An indicator-based approach to assessing resilience of smart critical infrastructures

A. Jovanovic, K. Øien, A. Choudhary

1 Introduction

1.1 Resilience of critical infrastructures

The overall resilience of modern societies is largely determined by and dependent on resilience of their critical infrastructures such as energy grids, transportation systems, governmental bodies and water supply. This is clearly recognized by the European Union in its policies and research agenda, such as the DRS (Disaster-Resilience) actions and projects safeguarding and securing society, including adapting to climate change [12]. In this context, the issue of "measuring resilience" has an important place and it is tackled primarily by means of indicators, within the DRS-14 line of calls [12] emphasizing the need for "… a better understanding of critical infrastructure (and)… for defining measures to achieve a better resilience against threats in an integrated manner including natural and human threats/events (e.g. due to human errors or terrorist/criminal attacks)…". The overall goal of the current research agenda is, hence, to improve current approaches by providing an innovative "holistic" methodology for assessing resilience of critical infrastructure. The methodology proposed here is based on resilience indicators. The EU does not provide a clear definition or framework for tackling the concept of resilience – single projects and activities currently follow a number of often quite different paths. Thus, one main goal of the recent research agenda is to establish common frameworks, approaches, definitions and guidelines.

Resilience concepts have been developed by the Federal Agency of Emergency Management (FEMA), which is a part of the United States Department of Homeland Security (USDHS) [13], by the OECD [27] and the United Nations Office for Disaster Risk Reduction (UNISDR) [45]. New research, initiated by the EU Horizon 2020 projects like Resilens [37], Resolute [38], Darwin [7] and SmartResilience also addresses the issue of developing resilience approaches [40]. The need for guidelines and frameworks for resilience is particularly important in the areas of IT security and related critical infrastructures, which may be considered as "smart infrastructures". While the information technology provides more and more possibilities to make critical infrastructures "smarter", it also creates more risks and vulnerabilities [44]. The EU research project SmartResilience makes an attempt of

combining a common framework for resilience with the need to adapt this framework to new technology related risks and opportunities.

The basic idea is that modern critical infrastructures are becoming increasingly "smarter" (e.g. "smart cities"), providing an increasing amount of data and thereby, the possibility to measure resilience by using big and open data indicators. Following this idea and the objectives of the project, SmartResilience defines resilience of an infrastructure as "*Resilience of an infrastructure is the ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions*" [20].

Making an infrastructure "smarter" usually means making it smarter in normal operations and use. Further, these "smarter" systems may be characterized by the following features [22]:

1. Integrative and interconnected
2. Intelligent by the use of ICT, web technology and smart computing
3. Smart governance oriented, inclusive of end-users
4. Sustainable/progressive/future-oriented
5. Efficient and maximize service

However, it has to be checked if such a smart critical infrastructure (SCI) will behave equally "smartly" and be "smartly resilient" also when exposed to extreme threats, such as extreme weather disasters or, e.g., terrorist attacks. Similarly, the question is, 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 in its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? These questions are of increasing interest for the research community. Thus, the SmartResilience project is developing a new, advanced, resilience assessment methodology, which takes the vulnerability of SCIs into account in a holistic manner. This methodology is based on the identification of existing and new, smart indicators of resilience [40].

1.2 Challenges of smart critical infrastructures

The approach proposed here assumes that an event challenging the resilience of modern infrastructure will potentially be an emerging risk [21]. Emerging risk is understood as a risk not necessarily well known and spreading increasingly in its infrastructural context over time, leading to cascading and ripple effects. Figure 6 visualizes an example for such an emerging risk, a man-caused release of toxic aromatic liquids. Policy priorities in such a situation can, and often will, evolve over time. Thus, emerging risks, especially if combined with Smart Critical Infrastructures (SCIs), represent a challenge for both infrastructure owners and the policy-makers.

The SmartResilience project [40], proposes a new approach to tackle the specific emerging challenges to the resilience of SCIs. The approach includes a shift from

the common V-model established in the resilience literature [2] [26] to an adapted UV-model [19] as shown in Figure 1.

Further, with the indicator-based approach, one of the pressing challenges to find trends and patterns in the large and high-dimensional datasets can be captured in intuitive indicators of high practical use. Many infrastructures lend themselves exceptionally well to be analyzed from a complex network perspective [2]. Many real-world networks (such as communication networks, metabolic networks, or social networks) have a surprising high degree of robustness with respect to random errors or perturbation. However, this robustness comes at the high price of extreme vulnerability to targeted attacks. Network science methods have resulted in actionable information on network vulnerabilities in response to disruptive events in the context of transportation [15], power [41], and communications [9]. An additional challenge in the design of resilient infrastructures is that multiple interdependencies between mutually dependent networks induce an additional component of fragility [9], see also Figure 6.

The challenges for applying the approach are, obviously, greater when dealing with more complex infrastructures, and, generally, the “smart infrastructures” are more complex than the conventional infrastructures.

2 Basic idea of the approach

As mentioned in the introduction, in order to keep pace with new emerging risks and Smart Critical Infrastructures, it is crucial to develop new methodologies and tools; hence, it uses the UV model. Further, when it comes to resilience of critical infrastructures, the "UV"-model (or –curve) is more suitable, because "tipping points" are not of main interest, whereas the response phase is highly relevant. Since the response necessarily takes some time, a flat bottom curve is more representative, than a "V"-curve [22]. Moreover, the "UV"-model (or –curve) is more of a conceptual model. In reality, it will hardly be a smooth curve. It is more likely to fluctuate, making it difficult to model. Moreover, if there are interdependencies and cascading effects, several curves are needed to represent resilience graphically.

In addition, new smart resilience indicators can potentially be built upon [39]:

1. Indicators not specifically envisaged as resilience indicators, possibly already accepted and applied in related areas, such as risk, safety, business continuity, sustainability, e.g. those proposed by OECD, GRI, API, HSE, IAEA and other organizations;
2. New resilience specific indicators proposed by experts (the “conventional way” of creating and using indicators), including those proposed in standards;
3. New resilience indicators derivable out of Big Data and Open Data.

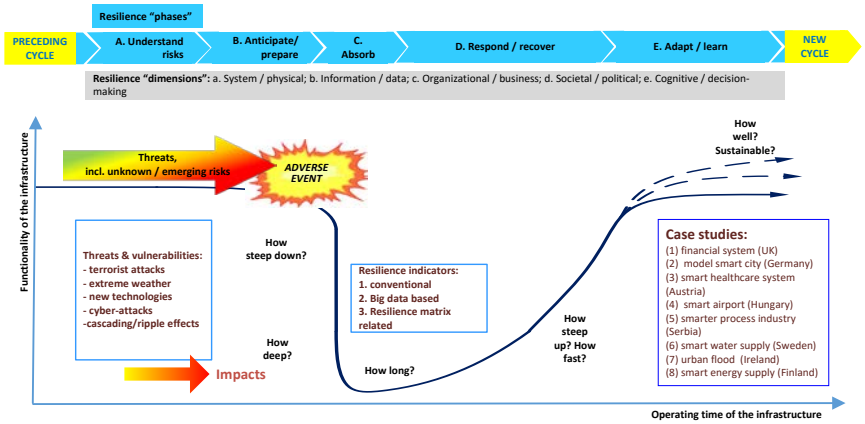

Figure 1: Resilience UV curve in SmartResilience project

The indicators can be, e.g., "supervised" or "unsupervised", lagging or leading, basic or more sophisticated, more or less dynamic. In principle, unconventional indicators can be considered to be "smarter" and, thus, are more appropriate in order to measure "smart resilience indicators". Each of the above sources might provide useful indicators for single phases of the resilience cycle (Figure 1).

