.1
CD.2
CD.3
Crowdsensing
ST.HS
HS.1
HS.2
HS.3
Existing systems
Physical
Cyber
(a)
Trend
Score
5
4
3
2
1
0
2.32
Before first accident
3.31
After first accident
AltID-486
3.9
Before second accident
AltID-485
3.97
After second accident
AltID-488
AltID-487
3.93
Monitor
3.97
second accident
OpA1: Install a new sensor
3.93
OpA2: More training
AltID-488
OpA3: No change
2016
2017
2018
2019
(b)

Figure 13.
InfraStress framework integrating resilience analysis and situational awareness and its application to resilience improvement decision-making: Within the overall framework (a), the embedded MCDM modules communicate with other modules and get values through a Kafka broker, and lead to the resilience assessment based decision optimization (b).

framework with resilience framework (definitions, concepts, requirements) and propose outputs such as a procedure for scanning for emerging risks, metrics for assessing possible impacts of those risks on critical infrastructure's resilience. The management framework, guidance for interoperability and common/agreed indicators, as well as the particular considerations related to emerging risks in resilience assessment. ISO 31050 will be part of the ISO 31000:2018 family of standards, monitored by the ISO Technical Committee TC262.

8. Conclusions

The ResilienceCube allows presenting the resilience of a critical infrastructure as a single point (Resilience Index) in a 3D space. The concept, especially as implemented in the tool (the ResilienceTool) is user-friendly, intuitively understandable and flexible. It supports end-users (authorities, critical infrastructure operators and owners) in improving the disaster resilience of respective critical infrastructures through indicator-based assessment of their resilience capabilities. This solution provided by SmartResilience and InfraStress projects is oriented towards the practical needs of end-users and has been developed in close collaboration with all relevant stakeholders. In order to achieve the Technology Readiness Level (TRL) beyond the initially planned 4, the Tool is being tested and constantly improved through the development of realistic use cases, both within and beyond the projects.

The SmartResilience and InfraStress ResilienceTool are envisaged to stay available, free of charge for the registered ERRA members, also after the project end. The main ERRA service (risk and resilience "Assessment-as-a-service") will be performed by the Agency together with and subcontracting to Agency member organizations (organizational members and individuals) which have the different competencies needed to meet the specific needs of specific industry branches or application areas (e.g. critical infrastructures or new technologies). In the most general terms, ERRA would contact and negotiate with the customers, engage the experts among the Agency members, process the contracts with the customer, and guarantee the quality of assessment provided by the Agency. Main Agency services would be the self-assessment, the audited self-assessment and the third party audit, similarly to the services of GRI (www.globalreporting.org).

The concepts and the tools were applied to the analysis of health infrastructures (over 100 hospitals) in a COVID-like scenario [33]. The concept allows integrating the qualitative approaches with those based on a more complex quantitative resilience analysis (e.g. [30, 34, 35] or [22]). In addition, the work in the background of this paper has clearly shown, that the current research on resilience has a number of different aspects: from those focusing on the "resilience of and within a network" (e.g. in the area of electric grids or transportation networks - **Figure 14**), to those looking at resilience as "ability of an organization to absorb and adapt in a changing environment" [36]. The latter, obviously not necessarily requiring a network, or measuring it within a network. Both approaches, on the other hand, are applicable to critical infrastructures.

To conclude, within the plethora of the "current" existing tools (e.g. those presented or reviewed in [25, 37–42] or [43]), that all can simulate different resilience aspects of large and complex systems and/or apply optimization techniques to improve it (e.g. by indicating the optimum path towards system recovery or improving preparedness to unknowns) the approach presented here proposes a pragmatic and flexible way to achieve improvement through applying resilience indicators. It has been "combat-tested" in a number of large-scale cases and it has confirmed being robust and combinable with the systems previously on site.

