Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

Resilience assessment of smart critical infrastructures based on indicators

K. Øien & L. Bodsberg
SINTEF Technology and Society, Trondheim, Norway

A. Jovanović
European Virtual Institute for Integrated Risk Management, Stuttgart, Germany
Steinbeis Advanced Risk Technologies GmbH, Stuttgart, Germany

ABSTRACT: The resilience of modern societies is to a large degree determined by the resilience of their Critical Infrastructures (CI). These infrastructures are critical because interruptions not only influence the infrastructures themselves, but loss of functionality has secondary effects on the society. The use of smart technologies makes these "Smart" CIs (i.e. SCIs) increasingly interdependent and vulnerable to various hazards, such as terror attacks, cyber-attacks and extreme weather. The EU H2020 research project SmartResilience has developed a baseline resilience assessment method, which measures the level of resilience indirectly through a selection of resilience indicators considered relevant by the user of the SCI in question. Other methods have also been developed in SmartResilience, but this paper focus on the development and application of the baseline resilience assessment method and the development and collection of resilience indicators used in the assessment method. The application is demonstrated using a production facility as a case.

1 INTRODUCTION

The power grid in Ukraine was cyber-attacked both in 2015 and 2017. The attack in 2015 was a complex and pervasive attack on three energy distribution companies, resulting in about 230 thousand people being left without electricity for a period from 1 to 6 hours (Wikipedia 2017). Energy supply systems, such as those attacked in Ukraine, are examples of critical infrastructures (CIs); *critical* because their functions are vital for the society.

Smart technologies are introduced in infrastructures to maximize the service they provide using intelligent systems. Thus, the term S*mart* Critical Infrastructure (SCI) is introduced. However, smart features may also make the SCIs more vulnerable, e.g. by providing a gateway for hackers and cyber-terrorists.

The need to defend these SCIs has been recognized for decades through e.g. Critical Infrastructure Protection (CIP) programs. However, in recent years, it has been realized that with increasingly complex and interdependent infrastructure systems, CIP is not enough (HSAC 2006). It is not enough to focus on protection of a CI from events like cyber-attacks, terror attacks and extreme weather, because the complexity and interdependencies makes it virtual impossible to foresee and prevent all scenarios, and when they occur—no matter how unlikely—it is vital for society that the loss of functionality is minimized, e.g. that the CIs are up and running as soon as possible after an event.

A shift of the focus from CIP towards CIR, i.e. Critical Infrastructure *Resilience* has been observed. "Overall, a resilience-based approach for CI is an approach that is gradually adopted by nations in order to face the challenges and costs of achieving maximum protection in an increasingly complex environment and to overcome limitations of the traditional scenario-based risk management approach, where the organization may lack capabilities to face risk from unknown or unforeseen threats and vulnerabilities" (Setola et al. 2016).

Resilience is not a straight-forward term. It has many different applications and a broad scope. A helpful review paper providing insights into the term and its history is Alexander (2013). Suffice to state here is that although the term was unfamiliar within risk of critical infrastructures in the US some ten years ago (HSAC 2006), it is now a well-recognized term. Resilience is also a familiar everyday term in English speaking countries, but it is not easily understood by lay people when translated to other languages. In addition, the CIR approach is relatively new in the EU compared to the US. This

gives some challenges for the implementation of CIR in EU and the single EU member states.

Recognizing the challenges with the term resilience, the questions are still: How can we make a system like the energy system in Ukraine, and other SCIs, resilient against cyber-attacks and other relevant threats? How can we know—and measure—the level of resilience of an SCI? These are the challenges that the EU H2020 project Smart-Resilience (2016) is set out to solve. It answers the DRS-14 call, which explicitly asks for an indicator-based approach.

Several methods and tools for assessing and monitoring resilience are developed in the SmartResilience project. In this paper, we present the baseline resilience assessment method measuring the Resilience Level (RIL) of SCIs through resilience indicators. We denote this as the "RIL method" in the following. It is based on review, adaptation and further development of relevant reference methods having their roots in high reliability theory (Wreathall 2006), resilience engineering (Woods 2006) and critical infrastructure resilience (Fisher et al. 2010).