Phase A, *understand risks*, is applicable prior to an adverse event. It emphasizes the emerging risks (ERs) and includes their early identification and monitoring; e.g. what could the "adverse event" be? This is followed by phase B, *anticipate/prepare*, also applicable before the occurrence of an adverse event. It includes planning and proactive adaptation strategies, possibly also "smartness in preparation" [20]. Phase C, *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 D, *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 includes the post event recovery; e.g. "how steep up" is the recovery curve for normalization of the functionality? It is followed by phase E, *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 the future events and hence, this resilience curve also exhibits a reoccurring cycle [20].

These five phases along with five resilience dimensions form the 5×5 SmartResilience resilience matrix (RM) as shown in Table 1. The dimensions help in categorizing the indicators. Dimension a, *system/physical*, includes technological aspects of the given infrastructure, as well as the physical/technical networks being part of a given infrastructure, and interconnectedness with other infrastructures and systems. Dimension b, *information/data*, is also related to the technical systems but is dealing with information and data, specifically. Further, dimension c, *organizational/business*, covers business-related aspects, financial and HR aspects

as well as different types of respective organizational networks. Dimension d, *societal/political*, encompass broader societal and social context, also stakeholders not directly involved in the operation and/or use of the infrastructure (e.g. social networks). Lastly, dimension e, *cognitive/decision-making*, accounts for perception aspects (e.g. perceptions of threats and vulnerabilities) [20].

Table 1: Resilience Matrix: Resilience indicators in different phases of the resilience cycle and resilience dimensions [20]

Phases →→→ vs. Dimensions ↓↓↓	A. Understand risks	B. Anticipate / prepare	C. Absorb / withstand	D. Respond / recover	E. Adapt / learn
a. System / physical					
b. Information / data		5×5			
c. Organizational / business					
d. Societal / political					
e. Cognitive / decision-making					

Depending on a given situation (infrastructure, scenario) all the sources may yield, often a large number of, indicators for all the phases of the resilience cycle. However, for practical purposes too many indicators may become a burden, especially in the case when the resilience of different infrastructures should be compared. In practice, the indicators cannot be considered neither independent, nor standardized. Ideally, in such a case, one would prefer dealing with one resilience indicator only. One indicator might be good for comparison, but it can hardly represent the complexity of practical situations (e.g. complex scenarios, unknown responses, uncertainties). The methodology being proposed in the SmartResilience project [21], [40], shown in Figure 2 and explained in Section 4, tries to combine the advantages of "one resilience indicator" (convenient for use, but not transparent) with the advantages of many indicators (transparent, but cumbersome).

For collecting the indicators and applying the approach, the theoretical framework for variable selection, weighting, and aggregation must be defined [6]. Once when the set of indicators is considered/accepted as representative, the

dynamic/"smart" resilience assessment "check-lists" can be created and used for the assessment of the respective SCI (e.g. water, energy, smart city) as described in Section 7.

3 Scenarios: Threats and infrastructures

The project covers 8 scenarios with a mix of infrastructures and related threats in order to assess the resilience of the smart critical infrastructures (SCIs), and in addition one hypothetical case to simulate a case showing cascading effects. The cases are ordered as per the phonetics [35] from ALPHA to INDIA as shown in Table 2.

Case 1 (ALPHA) of smart finances in the city of London emphasize to consider any disruptions to business continuity, whether it is a terrorist attack, cyber-attack or a natural threat such as a hurricane [4].

Case 2 (BRAVO), i.e. Heidelberg in Germany, considers terrorist attack and cyber-attack as major threats to their infrastructure [4], whereas natural threats such as urban floods are considered partly applicable.

Case 3 (CHARLIE) of smart health care system infrastructure (in Austria) considers cyber-attack leading to massive breach of privacy as the prime threat to their CI. Increasingly, terrorist attacks are also considered important. Further, different scenarios are considered important such as disasters and man-made crises that may lead to challenges in normal mode of operations or events leading to exceeding the capacity of emergency departments and failures in other critical infrastructures such as power supply for hospitals [4].

Case 4 (DELTA), i.e. smart transportation system of an airport in Hungary, considers terrorist attacks as most important threat. Besides this, property crimes endangering or disrupting operations, malevolent use of airport systems or airplane, attacks or incidents from outside the airport (UAV fly-in, firing lasers at approaching airplanes), accidents and disruptions caused by human negligence as well as strikes, are considered as specific threats. Natural disasters are second in importance for this case [4].

Case 5 (ECHO), i.e. smart industrial system case in Serbia, identifies terrorist attack, cyber-attack and extreme weather conditions as most important threats and these could possibly lead to interruptions in the critical supply chains.

Case 6 (FOXTROT), i.e. smart water supply in Sweden, evaluated climate change related events as crucial to the drinking water supply leading to either shortage or a heavy rainfall leading to contamination [4]. Also, cyber-attack is consider important in relation to security/ICT/human error.

Table 2: Critical infrastructures and threat scenarios

Infrastructure (CI) / Scenarios	Terrorist attack	Cyber attack	Natural threats	CI-specific events
Case 1 (ALPHA): Smart finances (UK)	✓	✓	✓	Disruptions leading to business continuity e.g. cyber risks, climate risks
Case 2 (BRAVO): Smart cities (Germany)	✓	✓	(✓)	Social unrest, urban floods
Case 3 (CHARLIE): Smart health care (Austria)	✓	✓	(✓)	Massive breach of privacy, disruption in power supply, scenarios of disasters and man-made crises, interconnected events
Case 4 (DELTA): Smart transportation (airports, Hungary)	✓	✓	(✓)	Disruption of airport services
Case 5 (ECHO): Smart industrial/production plants (Serbia)	(✓)	✓	(✓)	Industrial accidents
Case 6 (FOXTROT): Smart water supply (Sweden)		✓	✓	Climate change leading to water shortage, heavy rainfall leading to heavy water contamination
Case 7 (GOLF): Smart city (Ireland)			✓	Flash floods in urban areas leading to disruption of several CIs
Case 8 (HOTEL): Smart energy supply systems (Finland)		✓	✓	Interruption of coal supply & district heating
Case 9 (INDIA): Integrated Virtual case Study (Combined scenarios in all SCIs)	✓	✓	✓	Cascading effects

Applicability: ✓- yes, (✓) - partly

Case 7 (GOLF), i.e. city of Cork, has been vulnerable to extreme weather and flooding events in urban areas leading to disruption of several CIs [4].