Finally, the concepts might have one of an even more ambitious potential allocation: the biggest infrastructure of all is the "infrastructure of all infrastructures" of our planet Earth and the "global society". Technically, the methodology presented here can be applied for this case too, allowing to quantify the global

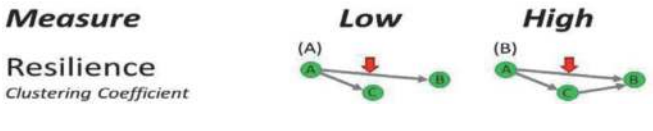


Figure 14.
Resilience of a network (graph representation) – Not always the same as the engineering resilience of an organization, defined by ISO as "ability of an organization to absorb and adapt in a changing environment" (ISO 23316, https://www.iso.org/obp/ui#iso:std:iso:22316:ed-1:v1:en).

resilience (note: we do not have anything better around yet!) and point out where the "investment in the improvement of the global infrastructure" will be the most effective and beneficial.

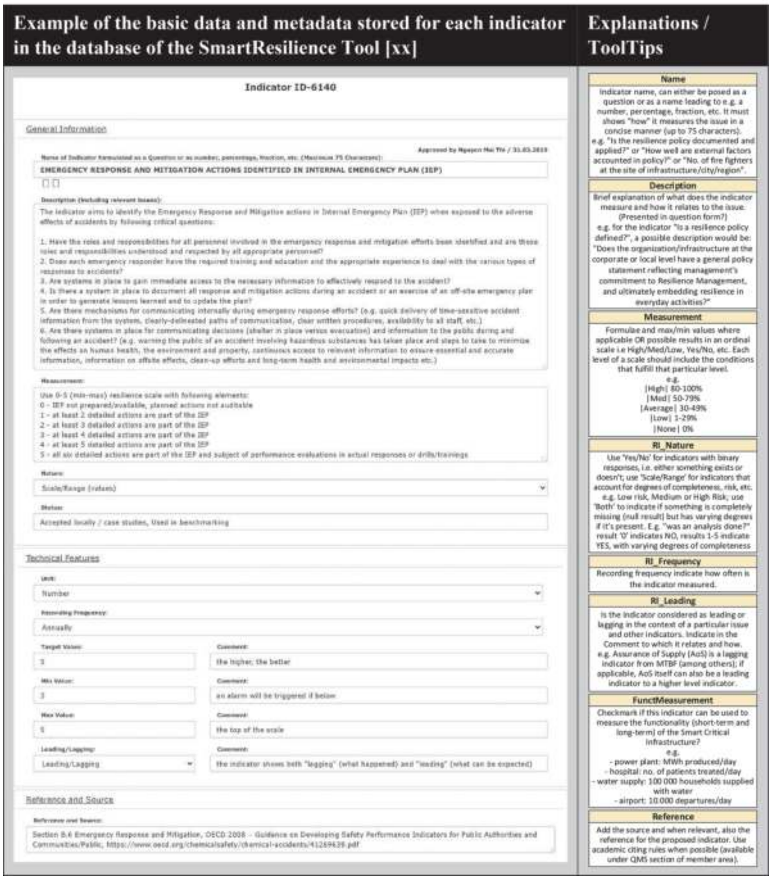
Acknowledgements

The contribution is based on the Grant Agreements No. 700621 and No. 833088 supporting the work on the SmartResilience and InfraStress projects, respectively, provided by the Research Executive Agency (REA) ('the Agency'), under the power delegated by the European Commission ('the Commission'). This support is gladly acknowledged. The work presented is a result of a great collective effort of all the partners of the SmartResilience and InfraStress projects – many thanks for this to all of them. Nevertheless, some of these contributions were particularly important for this particular paper, e.g., the methodological ones of K. Øien, big-data related ones of P. Klimek, and technical preparatory ones of Sh. Macika, M. Th. Nguyen and T. Rosen. The authors mention this with appreciation and gratitude.

Appendix 1

Example of the resilience indicator data sheet in SmartResilience and InfraStress systems (a) and their implementation in the database (b).