The resilience indicators have been developed (identified and/or proposed) mainly by the case study partners in the SmartResilience project, covering a range of different critical infrastructures. They are stored in a database as "candidate" resilience indicators, i.e. the users select the most relevant indicators for their case from the candidates in the database, or add new indicators, when necessary.

Based on the selected set of resilience indicators, the RIL method provides a level of resilience on a scale from E (worst) to A (best) for one specific SCI, or several SCIs, within an area. In addition to an overall level of resilience, that can be trended periodically, the results point to areas where improvements are most needed. In this paper, the application of the RIL method is demonstrated for a production facility.

The description of the development of the RIL method and the resilience indicators are based on Øien et al. (2017a-c). Earlier versions of the Smart-Resilience methodology are also presented in Jovanović et al. (2017a; 2018).

1.1 *Concepts and definitions*

In the SmartResilience project, the *resilience* of an infrastructure is defined as: "The ability to anticipate possible adverse scenarios/events (including the new/emerging ones) representing threats and leading to possible disruptions in operation/functionality of the infrastructure, prepare for them, withstand/absorb their impacts, recover from disruptions caused by them and adapt to the changing conditions" (Jovanović et al. 2016).

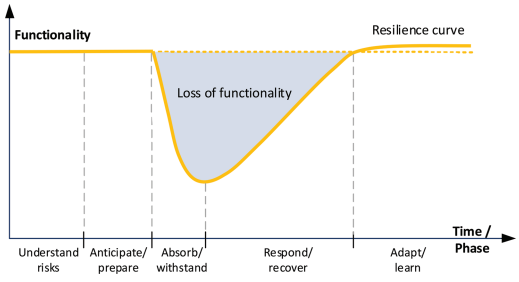

Figure 1. Resilience phases in the resilience curve/cycle.

Based on this definition, we derive at the following five *phases* of the resilience curve/cycle: understand risks, anticipate/prepare, absorb/withstand, respond/recover, and adapt/learn. The five phases, representing the main resilience attributes in SmartResilience, are illustrated in Figure 1.

Each of the phases are measured by indicators through the most important "issues" affecting each of the phases.

An *issue* is a very general term referring to anything (factors, conditions, functions, actions, capacities, capabilities, etc.) that is important in order to be resilient against severe threats such as terror attacks, cyber threats and extreme weather. It is *what* is important, and it is allocated to one of the five phases in the resilience cycle. E.g., it can be "training" performed in the anticipate/prepare phase.

An *indicator* is the description of *how* to measure an issue. Any type/form of indicators are considered appropriate in the RIL method, meaning that they can be yes/no questions, numbers, percentages, frequencies, or some other type. E.g., it can be "percentage of personnel in a certain response team taken a certain course".

2 METHOD DEVELOPMENT

The RIL method is an indicator based approach consisting of two main parts; the resilience assessment method itself and the indicators used to measure the resilience level. The development of the two parts are described in the following.

2.1 *Resilience assessment method*

The RIL method has its roots in high reliability organization theory (EPRI 2000, 2001) and resilience engineering (Øien 2010, 2012; Øien & Nielsen, 2012; Øien et al. 2012), but also more resent resilience developments within critical infrastructures, especially in the US (e.g. Petit et al. 2013, Linkov et al. 2014).

2.1.1 *The ANL method*

The Argonne National Laboratory (ANL) method for assessing a resilience index (RI) (Fisher et al., 2010), or a resilience measurement index (RMI), as it is termed in the most recent version (Petit et al. 2013), is structured in five (or six) 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 comparable 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.

2.1.2 *The LIOH method*

The Leading Indicators of Organizational Health (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) (Wreathall 2006). They also formed part of the basis for factors considered important in resilience engineering. In addition to *themes*, LIOH uses *issues* and *indicators* as the three levels in the structure of the method.