Case 8 (HOTEL) of smart energy supply system in Finland recognizes cyber-attack and extreme weather conditions as major threats. Also, interruption in critical

supply chain such as coal supply and district heating are of considerable importance [4].

Case 9 (INDIA) is a hypothetical integrated case as shown in Figure 6, considering multiple infrastructures and multiple threats leading to cascading and ripple effects.

4 Assessment methodology

4.1 Reference approaches

The methodology developed in the SmartResilience project [40] is based on several previous methods, notably the ANL/Argonne method [14], the Leading Indicators of Organizational Health (LIOH) method [10], [11], [33], and the Resilience-based Early Warning Indicator (REWI) method [30], [29], [31], [32].

The ANL/Argonne method for assessing a resilience index (RI) is structured in five levels, providing indicators on the lowest level. A similar hierarchy is used in the SmartResilience project for assessing resilience levels, entering the indicators on level 6. The structure is somewhat similar in the two approaches, and many of the resilience attributes are the same; however, the level at which the various resilience attributes are found, differs between these two methods.

The LIOH method focused on developing indicators for a set of seven themes important for the "health" of a nuclear power plant, some of which have their roots from the research on high reliability organizations (HRO) [46]. They also formed part of the basis for factors considered important in resilience engineering. The LIOH method uses three distinct terms for the levels in their structure of the method. These are *themes*, *issues* and *indicators*. The issues are in principle divided in general issues and specific issues (for nuclear power plants); however, in some of the applications it was regarded as sufficient to use only one common level for the issues.

This idea was brought further to the REWI method, using three levels to identify early warning indicators for resilience, i.e. starting with resilience attributes, followed by issues important for these resilience attributes, and finally develop indicators to measure the issues. In REWI, the level of resilience attributes is not termed themes as in LIOH, but rather *contributing success factors* (CSFs). Thus, the structure consists of *CSFs*, *issues* and *indicators*. The CSFs are determined based on identification of factors contributing to successful operations including recovery of potential incidents, prior to causing any accident with consequences; thus the term contributing success factors [43]. They are structured in two levels, of which the lowest level consists of eight factors, or resilience attributes. The CSFs are partly, but not entirely sequential.

4.2 Basic idea and assumptions

In SmartResilience, the resilience attributes are based on the definition of resilience used in the project [40], described in the introduction. From the definition, the five phases of the resilience cycle, presented in Table 1, are obtained.

For each of these phases, the issues that are important for them are identified, and indicators to measure those issues are developed. Thus, the three lowest levels in the SmartResilience structure are *phases*, *issues* and *indicators*. In addition, the issues (and corresponding indicators) are structured according to five dimensions [20], also presented in Table 1. These phases and dimensions forms the Resilience Matrix, as illustrated in Table 1 and Figure 2. Variations of such resilience matrices exists in the literature (e.g. Linkov et al. [25], IMPROVER project [18] and READ project [36]).

One difference with the 5×5 matrix in SmartResilience, compared to some other matrices proposed (4×4, 7×3, etc.) is that the dimensions are only used for structuring the issues and indicators, and to support the identification of issues. It is the phases which are important and it is not necessary to fill every cell in the matrix with issues and indicators. The cells themselves have no part in the calculations of the resilience levels.

4.3 Levels of assessment

In addition to the three lower levels of the structure, i.e. phases, issues and indicators, the overall structure consists of three more levels. Starting from the top, is the area level, e.g. a city or smart city, for which the degree of "smartness" will differ, but the assessment methodology applies for all cases. The second level consists of the critical infrastructures (CIs), and the third level deals with the threats. The overall structure of the SmartResilience methodology is illustrated in Figure 2.

Since the users performing resilience assessments of their area/city, critical infrastructures and/or specific threats are not assumed to be resilience or risk experts, the SmartResilience methodology is deliberately kept as simple, transparent and easily understandable as possible. Thus, there is reluctance to add additional levels or crosscutting topics, which will increase the complexity of the model. All models are simplifications of reality, and it will always be a balance between having a model that is simple and transparent on one hand, and being sufficiently realistic on the other hand.

Three specific features are treated within the six level structure. These features are related to how to deal with the Information & Communication Technology (ICT) infrastructure as an overarching infrastructure, how to deal with cascading effects, interdependencies and interactions, and finally, how to deal with the potential vulnerability and opportunities of smart features being increasingly introduced in critical infrastructures.