(a)



Example of the basic data and metadata stored for each indicator in the database of the SmartResilience Tool [xx]

Indicator ID-6140

General Information

Approved by Nguyen Mai Thi / 31.03.2019

Name of Indicator formulated as a Question or as number, percentage, fraction, etc. (Maximum 75 Characters):

EMERGENCY RESPONSE AND MITIGATION ACTIONS IDENTIFIED IN INTERNAL EMERGENCY PLAN (IEP)

□ □

Description (including relevant issues):

The indicator aims to identify the Emergency Response and Mitigation actions in Internal Emergency Plan (IEP) when exposed to the adverse effects of accidents by following critical questions:

1. Have the roles and responsibilities for all personnel involved in the emergency response and mitigation efforts been identified and are these roles and responsibilities understood and respected by all appropriate personnel?
2. Does each emergency responder have the required training and education and the appropriate experience to deal with the various types of responses to accidents?
3. Are systems in place to gain immediate access to the necessary information to effectively respond to the accident?
4. Is there a system in place to document all response and mitigation actions during an accident or an exercise of an off-site emergency plan in order to generate lessons learned and to update the plan?
5. Are there mechanisms for communicating internally during emergency response efforts? (e.g. quick delivery of time-sensitive accident information from the system, clearly-delineated paths of communication, clear written procedures, availability to all staff, etc.)
6. Are there systems in place for communicating decisions (shelter in place versus evacuation) and information to the public during and following an accident? (e.g. warning the public of an accident involving hazardous substances has taken place and steps to take to minimize the effects on human health, the environment and property, continuous access to relevant information to ensure essential and accurate information, information on offsite effects, clean-up efforts and long-term health and environmental impacts etc.)

Measurement:

Use 0-5 (min-max) resilience scale with following elements:
0 - IEP not prepared/available, planned actions not auditable
1 - at least 2 detailed actions are part of the IEP
2 - at least 3 detailed actions are part of the IEP
3 - at least 4 detailed actions are part of the IEP
4 - at least 5 detailed actions are part of the IEP
5 - all six detailed actions are part of the IEP and subject of performance evaluations in actual responses or drills/trainings

Nature:

Scale/Range (values)

Status:

Accepted locally / case studies, Used in benchmarking

Technical Features

Unit:

Number

Recording Frequency:

Annually

Target Value:	Comment:
3	the higher, the better
Min Value:	Comment:
3	an alarm will be triggered if below
Max Value:	Comment:
5	the top of the scale
Leading/Lagging:	Comment:
Leading/Lagging	the indicator shows both "lagging" (what happened) and "leading" (what can be expected)

Reference and Source

Reference and Source:

Section B.6 Emergency Response and Mitigation, OECD 2008 – Guidance on Developing Safety Performance Indicators for Public Authorities and Communities/Public; https://www.oecd.org/chemicalsafety/chemical-accidents/41269639.pdf

Explanations / ToolTips

Name

Indicator name, can either be posed as a question or as a name leading to e.g. a number, percentage, fraction, etc. It must shows "how" it measures the issue in a concise manner (up to 75 characters). e.g. "Is the resilience policy documented and applied?" or "How well are external factors accounted in policy?" or "No. of fire fighters at the site of infrastructure/city/region".

Description

Brief explanation of what does the indicator measure and how it relates to the issue. (Presented in question form?) e.g. for the indicator "Is a resilience policy defined?", a possible description would be: "Does the organization/infrastructure at the corporate or local level have a general policy statement reflecting management's commitment to Resilience Management, and ultimately embedding resilience in everyday activities?"

Measurement

Formulae and max/min values where applicable OR possible results in an ordinal scale i.e High/Med/Low, Yes/No, etc. Each level of a scale should include the conditions that fulfill that particular level.
e.g.
|High| 80-100%
|Med| 50-79%
|Average| 30-49%
|Low| 1-29%
|None| 0%

RI_Nature

Use 'Yes/No' for indicators with binary responses, i.e. either something exists or doesn't; use 'Scale/Range' for indicators that account for degrees of completeness, risk, etc. e.g. Low risk, Medium or High Risk; use 'Both' to indicate if something is completely missing (null result) but has varying degrees if it's present. E.g. "was an analysis done?" result '0' indicates NO, results 1-5 indicate YES, with varying degrees of completeness

RI_Frequency

Recording frequency indicate how often is the indicator measured.