The LIOH method is a contributory-based method in which the users of the indicators take part in workshops and define their own issues (general and nuclear power plant—NPP—specific) for each theme, and for each issue they define indicators. There are no predefined examples of issues prior to the workshops, and no proposals or "candidate" indicators are in place prior to the workshops.

The case studies of the LIOH method show that there is often only one level of issues used, i.e. the issues are not divided into general and NPP issues (EPRI 2000, 2001). A second observation is that the results (the issues and indicators defined) from identical power plant units are very different. The reason for this difference is that there is no guidance with respect to issues and indicators (no a priori "candidates"), and that there have been different participants in the workshops in each of the case studies.

2.1.3 *The REWI method*

The idea of combining the issues into one common level was brought further to the Resilience-based Early Warning Indicator (REWI) method (Øien et al. 2010, 2012); 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 developing 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 structured in two levels, of which the lowest level consists of eight factors, or resilience attributes. The CSFs at the first level are: risk awareness, response capacity, and support. The CSFs at the second level are: risk understanding, anticipation, attention, response, robustness (of response), resourcefulness/rapidity, decision support, redundancy (for support). The CSFs represent the REWI operationalization of the concept of resilience, similar as themes are used in LIOH and phases are used in the Smart-Resilience project. The CSFs are partly, but not entirely, sequential. For each CSF, there is a set of issues contributing to the fulfillment of the goals of the CSF. There is only one level of issues—denoted general issues—for which indicators are developed. The CSFs were developed based on a literature review and an empirical study on successful recovery of high-risk incidents; thus, the term *contributing success factors* (Størseth et al. 2009).

The REWI method consists of a predefined set of issues and a set of candidate indicators for each issue. This is a main difference compared to the LIOH method, and makes it less "open ended". However, it is still a contributory-based method and new issues may be added. The predefined set of issues and sets of candidate indicators "forces" the participants to assess the a priori set of general issues and candidate indicators. Thus, it counteracts the tendency to identify indicators during workshops just as random "indicators of the day".

The issues are just candidates, which may be considered appropriate or rejected, and additional issues may be included. After selecting the important issues, the next step is to consider how to measure them. How well are we doing with the selected issues? What would tell me that we are doing well (or have problems) with a specific issue? What information do we have about this? This is the role of the indicators.

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

2.1.4 *The SmartResilience RIL method*

Like the LIOH method and the REWI method, the RIL method uses *issues* and *indicators* on the two lowest levels of the structure, whereas *phases* are used on the next higher level, compared to themes in LIOH and contributing success factors

in REWI. For each of the phases, issues that are important for them are identified, and indicators to measure the issues are developed.

In addition, the issues (and corresponding indicators) may be structured according to five *dimensions*, which are system/physical, information/data, organizational/business, societal/political, and cognitive/decision-making (Jovanović et al. 2016). The phases and dimensions forms what is denoted the Resilience Matrix, commonly used in several resilience assessment methods (e.g. Linkov et al. 2014). However, in the SmartResilience project, dimensions are only optionally used for structuring and triggering the identification of issues and indicators. Only phases are directly included in the quantification, i.e. it is the columns in the Resilience Matrix that are of interest, not the rows (or the single cells) in the matrix.

The SmartResilience RIL method has been developed through several iterations, including input from user requirements (Buhr et al. 2016), test case use, and feedback from case study partners in workshops and through a questionnaire (Jovanović et al. 2017b). A description of the resulting method is provided in Section 3.1.

2.2 *Resilience indicators*

The candidate issues and indicators collected in the SmartResilience project are to a large degree provided by the partners from existing standards, guidelines and reports within the areas of risk, safety, security, crisis management, business continuity and similar domains.

Resilience is considered an "umbrella" term (Setola et al. 2016), covering all the mentioned domains; thus, the term *resilience indicators* may include risk indicators, safety indicators, etc. The umbrella concept is illustrated in Figure 2.