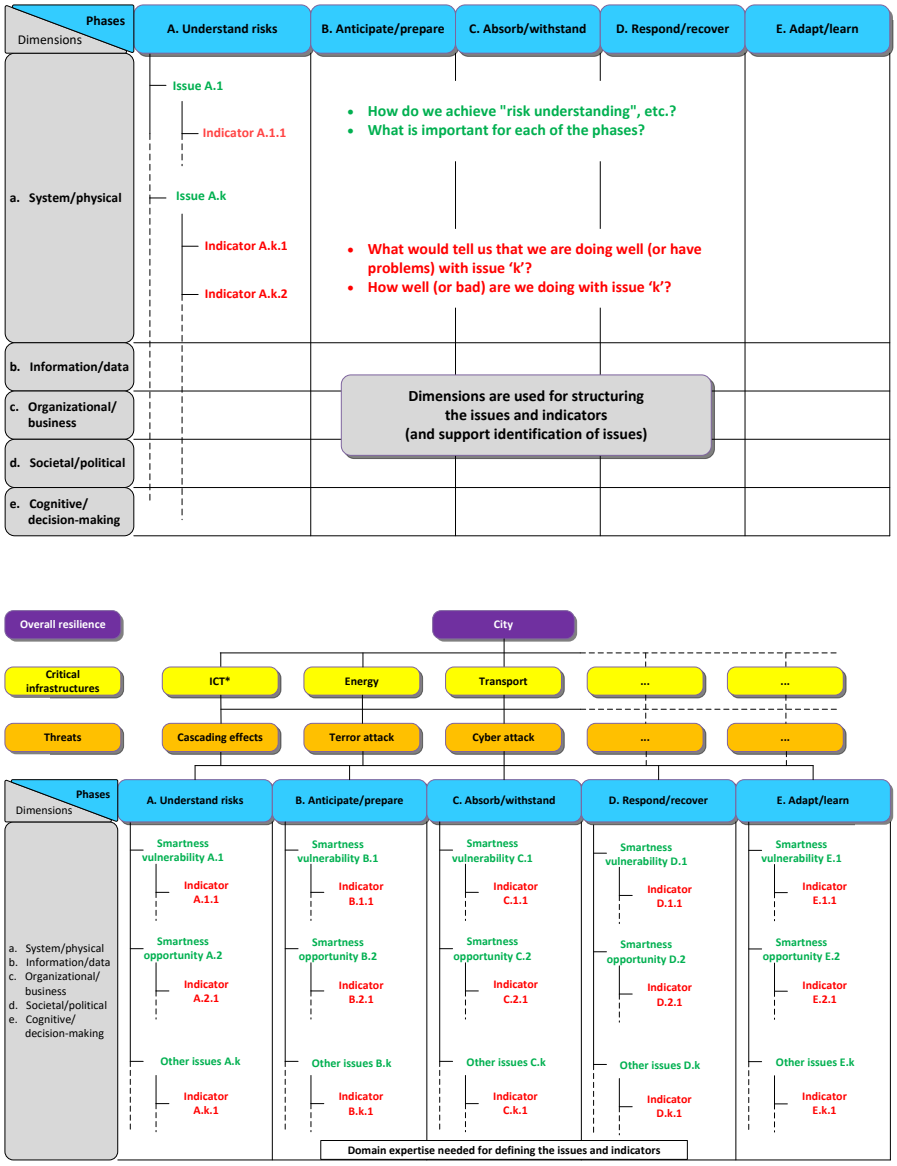

Figure 2: Basic outline of the methodology

The ICT infrastructure may affect several of the other critical infrastructures, and this need to be explicitly considered as a potential issue when issues are defined in the resilience matrix for the ICT infrastructure. This is indicated in Figure 2 adding an asterisk, i.e. ICT*. Cascading effects are treated as a specific type of threat, also shown in Figure 2. Other types of interdependencies or interactions may also be

treated as specific threats, and added as indicated by "others/specify" in Figure 2. Smart features ("smartness") of critical infrastructures are included explicitly as smartness vulnerability and smartness opportunity on issue level. These are default issues (candidate issues), for which the relevance should be considered for all phases in all types of assessments.

Another specific issue, which could be treated on issue level, is related to one of the distinctions between resilience assessment and risk assessment, which is the focus on the unexpected, and how well a city/area or critical infrastructure, is prepared for the unexpected. This can be explicitly focused by e.g. measuring the number of incidents/accidents not included in the response plans, and the degree of learning from incidents/accidents experience by others, which may occur in your own case, but not being included in the response plans. This could be included as issues in the adapt/learn resilience phase.

Two important general features of the methodology are its flexibility, and its 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 city or area using the methodology to decide which infrastructures that are critical for them. Similarly, no fixed list of threats exists, neither on area level nor for the single critical infrastructures. Thus, it will be up to the users to define which threats they consider relevant. This is shown in Figure 2 with "others/specify" both for critical infrastructures and threats.

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 with close collaboration between the users, the method developers, and the IT developers (of calculation and presentation tools).

4.4 Resilience index

The SmartResilience method steps are as follows:

Step 1. Select the area, e.g. a smart city – *Level 1*
Step 2. Select the relevant critical infrastructures (CIs) for the area – *Level 2*
Step 3. Select relevant threats for each critical infrastructure – *Level 3*
Step 4. Consider each phase for each threat – *Level 4*
Step 5. Define the issues within each phase – *Level 5*
Step 6. Search for the appropriate indicators for each issue – *Level 6*
Step 7. Determine the range of values (best and worst) for each indicator
Step 8. Assign values to the indicators
Step 9. Perform the assessment (e.g. by calculating the score(s))
Step 10. Use results for e.g. comparison, benchmarking and "stress-testing"

The assessment of resilience can be performed at different levels, e.g. for an entire city or some other area, for one or more critical infrastructures, and for one or more threats. It may also be an assessment of a particular threat within an area, affecting certain critical infrastructures, e.g. flooding in a city affecting water supply, energy and transport. The term "scenario" is used here, for a specific selection of critical infrastructures and threats for a given area/city, i.e. the selected area, critical infrastructures and threats.

Steps 1-6 are selections and considerations related to the six levels of the methodology as explained previously, whereas steps 7-10 are related to the calculations and the use of the results.

Any type/form of indicators are considered appropriate in the SmartResilience methodology, meaning that they can be yes/no questions, numbers, percentages, portions, or some other type. Their real values, of whatever type, are collected and transformed to a *score* (or rating) on a scale from 1 (worst) to 5 (best). This requires the determination of best and the worst values for each indicator, i.e. Step 7. The score is obtained by interpolation between the best and worst values.

At every level, there is a possibility to give *weights*; however, it is recommended to be restrictive with the use of different weights as this will lead to less transparent calculations and results. Thus, equal weights are the default values at all levels.

When performing the resilience assessment, the indicators' real values are entered into the calculation (Step 8), and the issue scores are obtained as average weighted scores of the indicator scores. Thus, also issues (level 5) are measured using scores on a scale from 1 to 5, similar as the indicators (level 6). It is also 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.

On the next higher level (level 4 – phases), the scores are transformed to a scale from 0 to 10, providing *resilience levels*. This scale is kept from phases and upwards, i.e. for threats (level 3), critical infrastructures (level 2) and areas (level 1).

The reasoning behind the selected scales is that a scale from 1 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 [28]. A main goal of the SmartResilience project has been to develop a method for assessing level of resilience using a scale approach of resilience level, which was included in the call text for the project [39]. This has similarities to the use of safety integrity levels (SIL) for safety instrumented systems [17], only using integer values from 0 to 4. However, in SmartResilience the resilience levels are increased to a scale from 0 to 10, which is considered to provide sufficient differentiation, and at the same time not give the illusion that the assessment is more accurate than it can really be.

The calculation is performed in a database and the assessment for the given case/scenario is saved (Step 9). The structure of an example case in the database is illustrated in Figure 3. Only the selections made at each level are shown, since the "complete" structure for the most complex case may consist of thousands of nodes.