RI_Leading

Is the indicator considered as leading or lagging in the context of a particular issue and other indicators. Indicate in the Comment to which it relates and how. e.g. Assurance of Supply (AoS) is a lagging indicator from MTBF (among others); if applicable, AoS itself can also be a leading indicator to a higher level indicator.

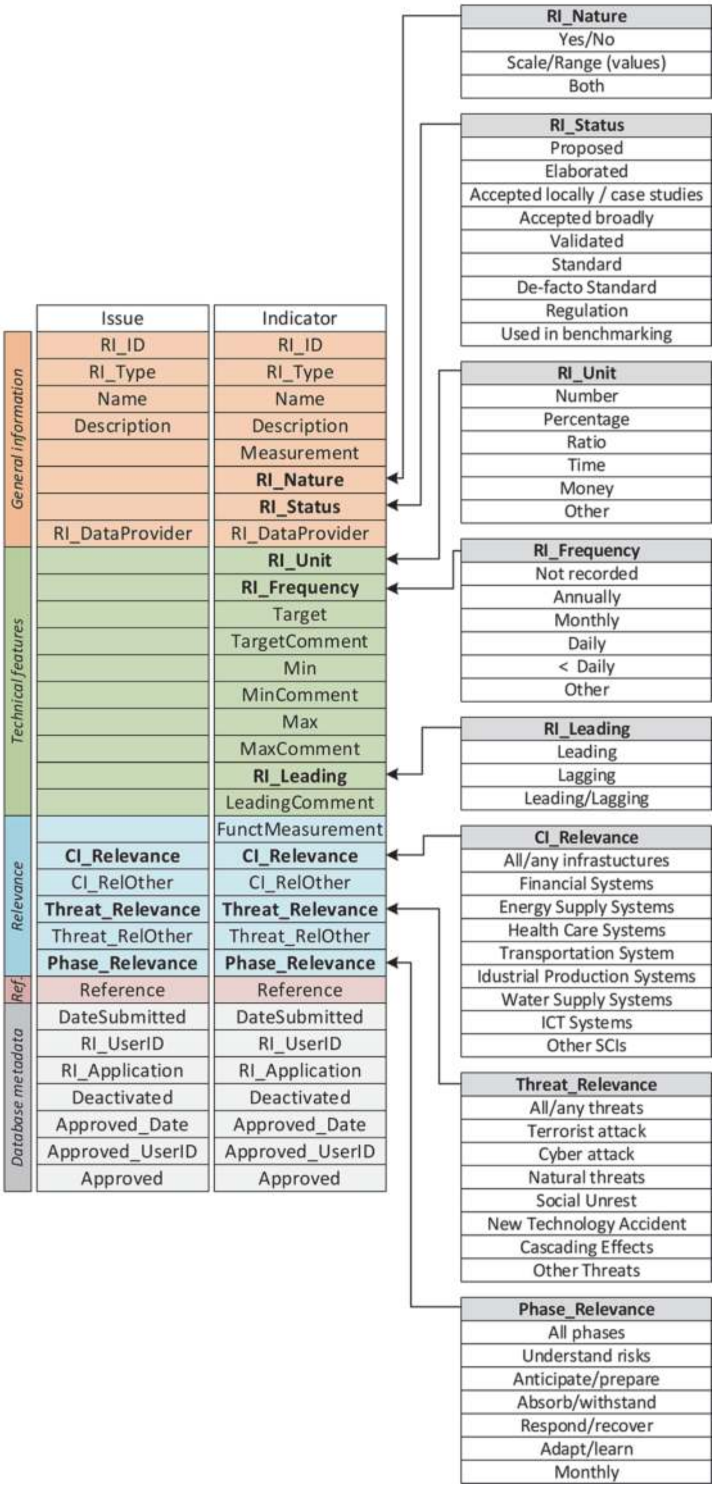
FunctMeasurement

Checkmark if this indicator can be used to measure the functionality (short-term and long-term) of the Smart Critical Infrastructure?
e.g.
- power plant: MWh produced/day
- hospital: no. of patients treated/day
- water supply: 100 000 households supplied with water
- airport: 10 000 departures/day