In addition to standards, guidelines and reports, some indicators are based on what the case study providers already are using, and some indicators are developed as part of the project. Figure 2 also illustrates that the resilience concept in general and the resilience indicators, aim at capturing the unexpected, by using the metaphor "rain from a blue sky".

Candidate issues and indicators are stored in a database, and reported in Øien et al. (2017a), representing the status of the collected issues and indicators approximately half way through the project.

In addition, Øien et al. (2017c) present generic candidate issues (without indicators) covering more genuine resilience issues, i.e. capturing topics typically discussed in the resilience literature. The two main sources are the guideline for implementing the REWI method (Øien et al. 2012), and an emergency preparedness plan developed by SINTEF

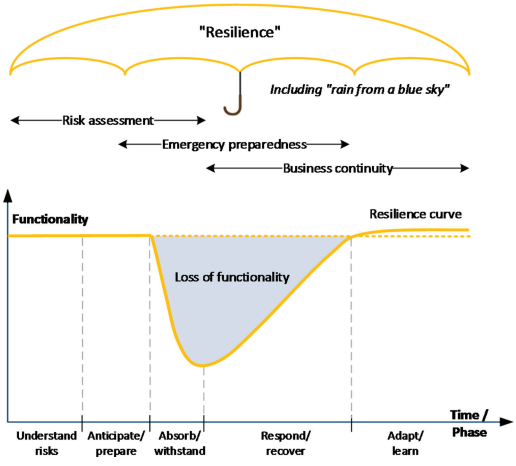

Figure 2. Resilience as an "umbrella" term.

(2014). Some issues are derived from IMPROVER (2016), a few from RESILENS (2016a, b), and the rest is based on input from SINTEF as part of the SmartResilience project. Some issues are taken directly from the original sources, whereas others are slightly adapted. Only for those generic candidate issues that are considered relevant for each user, indicators need to be developed.

A presentation of the collected candidate issues and indicators is provided in Section 3.2.

3 RESULTS

3.1 *The SmartResilience RIL Method*

3.1.1 *Model*

The three lower levels (level 4–6) of the hierarchical model are phases, issues and indicators, as described in Section 2.1. In addition, the overall structure consists of three more levels. The first level is the area level, e.g. a city. The second level consists of the smart critical infrastructures (SCIs), and the third level defines the threats. This is illustrated in Figure 3.

3.1.2 *Method steps*

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

The method steps are as follows:

Step 1: Select the area, e.g. a smart city
Step 2: Select the relevant SCIs for the area
Step 3: Select relevant threats for each SCI

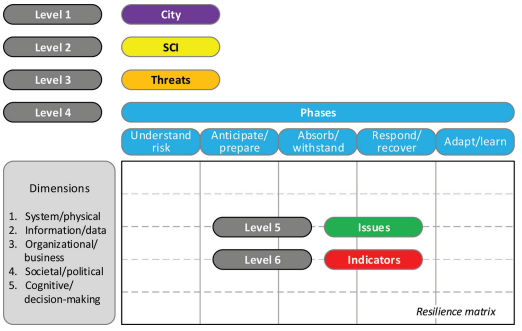

Figure 3. The six levels in the hierarchical model.

Step 4: Consider each phase for each threat
Step 5: Define the issues within each phase
Step 6: Search for the indicators for each issue
Step 7: Determine the range of values for each indicator (and optionally assign weights)
Step 8: Assign values to the indicators
Step 9: Perform the calculations (scores and RILs)
Step 10: Use the results and make decisions

The method steps have been described in Jovanović et al. (2017a) and we will only focus on the changes that have been made lately. This apply to Steps 7 and 9.

The indicators real values are collected and transformed to a *score* (or rating) on a scale from 0 (worst) to 5 (best). This requires the determination of best and the worst values for each indicator, i.e. Step 7. This part is simplified by using five categories, or value ranges (Øien et al. 2017b).