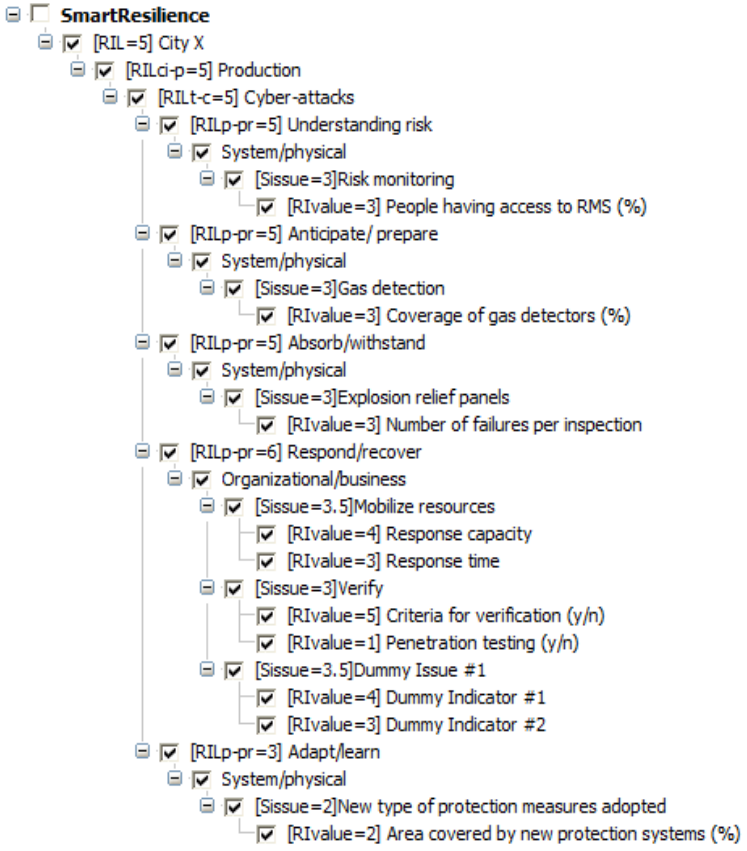

Figure 3: Calculation performed in database

The results of the resilience assessment, which in the case of a full scope assessment for a smart city covers all the relevant critical infrastructures, all relevant threats for each critical infrastructure, all five phases of the resilience cycle, all relevant issues for each phase and all indicators for measuring the issues, can be used in various ways (Step 10). One is to compare with previous assessment, i.e. providing a trend showing how the level of resilience is progressing. Since the calculation is performed on all levels, it is also possible to "drill down" and identify the reason for an increase or decrease in resilience compared to the previous assessment. Another use is to compare with other cities, areas or critical infrastructures, i.e. to benchmark against others, which provides the opportunity to learn from others. The resilience of a city/area or a critical infrastructure can also be assessed by imposing a set of threats (including defined challenges such as interactions and cascading effects), i.e. stress-testing the resilience ability of the city/area/critical infrastructure, and compare the results with predefined criteria. This is further described in Section 7.

4.5 Use cases

Selected use cases have been employed during the development of the structure of the model, the mathematical equations and the overall calculations. The development and testing of the equations and calculations have been performed independently using the SmartResilience database, in a progressive manner starting from simple and transparent examples, such as case dealing with one threat and one infrastructure to cases dealing with multiple threats, multiple smart critical infrastructure and ripple effects.

The three use cases have been selected from the eight case studies in the SmartResilience project. The three use cases are:

1. Refinery in the city of Pančevo in Serbia, representing production/supply as a critical infrastructure

2. Heidelberg Bahnstadt in Germany, representing a smart city/area

3. Budapest Airport in Hungary, representing a critical transport infrastructure

Use cases #2 and #3 have only been used to develop the structure, not for any calculations, whereas use case #1 has been used for development of the equations and calculations. The use cases (sample application cases) are further described in Section 5.

5 Implementation of the methodology

5.1 Data collection

The data collection is performed in phases and are refined through an iterative process. It consists of relevant issues and corresponding indicators that are used in each case (as specified in Section 3) to measure the resilience of the respective infrastructure.

In the initial phase, the preliminary collection of over 450 resilience indicators was compiled. The prime proportion of these are conventional indicators and only a small proportion represent the big data indicators. This collection of indicators will be further refined after domain experts search for specific issues in every scenario and a final list of indicators will be devised. Then, these indicators are structured according to the methodology [20] into phases of the resilience cycle as explained in Section 4.

5.2 Tools – visualization

Considering that the number of indicators to assess the resilience and the data related to each of these indicators especially big data can be overwhelming to analyze and create problems in understanding the impact of any disruptive event and the corresponding cascading effects on the critical infrastructure. Hence, it is crucial to use data visualization to ease the process. In order to do so, D3 (Data-Driven

Documents) a JavaScript library is used. It brings data to life through its interactive visualization tools [8] and will support the indicator based methodology to measure resilience of SCI and inform decision making.

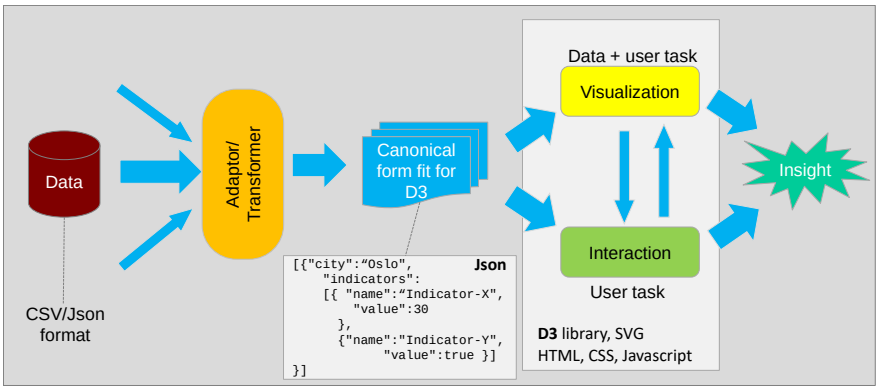

Figure 4: Design and Application of interactive visualization for RIs

As shown in Figure 4, the data in the CSV or Json format is transformed into canonical form to fit in D3 and provides insights which are easy to visualize and interactive to the user needs.

6 Sample application cases

6.1 A smart city

One of the use cases introduced in Section 4.5, use case #2, is Bahnstadt in Heidelberg, Germany. It constitutes an example/representation of a smart city, or smart community/neighborhood, i.e. a defined area within the city of Heidelberg.

Bahnstadt in Heidelberg is one of Germany's largest urban development projects. It is designed to be Heidelberg's first smart neighborhood. Bahnstadt is located in the southwestern part of Heidelberg's city center, and it shares a border with the main station. The energy concept consists of passive house standards as a universal construction method, district heating supply to be covered in the medium term by renewable energies, and intelligent control of power consumption using smart metering. Bahnstadt being the first smart neighborhood is dependent on the critical infrastructure: Stadtwerke Heidelberg (SWH) [42] [4].

SWH provides its customers in Heidelberg and the region with reliable electricity, gas and heat, and offers many services related to energy saving and climate protection. On behalf of the city of Heidelberg and other communities, they are also responsible for water supply. In addition, SWH operates the swimming pools, the cable cars, garages, and also controls the city coordination tasks and are a part of the funding for public transportation. With a turnover of over 200 million euros and more than 1,000 employees, of which around 350 are on loan to the regional

transport company, it is a major employer in Heidelberg. As one of the largest public energy suppliers, SWH along with the City of Heidelberg and other partners is leading the way into providing electricity without any nuclear power. The energy concept 2020 shows the way to this goal: with a clear plan of action along the entire value chain of an energy supplier – this includes measures for greater energy efficiency and expanding renewable energies - from generation and storage through offering products [42]. According to Bundesministerium des Innern [5] "Definition of Critical Infrastructures" SWH belongs to the Critical Infrastructure Sectors "Energy" and "Water" and the subsectors "Electricity" and "Public Water Supply" [4].