Reference

Add the source and when relevant, also the reference for the proposed indicator. Use academic citing rules when possible (available under QMS section of member area).

(b)



	Issue	Indicator
General information	RI_ID	RI_ID
	RI_Type	RI_Type
	Name	Name
	Description	Description
		Measurement
		RI_Nature
		RI_Status
	RI_DataProvider	RI_DataProvider
Technical features		**RI_Unit**
		RI_Frequency
		Target
		TargetComment
		Min
		MinComment
		Max
		MaxComment
		RI_Leading
		LeadingComment
Relevance		FunctMeasurement
	CI_Relevance	**CI_Relevance**
	CI_RelOther	CI_RelOther
	Threat_Relevance	**Threat_Relevance**
	Threat_RelOther	Threat_RelOther
	Phase_Relevance	**Phase_Relevance**
Ref.	Reference	Reference
Database metadata	DateSubmitted	DateSubmitted
	RI_UserID	RI_UserID
	RI_Application	RI_Application
	Deactivated	Deactivated
	Approved_Date	Approved_Date
	Approved_UserID	Approved_UserID
	Approved	Approved

RI_Nature
Yes/No
Scale/Range (values)
Both

RI_Status
Proposed
Elaborated
Accepted locally / case studies
Accepted broadly
Validated
Standard
De-facto Standard
Regulation
Used in benchmarking

RI_Unit
Number
Percentage
Ratio
Time
Money
Other

RI_Frequency
Not recorded
Annually
Monthly
Daily
< Daily
Other

RI_Leading
Leading
Lagging
Leading/Lagging

CI_Relevance
All/any infrastructures
Financial Systems
Energy Supply Systems
Health Care Systems
Transportation System
Idustrial Production Systems
Water Supply Systems
ICT Systems
Other SCIs

Threat_Relevance
All/any threats
Terrorist attack
Cyber attack
Natural threats
Social Unrest
New Technology Accident
Cascading Effects
Other Threats

Phase_Relevance
All phases
Understand risks
Anticipate/prepare
Absorb/withstand
Respond/recover
Adapt/learn
Monthly

Author details

Aleksandar S. Jovanovic[1,2]*, Somik Chakravarty[1,2] and Marjan Jelic[2]

1 European Risk and Resilience Institute (EU-VRi), Stuttgart, Germany

2 Steinbeis Advanced Risk Technologies (R-Tech), Stuttgart, Germany

*Address all correspondence to: jovanovic@eu-vri.eu;
jovanovic@risk-technologies.com

References

[1] SmartResilience (2016). Smart Resilience Indicators for Smart Critical Infrastructures – The European Union's Horizon 2020 Research and Innovation Programme, Grant Agreement No 700621 (2016-2019). Coordinator: EU-VRi, www.smartresilience.eu-vri.eu.

[2] InfraStress: Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system; Project reference: 833088, Project type: Innovation Action, Call: SU-INFRA01-2018-2019-2020 - Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe https://www.infrastress.eu

[3] European Commission (2013). DRS-14-2015: Topic: Critical Infrastructure Protection topic 3: Critical Infrastructure resilience indicator – analysis and development of methods for assessing resilience, https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/143-drs-14-2015.html

[4] Jovanović, A., Bellini, E. (Eds.), Aligning the resilience-related research efforts in the EU-DRS projects, Joint Workshop DRS-7&14 projects | Brussels, September 13–14, 2017, Steinbeis Edition, Stuttgart, Germany 2017, ISBN 978-3-95663-143-6 2017 |E-Book (PDF), 165 p.