At every level, there is a possibility to give *weights*; however, we recommend being restrictive with the use of different weights. It is challenging to substantiate the assignment of weights (who and how), and the assignment itself can easily be criticized. Thus, equal weights are the default values at all levels. However, if different weights are considered necessary, we now propose using a simple type of pairwise comparison (Øien et al. 2017b). It can also be considered to include weights after gaining some experience, i.e. "tuning" the assessment.

In Step 8, the values are assigned to the indicators, i.e. the measurement itself is performed, and in Step 9 scores are calculated, first on the indicator level, and then aggregated upwards through all levels until the area level. On each level in the hierarchy, the scores can be transformed to resilience levels. This is new, and also the use of characters E-A is new; previously a scale 0–10 was used for RILs, and the transformation from scores to RILs only took place at the phase level (Øien et al. 2017b).

The use of the results, in Step 10, is described in Section 3.3.

3.1.3 *Special topics*

The way cascading effects, dependencies and interdependencies, interoperability, and smartness opportunities and vulnerabilities are treated in the RIL method is briefly described below. We strive for a good balance between the comprehensiveness of the analysis framework and the simplicity of understanding and using the framework. Thus, the specific topics have been addressed explicitly, but relatively simplistic.

Cascading effects where the SCI in question is affected from the outside should be *treated as a specific threat* e.g. toxic cloud, flooding, etc. If the effect is in the form of loss of service, then it is treated as dependencies as part of Step 5, i.e. explicitly as issues. Internal escalation of an event is also treated explicitly as issues (Step 5) reflecting the required safety systems or barriers needed to prevent escalation.

Critical infrastructures, or other infrastructures, services or systems that the SCI are dependent on, should be *addressed explicitly as issues* in the relevant phases for the relevant threats. This could e.g. be the need for redundant energy supply or communication networks. Interdependencies are treated in the same way. The difference is that the SCIs being dependent on "your" SCI, need to explicitly include this as issues in their resilience assessment.

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

The relevance of smartness opportunities and smartness vulnerabilities related to smart features (sensors, gateways, processors, actuators, etc.) should be considered *explicitly as issues* in each phase.

3.2 *The collection of issues and indicators*

Øien et al. (2017c) describes candidate resilience issues and indicators to be used when assessing, predicting and monitoring resilience of Smart Critical Infrastructures (SCIs). A total of 233 candidate issues and 1264 indicators are provided for various threats, SCIs and the five phases of the resilience cycle.

Table 1 shows the number of issues and indicators in the five phases defined in the Smart-Resilience project. In addition, some issues and indicators are considered relevant for all phases.

Table 1. No. of issues and indicators in each phase.

Phase		Issues	Indicators
Phase I	Understand risks	46	226
Phase II	Anticipate/prepare	93	520
Phase III	Absorb/withstand	45	236
Phase IV	Respond/recover	39	180
Phase V	Adapt/learn	20	95
Relevant for all phases		10	182

Although a substantial number of issues and indicators have been collected, they will never be complete and they are just candidates. There will always be a need for additional and/or more relevant issues and indicators for each specific user; and in the end, it is always the user that is responsible for finding a relevant and complete set of issues and indicators for his/her own case study.

Issues are essential in order to focus on those aspects that are most important to measure. Therefore, issues are considered first, and then indicators to measure the selected issues are established. Focusing on indicators first may result in important aspects (issues) being missed and not measured.

The importance of issues is also reflected by the 143 generic candidate issues provided in Øien et al. (2016c).

3.3 *Results obtained by using the method*

From the overall result, i.e. the resilience level of an area or a specific SCI, we can "drill-down" through the levels 2–6 for detailed results, which can be used in Step 10, together with the overall result. We do *not* have "just one number" (the overall resilience level).

There are many possibilities for use of the results, including:

1. Following up own development over time (trending) and analyse status
2. Comparing with others (benchmarking)
3. Providing overview of strengths and weaknesses and point at improvement needs
4. Making any gaps visible (lack of relevant indicators)

3.4 *Example*

To explain the assessment and calculations performed, Table 2 shows an extract of an example RIL assessment of a production facility within the chemical industry. The threat considered is terrorist attack (threat 1), and only the first phase (phase I) is shown.