In general, the Heidelberg case study covers multiple critical infrastructures, which are exposed to multiple threats requiring resilience in all phases through multiple issues measured by multiple indicators; however, in the simplified use case referred to in Section 3, only one critical infrastructure, one threat and one phase are included. The threat selected – terrorist attack – is one of the three main threats identified by SWH, the other two being flash floods and cyber security breach [4]. Some of the important issues identified for resilience against terrorist attacks are surveillance, communication and training [4]. This is illustrated in Figure 5, including examples of potential indicators to measure the issues. It is not distinguished between the different dimensions.

6.2 Smart production (refinery)

Use case #1, introduced in Section 4.5, is a refinery in an industrial zone of the city of Pančevo in Serbia, representing (smart) production/supply as a critical infrastructure.

City of Pančevo with its Southern Industrial Zone is chosen to represent a case study for the resilience of critical infrastructures as a representative of industry sector, with many recognized threats in the neighborhood, in a smart city. In order to perceive and understand the influence of industry in the sense of resilience it is necessary to cover the impact of each individual risk factor in this industrial zone as well as the impact of this zone on other systems of smart city [4].

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

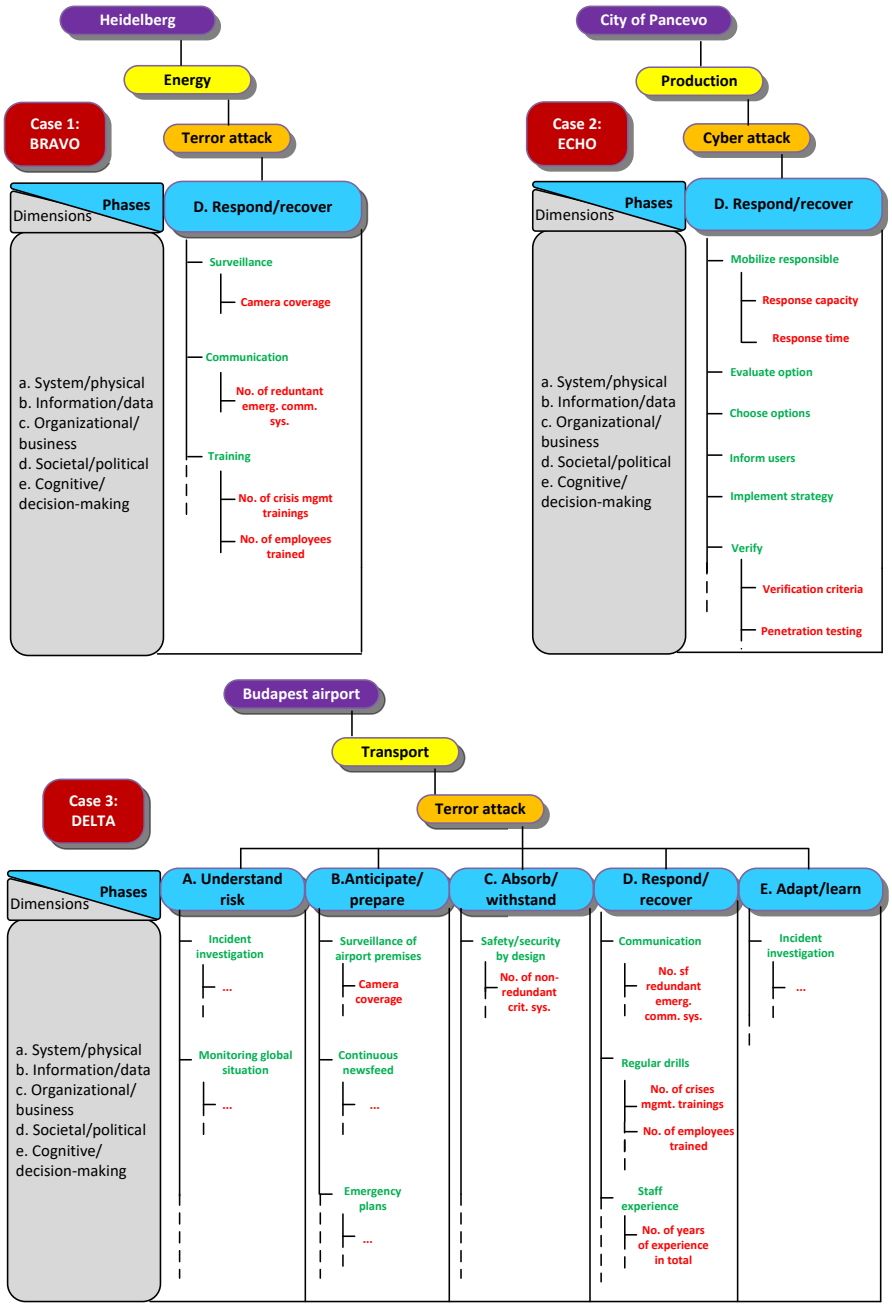

Figure 5: Examples of different scenarios for the use cases BRAVO, ECHO & DELTA

In general, the industrial zone is an area covering one type of critical infrastructure (although multiple plants), is exposed to multiple threats, and needs to be resilient in all phases through multiple issues measured by multiple indicators. In the simplified use case referred to in Section 4.5, only one single plant and one threat are included; however all phases are covered, but only for the calculations. The threat selected is cyber-attack, although this is not explicitly highlighted by the stakeholders [4]; thus, this use case is somewhat fictitious. The main emphasis of this use case was the development of the calculations. The scenario is illustrated in Figure 5, with some examples of issues and indicators. Only the phase respond/ recover is shown.

6.3 Smart transportation

Use case #3, introduced in Section 4.5, is the Budapest Airport in Hungary, representing a smart transportation critical infrastructure.

The Budapest Liszt Ferenc International Airport is the largest international airport in Hungary and is built at the easternmost limits of the Hungarian capital city, Budapest. The total land area of the facility is 15,050,000 square meters, 25% larger than London Heathrow International Airport [3]. The facility has both commercial (passenger, cargo) and general aviation traffic, but is also occasionally serving military airplanes (e.g. KC-130s [24] airplanes in the Balkan wars). In 2015, the commercial aviation served 10,298,963 passengers, 92,214 airplanes and 91,421 tons of cargo with coordinated work of approximately 12,000 people [1], [4].

Currently, BLFNR is the second most protected critical infrastructure in Hungary. The level of security is provided by a well-coordinated cooperation of authorities (including first responders) and private companies, with the airport operator company in the first place. With 52 flight companies, 8 authorities, 3 ground handling companies, 27 shops and so on, there are more than one hundred of actors, all obliged to take its part in protection of the airport as a critical infrastructure [4].

In general, an airport is a specific type of critical transportation infrastructure, exposed to multiple threats requiring resilience in all phases through multiple issues measured by multiple indicators. In the simplified use case referred to in Section 3, only one threat is considered; however all phases, and multiple issues and indicators are included. Terrorism is considered one of the main threats, and are selected in this use case. Issues identified as important are e.g. drills, staff experience, communication, and incident investigation [4]. This is illustrated in Figure 5, including examples of potential indicators to measure the issues. All phases are covered, but it is not distinguished between the different dimensions.