[5] Brown, B., Neil-Adger, W., Tompkins, E., Bacon, P., Shim, D. and Young, K. (2001). Trade-off analysis for marine protected area management, Ecological Economics, vol. 37, no. 3, pp. 417–434.

[6] Jovanović, A., Klimek, P., Choudhary, A., Schmid, N., Linkov, I., Øien, K., ... Lieberz, D. (2016). SmartResilience D1.2: Analysis of existing assessment resilience approaches, indicators and data sources: Usability and limitations of existing indicators for assessing, predicting and monitoring critical infrastructure resilience, EU project SmartResilience https://www.smartresilience.eu-vri.eu , Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[7] IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7. Geneva: International Electrotechnical Commission

[8] SmartResilience (2017). Deliverable D 3.2: Assessing resilience of smart critical infrastructures based on indicators http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.2.pdf.

[9] SmartResilience (2017). Deliverable D 5.1: Report on the results of the interactive workshop http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD5.1.pdf

[10] SmartResilience (2017). Deliverable D2.1: Understanding "smart" technologies and their role in ensuring resilience of infrastructures, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany

[11] SmartResilience (2017). Deliverable D3.1: Contextual factors related to resilience, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany http://www.smartresilience.eu-vri.eu/sites/default/files/publications/Smart ResD3.1.pdf

[12] SmartResilience (2017). Stress test and evaluation framework. EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany. http://smartresilie

nce.eu-vri.eu/sites/default/files/publications/SmartResD5.2.pdf

[13] Jovanovic, A., M. Jelic, T. Rosen, P. Klimek, S. Macika, and K. Øien (2019). SmartResilience D3.7: "The ResilienceTool" of the Smart-Resilience project. EU project SmartResilience, Project No. 700621. http://www.smartresilience.eu-vri.eu/sites/default/files/publications/SmartResD3.7.pdf

[14] Fisher, R.E., Bassett, G.W., Buehring, W.A., Collins, M.J., Dickinson, D.C., Eaton, L.K., … Peerenboom, J.P. (2010). Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-10-9, Argonne, IL, USA http://www.ipd.anl.gov/anlpubs/2010/09/67823.pdf

[15] EPRI (2000). Guidelines for Trial Use of Leading Indicators of Human Performance: The Human Performance Assistance Package. EPRI (U.S. Electric Power Research Institute), Palo Alto, CA, 10000647.

[16] EPRI (2001). Final report on Leading Indicators of Human Performance. EPRI, Palo Alto, CA, and the U.S. Department of Energy, Washington, DC, 1003033.

[17] Øien, K. (2001). A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety, 74, 147–167.

[18] National Infrastructure Advisory Council. (2009) Critical Infrastructure Resilience, Final Report and Recommendations, U.S. Department of Homeland Security, Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

[19] Øien, K., Massaiu, S., & Tinmannsvik, R.K. (2012). Guideline for implementing the REWI method; Resilience based Early Warning Indicators. SINTEF report A22026, Trondheim, Norway.

[20] Cai, X., Lasdon, L. and Michelsen, A.M. (2004). Group decision-making in water resources planning using multiple objective analysis, Journal of Water Resources Planning and Management, vol. 130, no. 1, pp. 4–14.

[21] Øien, K., A. Jovanović, et al. (2018). D3.6 Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures, , EU project SmartResilience https://www.smartresilience.eu-vri.eu , Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[22] Tofani, A., D'Agostino, G., Di Pietro, A., Rosato, V. (2019). Modeling Resilience in Electrical Distribution Networks. In book: Management of Critical Infrastructure, November 2019 (10.5772/intechopen.85917)

[23] Zobel, C.W. (2014). Quantitatively representing nonlinear disaster recovery. *Decision Sciences*, 43(4), 687-710.

[24] Mustajoki, J., Hamalainen, R.P. and Marttunen, M. (2004). Participatory multicriteria decision analysis with Web-HIPRE: A case of lake regulation policy. Environmental Modeling & Software, vol. 19, no. 6, pp. 537–547.