Issues and indicators (I & I) IDs are listed in the first column. The indicators for the first issue (I.1) are: Does a safety risk register exist? (I.1.1); Is this registry used in decision making? (I.1.2); Is a frequency for updating the registry defined? (I.1.3). The second issue (I.2) only have one indicator: Is a procedure for MOC established? (I.2.1). The third issue (I.3) has the following three indicators: Does an accident/incident register exist? (I.3.1); Frequency of communication about incidents (I.3.2); Percentage of employees informed about incidents (I.3.3).

Table 2. Calculations on indicator level (example).

Indicator scores, weights and RILs					
I & I	Real value	Score value	RIL	Weight	Weighted score
I.1 Safety risk registry					
I.1.1	Y	5	A	0,33	1,67
I.1.2	Y	5	A	0,33	1.67
I.1.3	N	0	E	0,33	0,00
I.2 Management of change—MOC					
I.2.1	N	0	E	1,00	0,00
I.3 Register of accidents/incidents					
I.3.1	Y	5	A	0,33	1,67
I.3.2	1/6 mth	1,5	D	0,33	0,50
I.3.3	80%	3,5	B	0,33	1,17

Each indicator is measured, i.e. providing the real values for the indicators, whether it is yes/no questions, frequencies, percentages, or some other type of indicator. Based on the real value and the predetermined range of values, from worst to best (not shown in Table 2), an indicator score value is calculated. This value can be transformed to an indicator resilience level, from E (worst) to A (best) according to a predefined scale. Weights are determined, and the default values are equal weights. By multiplying the indicator scores with the indicator weights, the indicator weighted score is obtained in the last column. The indicator weighted scores are brought to the next level in the calculations, i.e. the issue level (level 5), where similar calculations are performed obtaining issue weighted scores, and so on, all the way to the area level (level 1).

The calculations gave an overall score on area level of 3,06 corresponding to RIL = B (Øien et al. 2017b).

The overall result just represents one aggregated character or value, which provides limited information. We need to "drill down" in the levels beneath, to reveal more detailed information about the various contributions to the overall result. One example of results on level 2 (SCI level) is shown in Figure 4. Here it is revealed that the threats with the lowest scores are *Threat 1 – Terrorist attack* and *Threat 2 – Natural threats*, both with a score of 2,64, which would be natural to look further into to improve resilience.

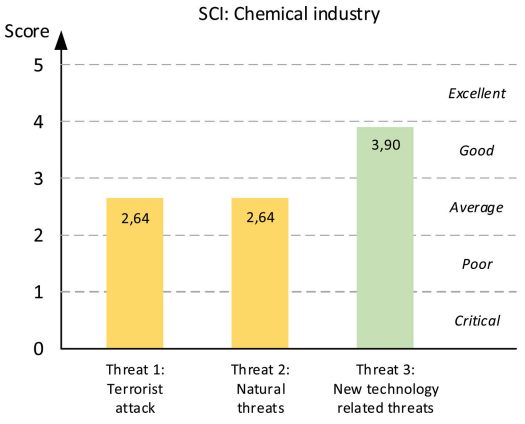

Figure 4. Resilience status at threat level (example).

4 DISCUSSIONS AND CONCLUSIONS

The SmartResilience RIL method helps to understand how resilient the SCIs are against specific types of threats and what measures could help improve their resilience. The results show the level of resilience (RIL) and where improvements are most needed ("drill-down"), emphasizing and fostering a continuous improvement mindset through regularly (typically yearly) updated assessments.

The resilience assessment uses a holistic ("umbrella") approach that goes beyond traditional risk of known events, emergency preparedness, crisis management, and business continuity. It covers e.g. preparing for the unforeseen, imagination, vigilance, flexibility, improvisation, recovery including business continuity aspects, and learning and adaptation.