The sample application cases are illustrated using only specific limited scenarios. The threats are selected from those considered as important by the sample application cases themselves [20] and the same is true for the issues (except for use case #1, where the issues were identified in a separate workshop by the method developers). When the method is tested in the case studies in the SmartResilience project, including the three use cases, it is important that domain experts identify all

relevant issues and indicators for all phases, all relevant threats, and all relevant critical infrastructures. This will provide a full scope testing of the calculation of the resilience level on all relevant levels.

As an alternative to define issues first and then indicators, it is possible to start with existing indicators in use and ask what issue they actually measure, and then consider if these issues are of sufficient importance to be included in the overall resilience model. Further, the database of collected (resilience) indicators in the SmartResilience project can be reviewed in order to (i) determine if some of these are relevant as supplementary indicators for measuring the already identified important issues, or (ii) determine whether some of the indicators are relevant measures of new issues.

7 Conclusions: Comparison, benchmarking and stress testing of resilience in different CIs

The examples presented in Chapter 6 integrate smoothly into a “smart city” integrative example (see Figure 6). In other words, the “smart city example” is the integration platform for different critical infrastructures including the examples considered in Chapter 6.

The approach presented in this contribution is a snapshot of the development efforts in the SmartResilience project (end of 2016). The approach is at this point in time still under development and it is expected to be extended in the direction of its applicability for other features (models/tools) within the project ([22], [23], [40]):

- the “resilience cube”
- the “dynamic checklists” and
- the resilience indicators based on and derived from the “big data”

Comparing this approach to some of those applied elsewhere ([6], [13], [25], [26], [27]), one can see that its orientation onto critical infrastructures and use of indicators, make it probably more adapted for the quantitative resilience assessment. This enable improved qualitative assessment was one of the main goals of the resilience model development in the SmartResilience project.

Once when developed and implemented in terms of the IT tools, it will enable improved assessment, comparison, benchmarking and stress testing of resilience in different critical infrastructures, in particular the “smart” infrastructures. Basic idea of this type of use of the approach is shown in Figure 7, showing that, for instance, the comparison of resilience in different phases in the resilience cycle can be done in a very intuitive and transparent way. The stress-test of resilience for all infrastructure is, on the other hand still an open issue which has to be explored in due course.

Particular challenges to be addressed are those related to the cascading/ripple effect in multi-infrastructure systems (e.g. Figure 6) and consistent consideration of time in the analysis.

Acknowledgements

The contribution is based on the Grant Agreement No. 700621 supporting the work on the SmartResilience project provided by the Research Executive Agency (REA) ('the Agency'), under the power delegated by the European Commission ('the Commission'). This support is gladly acknowledged here, as well as the collaboration of all the partners and their representatives (persons) involved. Special thanks go to Mr. M. Jelic of EU-VRi for the IT support.

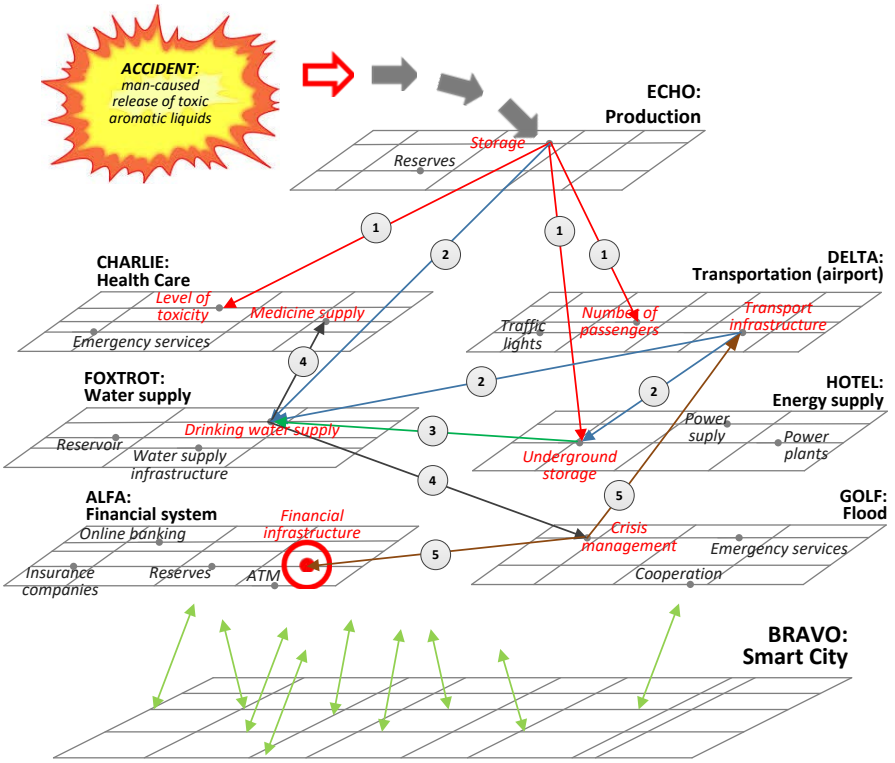

Figure 6: Interaction between the SCIs in a hypothetical case taking place in a "Smart City" (The SmartResilience "integrative" hypothetical case [39], [40])

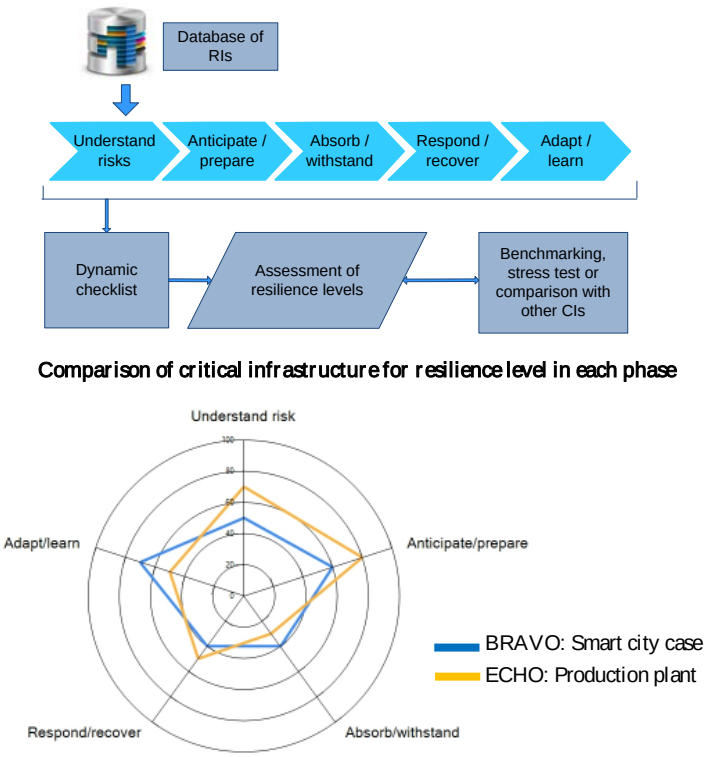

Figure 7: Application of the approach for benchmarking, stress test and comparison of resilience of different CIs

References

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

[2] Albert R., H. Jeong, A. L. Barabási (2000). Error and attack tolerance of complex networks, *Nature 406*, 378-382

[3] Allet, T. (2004). *Budapest 'New' EU Airport*, Airports International, 37(4) 37-39.