[25] Boumphrey, R., and Bruno, M. (2015). "Foresight Review of Resilience Engineering: designing for the expected and unexpected."

[26] Business Dictionary (2017). Downtime. Business Dictionary. http://www.businessdictionary.com/definition/downtime.html

[27] Sahebjamnia, N., Torabi, S. A., Mansouri, S. A. (2015). Integrated business continuity and disaster

recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273. https://doi.org/10.1016/j.ejor.2014.09.055

[28] Ruiying. Li. et.al. (2017). A new resilience measure for supply chain networks. MDPI. Sustainability. 9(1), 144. doi:10.3390/su9010144

[29] Zhao. S., Liu. X., Zhuo. Y. (2017). Hybrid Hidden Markov Models for resilience metrics in a dynamic infrastructure system. Reliability engineering and safety systems. Elsevier. http://www.sciencedirect.com/science/article/pii/S095183201730248X accessed on November 17, 2017

[30] Ganin et al (2017). Resilience and efficiency in transportation networks. Science Advances, 3(12): e1701079

[31] Kabir, G., Sadiq, R. and Tesfamariam, S. (2014). A review of multi-criteria decision-making methods for infrastructure management, Structure and Infrastructure Engineering, vol. 10, no. 9, pp. 1176-1210.

[32] Greiner, R., Herr, A., Brodie, J., and Haynes, D. (2005). A multi-criteria approach to great barrier reef catchment (Queensland, Australia) diffuse-source pollution problem, Marine Pollution Bulletin, vol. 51, no. (1–4), pp. 128–137.

[33] Jovanović, A. et al. (2020): Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards; Environment Systems and Decisions, June 2020 https://doi.org/10.1007/s10669-020-09779-8

[34] Fox-Lent, C., & Linkov, I. (2018). Resilience Matrix for Comprehensive Urban Resilience Planning. In: Resilience-Oriented Urban Planning (pp. 29-47). Springer, Cham

[35] Fox-Lent, C., Bates, M.E., & Linkov, I. (2015). A matrix approach to community resilience assessment: an illustrative case at Rockaway Peninsula. Environment, Systems, and Decisions, 35: 209-218

[36] ISO23316 - Security and resilience — Organizational resilience — Principles and attributes, ISO https://www.iso.org/standard/50053.html

[37] Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., and Baker, T. (2018). “Security threats to critical infrastructure: the human factor.” *The Journal of Supercomputing*, 74(10), 4986– 5002.

[38] Gouglidis, A., Shirazi, S. N., Simpson, S., Smith, P., and Hutchison, D. (2016). “A multi-level approach to resil-ience of critical infrastructures and services.” *2016 23rd International Conference on Telecommunica- tions (ICT)*, IEEE, Thessaloniki, Greece, 1–5.

[39] König, S., Schaberreiter, T., Rass, S., and Schauer, S. (2019). “A Measure for Resilience of Critical Infrastruc- tures.” *Critical Information Infrastructures Security*, E. Luiijf, I. Žutautaitė, and B. M. Hämmerli, eds., Springer International Publishing, Cham, 57–71.

[40] Martin, H., and Ludek, L. (2013). “The status and importance of robustness in the process of critical infrastructure resilience evaluation.” *2013 IEEE International Conference on Technologies for Homeland Secu- rity (HST)*, IEEE, Waltham, MA, USA, 589–594.

[41] Royal Academy of Engineering. (2018). *Cyber safety and resilience - strengthening the digital systems that support the modern economy*. London.

[42] Tokgoz, B. E., and Gheorghe, A. V. (2013). “Resilience quantification and its application to a residential build- ing

subject to hurricane winds." *International Journal of Disaster Risk Science*, 4(3), 105–114.

[43] Walker-Roberts, S., Hammoudeh, M., and Dehghantanha, A. (2018). "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure." *IEEE Ac- cess*, 6, 25167–25177.