4.1 *How to use the SmartResilience RIL method*

There are two main options for resilience assessment; internal self-assessment and external assessor audit. One main reason for using external assessments is the possibility for bench-marking between similar SCIs or even areas/cities with similar SCIs. To ensure comparability, it is important to use the same threats, issues and indicators, with the same range of indicator values, weights and similar requirements for collecting data for the indicators. This is possible to achieve (at least for a simple assessment/audit), but may not prove very useful for each individual user.

It is also possible to make user adaptation and customize the set of threats, issues and indicators, ranges of indicator values, weights and so on, e.g. by allowing to reject or add new indicators. However, the more the "dynamic checklists" (the tool used in the SmartResilience project) of threats, issues and indicators are adapted to take user requirements into account, the less comparable they will be.

Internal self-assessment can also be performed using similar checklists as an external assessor would use; however, if the focus is not on benchmarking and comparing with others, the assessment can be adapted to the specific requirements of each user. This will ensure a more relevant and accurate assessment useful for trending own development over time. A user customized self-assessment approach requires more engagement from the users. On one hand this is positive, since the users will take more ownership to the analysis framework and the results; however, on the other hand it will require more resources compared to an external assessment using a standardized framework.

4.2 *Usefulness of the SmartResilience RIL method*

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

A RIL assessment goes beyond traditional risk assessments by focusing on unknown and unforeseen events, and the capability to recover from events. This is achieved by capturing the time dimension through (five) distinct phases, incorporating e.g. emergency response and business continuity. A RIL assessment complements risk assessment; it is not a substitute for risk assessment. Risk assessments also provide valuable input to a RIL assessment, specially to phase I "Understanding risks".

An important purpose of a RIL assessment is to identify potential problems before they occur, so that risk reducing measures may be planned and implemented as needed, regardless of the likelihood of events. Most SCIs in the world have never, and will never, experience an extreme event. Still it is possible to assess the RIL, i.e. the level of risk understanding, anticipation and preparation, the capability to absorb and withstand, to respond and recover, and the abilities to learn and adapt. With a high RIL, it is less likely to experience adverse consequences due to an extreme event, and should it occur, then disruptions are likely to be less severe.

4.3 *Conclusions*

The SmartResilience project has developed a method for assessing resilience of SCIs with respect to specific type of threats on a scale from E

(worst) to A (best). An overall RIL is obtained by combining resilience levels for five main attributes/phases of resilience for each threat. For each phase, the user/analyst must identify the most important "issues" affecting SCI resilience and for each issue select relevant indicators, indicator range values, and perform calculations. The Smart-Resilience project has provided candidate issues and indicators for various SCIs that may be used as a starting point for identifying issues and indicators for resilience assessment of specific SCIs. This baseline resilience assessment can be used for trending as well as identifying improvement needs.

The resilience curve, describing the SCI functionality as a function of time, before, during and after an adverse event, is treated as a conceptual model, i.e. the method does not consider the exact shape, size or area of the curve directly. It is an indirect measurement. For direct assessment of SCI resilience, the SmartResilience project has developed a functionality assessment method with respect to specific threat scenarios. This alternative method provides a quantitative measure of loss of SCI functionality as a function of time addressing explicitly the resilience curve.

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, together with the support from all the partners in the project.

REFERENCES

Alexander, E. 2013. Resilience and disaster risk reduction: an etymological journey. *Nat Hazard Earth Syst Sci* 13:2707–16.

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.

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.

EPRI 2001. *Final report on leading indicators of human performance*. EPRI, Palo Alto, CA, and the U.S. Department of Energy, Washington, DC, 1003033.

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.

HSAC 2006. *Report of the Critical Infrastructure Task Force*. Homeland Security Advisory Council.

IMPROVER Consortium 2016. Deliverable 2.2: *Report of criteria for evaluating resilience*. www.improver-project.eu/2016/06/23/deliverable-2-2-report-of-criteria-for-evaluat-ingresilience/.

Jovanović, A., Øien, K., Choudhary, A. 2018. An indicator-based approach to assessing resilience of smart critical infrastructures. In A. Fekete & F. Fiedrich (eds), *Urban disaster resilience and security: addressing risks in societies*. Springer.