[4] Buhr, K., Karlsson, A., Sanne, J.M., Albrecht, N., Santamaría, N.A., Antonsen, S., ... Warkentin, S. (2016). *SmartResilience D1.3: End users' challenges, needs and requirements for assessing resilience*, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

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

[6] Cutter, S. L., C. G. Burton, Ch. Emrich (2010). Disaster Resilience Indicators for Benchmarking Baseline Conditions, *Journal of Homeland Security and Emergency Management: Vol. 7*: Iss. 1, Article 51.

[7] DARWIN project (2016). Expecting the unexpected and know how to respond. Retrieved from http://www.h2020darwin.eu/

[8] Data-Driven Documents (2016) Introduction. Retrieved from https://d3js.org/

[9] Doyle J. C., et al (2005). The "robust yet fragile" nature of the internet, Proceedings of the National Academy of Sciences USA 102, 14497-14502

[10] 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.

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

[12] European Commission (2013). Call H2020-DRS-2014-2015: *Disaster Resilience: Safeguarding and securing society, including adapting to climate change*, Retrieved from https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-drs-2014-2015.html#c,topics=callIdentifier/t/H2020-DRS-2014-2015/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc

[13] FEMA (2014). *FEMA Strategic Plan 2014–2018*. Washington, DC

[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] Guimerá R, Mossa S, Turtschi A, Amaral L. (2005). The worldwide air transportation network: anomalous centrality, community structure, and cities' global roles, Proceedings of the National Academy of Sciences USA 102, 7794-7799.

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

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

[18] IMPROVER (2016). IMPROVER - Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure. *Deliverable 2.2: Report of criteria for evaluating resilience*. Retrieved from www.improverproject.eu/2016/06/23/deliverable-2-2-report-of-criteria-for-evaluating-resilience/.

[19] Jovanovic, A., Auerkari P. (2016), EU project SmartResilience: The concept and its application on critical energy infrastructure in Finland, Baltica X-International conference on life management and maintenance for power plants, Vol. 1, Helsinki, June 07-09, 2016

[20] Jovanovic, 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, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[21] Jovanovic, A., P. Klimek (2015). Risk & Resilience: Emerging risks and resilience – how to find right indicators. Risk and Resilience in the face of Global Change, Aspen Global Change Institute, Aspen, Col., Nov. 30 - Dec. 5, 2015

[22] Jovanovic. A., Choudhary. A., Jovanovic. M., Szekely. Z. (2016) *SmartResilience D2.1 draft report: Understanding "smart" technologies and their roles in ensuring resilience of infrastructure*, EU project SmartResilience, Project No. 700621 (2016-2019), Contact: EU-VRi, Stuttgart, Germany.

[23] Jovanovic. A., Schmid. N., Klimek. P., Choudhary. A. (2016). Use of indicators for assessing resilience of Smart Critical Infrastructures, *IRGC Resource guide on resilience*. Lausanne: EPFL International Risk Governance Center. v29-07-2016

[24] KC 130 https://en.wikipedia.org/wiki/Lockheed_Martin_KC-130

[25] Linkov, I. et al. (2014). Changing the Resilience Paradigm. *Nature Climate Change 4(6)*, 407-409. Retrieved from (http://www.nature.com/doifinder/10.1038/nclimate2227).

[26] Linkov, I. et al. (2014). Changing the resilience paradigm. *Nature climate change, Vol. 4*, June 2014

[27] OECD (2014). *Guidelines for resilience systems analysis*, OECD Publishing

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

[29] Øien, K. (2010). *Remote operation in environmentally sensitive areas; development of early warning indicators*. 2nd iNTeg-Risk Conference, Stuttgart, Germany, 15-16 June 2010.

[30] Øien, K. (2013). Remote operation in environmentally sensitive areas: development of early warning indicators, *Journal of Risk Research, 16(3-4)*, 323-336.

[31] Øien, K., & Nielsen, L. (2012). *Proactive Resilience Based Indicators: The Case of the Deepwater Horizon Accident*. SPE / APPEA International Conference on Health, Safety and Environment in Oil & Gas Exploration and Production, Perth, Australia, 11-13 September 2012.

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

[33] Øien, K., Massaiu, S., Tinmannsvik, R.K., & Størseth, F. (2010). *Development of early warning indicators based on Resilience Engineering*. International Conference on Probabilistic Safety Assessment and Management (PSAM10), Seattle, USA, 7-11 June 2010.

[34] Øien, K., Utne I.B., & Herrera I.A. (2011). Building Safety Indicators. Part 1 – Theoretical foundation. *Safety Science 49(2*), 148-161.

[35] Radiotelephony phonetic alphabet (2016), International Civil Aviation Organization, Retrieved from http://www.icao.int/Pages/AlphabetRadiotelephony.aspx

[36] READ (2016). READ - Resilience Capacities Assessment for Critical Infrastructures Disruption: www.read-project.eu/

[37] Resilens project (2016). Realising European Resilience for Critical Infrastructure. Retrieved from http://resilens.eu/

[38] Resolute project (2016). RESilience management guidelines and Operationalization appLied to Urban Transport Environment. Retrieved from http://www.resolute-eu.org

[39] SmartResilience (2015). *Smart Resilience Indicators for Smart Critical Infrastructures – Project proposal Call*: H2020-DRS-2015, DRS-14-2015. Coordinator: EU-VRi, www.smartresilience.eu-vri.eu.

[40] 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.

[41] Solé R, M. Rosas-Casals, B. Corominas-Murtra, S. Valverde (2008). Robustness of the European power grids under intentional attack. *Phys Rev E 77*, 026102.

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

[43] Størseth, F., Tinmannsvik, R.K., & Øien, K. (2009). *Building safety by resilient organization – a case specific approach*. The European Safety and Reliability Conference (ESREL '09), Prague, Czech Republic, 7-10 September 2009.

[44] The future of smart cities: Cyber-physical infrastructure risks (2015). US Department of Homeland Security, Office of Cyber and Infrastructure Analysis

[45] UNISDR (2015). *The Sendai Framework for Disaster Risk Reduction 2015-2030*, United Nations Office for Disaster Risk Reduction

[46] Wreathall. J. (2006). Properties of resilient organizations: an initial view. In: *Resilience Engineering: Concepts and Precepts*. Ashgate, Aldershot.