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, Project No. 700621 (2016–2019), Contact: EU-VRi, Stuttgart, Germany.

Jovanović, A., Choudhary, A., Tetlak, K., Albrecht, N., Roque, R., Klimek, P., … Bergfors, L. 2017b. SmartResilience D5.1: *Report on the results of the interactive workshop*, EU project SmartResilience, Project No. 700621 (2016–2019), Contact: EU-VRi, Stuttgart, Germany.

Jovanović A., Quintero, F., Choudhary, A. 2017a. *Use of safety-related indicators in resilience assessment of Smart Critical Infrastructures (SCIs)*, ESREL 2017 – European Safety and Reliability Conference, 18–22 June 2017, Portoroz, Slovenia.

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.

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

Øien, K. 2013. Remote operation in environmentally sensitive areas: development of early warning indicators. *J Risk Res* 16(3–4):323–336.

Øien, K., Bodsberg, L., Hoem, Å., Øren, A., Grøtan, T. O., Jovanović, A., … Tuurna, S. 2017c. SmartResilience D4.1: *Supervised RIs: Defining resilience indicators based on risk assessment frameworks*, EU project SmartResilience, Project No. 700621 (2016–2019), Contact: EU-VRi, Stuttgart, Germany.

Øien, K., Jovanović, A., Grøtan, T.O., Choudhary, A., Øren, A., Tetlak, K., … Jelic, M. 2017a. SmartResilience D3.2: *Assessing resilience of SCIs based on indicators*, EU project SmartResilience, Project No. 700621 (2016–2019), Contact: EU-VRi, Stuttgart, Germany.

Øien, K., Jovanović, A., Bodsberg, L., Øren, A., Choudhary, A., Sanne, J., … Szekely, Z. 2017b. SmartResilience D3.6 draft report: *Guideline for assessing, predicting and monitoring resilience of Smart Critical Infrastructures (SCIs)*, EU project SmartResilience, Project No. 700621 (2016–2019), Contact: EU-VRi, Stuttgart, Germany.

Øien, K., Massaiu, S., Tinmannsvik, R.K. 2012. *Guideline for implementing the REWI method; resilience based Early Warning Indicators*. SINTEF report A22026, Trondheim, Norway.

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.

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.

Petit, F.D., Bassett, G.W., Black, R., Buehring, W.A., Collins, M.J., Dickinson, D.C., … Peerenboom J.P. 2013. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-13-01, Argonne, IL, USA.

RESILENS Consortium 2016a. *Qualitative, Semi-Quantitative and Quantitative Methods and Measures for Resilience Assessment and Enhancement*. Ireland. Retrieved from http://resilens.eu/wp-content/uploads/2016/08/D2.2-Methods-for-Resilience-Assessment-Final.pdf.

RESILENS Consortium 2016b. *Resilience Management Matrix and Audit Toolkit*. Ireland. Retrieved from http://resilens.eu/wp-content/uploads/2016/06/D2.3-Resilience-Management-Matrix-and-Audit-Toolkit.pdf.

Setola, R., Luiijf, E., Theocharidou, M. 2016. Critical Infrastructures, Protection and Resilience. In R. Setola et al. (eds.), *Managing the Complexity of Critical Infrastructures, Studies in Systems, Decision and Control 90*, DOI 10.1007/978-3-319-51043-9-1.

SINTEF 2014. Emergency preparedness plan, Restricted.

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.

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.

Wikipedia, 2017. https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack, Accessed on Dec 4, 2017.

Woods, D.D. 2006. Essential Characteristics of Resilience. In: N. Leveson, E. Hollnagel, and D.D. Woods (eds), *Resilience engineering: concepts and precepts:* 21–34. Aldershot: Ashgate.

Wreathall, J. 2006. Properties of resilient organizations: an initial view. In: N. Leveson, E. Hollnagel, and D.D. Woods (eds), *Resilience engineering: concepts and precepts:* 21–34. Aldershot: Ashgate.