IMPROVED RISK EVALUATION AND IMPLEMENTATION OF RESILIENCE CONCEPTS TO CRITICAL INFRASTRUCTURE

Report of criteria for evaluating resilience

Editors:
C. PURSIAINEN (UiT) and B. RØD (UiT)

Contributors (in alphabetic order):

M. ALHEIB (INERIS)
G. BAKER (SPFR)
C. BOUFFIER (INERIS)
S. BRAM (SP)
G. CADETE (INOV)
E. CARREIRA (INOV)
P. GATTINESI (JRC)
F. GUAY (DBI)
D. HONFI (SP)
K. ERIKSSON (SP)
D. LANGE (SP)
E. LUNDIN (SP)
A. MALM (SP)
L. MELKUNAITE (DBI)
M. MERAD (INERIS)
M. MIRADASILVA (INOV)
L. PETERSEN (EMSC)
J. RODRIGUES (INOV)
R. SALMON (INERIS)
M. THEOCHARIDOU (JRC)
A. WILLOT (INERIS)

Deliverable Number: D2.2

Date of delivery: 31 May 2016

Month of delivery: M12

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390

Coordinator:	David Lange at SP Sveriges Tekniska Forskningsinstitut (SP Technical Research Institute of Sweden)

Table of Contents

1 Executive Summary

In the recent years, the focus has moved from critical infrastructure protection to that of resilience. But how do we know whether a critical infrastructure is resilient or not, how can it be evaluated, measured and enhanced?

Drawing on, combining and developing the ideas of the existing literature and practices, the current report develops a holistic, easy-to-use and computable methodology to evaluate critical infrastructure resilience, called Critical Infrastructure Resilience Index (CIRI). The methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors, facilities and hazard scenarios. The proposed methodology is especially suitable for organizational and technological resilience evaluation, but permits including also elements of societal resilience indicators to the evaluations.

The methodology is based on four levels of hierarchically organized indicators. Level 1 consists of the phases well known from the so-called crisis management cycle. Under these phases, we find sets of Level 2 rather generic indicators. Thus under level 1 'Prevention', for instance, we may find a Level 2 indicator such as 'Resilient design', further divided into Level 3 more detailed indicators such as 'Physical robustness', 'Cyber robustness', 'Redundancy', 'Modularity', and 'Independency'. The task is to study these indicators on Level 4 in the context of concrete critical infrastructure facilities and hazard scenarios, that is, applying Level 3 indicators into concrete circumstances.

The methodology then permits to transfer quantitative, semi-quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels. This in turn makes it possible to give a specific critical infrastructure, or its part, a resilience value on the scale 0-5.

While the real resilience value becomes clear only when one engages in the analysis of several indicators, the methodology can be used also as a step-by-step measurement and development tool for resilience, without necessary immediately engaging in time-consuming total resilience analysis.

The user of this methodology is supposed to be the operator of critical infrastructure, or part of it, in the spirit of self-auditing. In case it would be implemented in a wider scale, in cooperation between the operators and authorities, it would give the authorities a holistic picture about the respective society's critical infrastructure resilience.

In this report, we draw a concise picture of the methodology and illustrate how this methodology could be applied to a specific infrastructure and hazard scenario.

2 Introduction

The current report is worked out within the IMPROVER project's Work Package 2 and it is its Deliverable D.2.2. According to the project plan, the deliverable is a "Report of criteria for evaluating resilience (based on outcome of task 2.3) M12." The referred Task 2.3 bears the title "Development of common criteria for measurement of resilience and a methodology for critical evaluation of resilience". It is described as follows: "In this task, common criteria for describing infrastructure resilience will be developed. The objective here is that the criteria are transferable between different infrastructures and that they are scalable so that they are informative on a policy level as well as an asset level. Examples of criteria, which may be considered, include criticality of function; cost of interruption; downtime; or even societies' expectations of infrastructure functionality or some other quantitative measure of resilience based on a function or combination of the above – reflecting, possibly, requirements for infrastructure on a policy level."

To this effect, the current reports concisely presents the results of this work. It is based on a step-by-step development work of the first project year, documented in several reviews, background papers and conference contributions, produced by all the IMPROVER partners within WP1 and WP2. Most notably the following ones, marked as separate appendices to the current report and available by request from the project's database, should be mentioned:

- Appendix 1: Laura Melkunaite (DBI), *Concept of Resilience* (September 2015, WP1)
- Appendix 2: Christer Pursiainen (UiT), Bjarte Rød (UiT), Peter Gattinesi (JRC), and Marianthi Theocharidou (JRC) *Background Paper for IMPROVER WP2 D2.2. Criteria for evaluating critical infrastructure resilience* (August 2015, WP2).
- Appendix 3: Christer Pursiainen (UiT), *Methodological paper* (December 2015, WP2)
- Appendix 4: Laura Petersen (EMSC), Kerstin Eriksson (SP), and Laura Melkunaite (DBI), *Social Resilience Indicators* (March 2016, WP2)
- Appendix 5: Marianthi Theocharidou (JRC), Fanny Guay (DBI), and Laura Melkunatite (DBI). *Organizational Resilience Indicators* (March 2016, WP2)
- Appendix 6: Greg Baker (SPFR), *Oslo Airport Gardermoen application to Task 2.3* (March 2016, WP2)
- Appendix 7: Greg Baker (SPFR), *Earthquake loading and the mobile telephone network application to Task 2.3* (March 2016, WP2)
- Appendix 8: Goncalo Cadete (Elisabete Carreira, Miguel Miradasilva, John Rodrigues) (all INOV), *Assessing the Resilience of ICT-dependent Critical Infrastructures* (March 2016, WP2)
- Appendix 9: David Lange and Daniel Honfi (both SP), *Technological indicators of resilience of bridges as critical infrastructure assets* (March 2016, WP2)
- Appendix 10: David Lange and Daniel Honfi (both SP), *Bridge indicators* (March 2016, WP2)
- Appendix 11: Emma Lundin and Annika Malm (SP), *Water network system indicators* (March 2016, WP2)
- Appendix 12: Romuald Salmon, Adrien Willot, Christian Bouffier, and Marwan Alheib (all INERIS). *Risk analysis and Warning application to Task 2.3* (March 2016, WP2)
- Appendix 13: Christer Pursiainen (UiT), Bjarte Rød (UiT), Daniel Honfi (SP), and David Lange (SP, Greg Baker (SPRF), *Critical Infrastructure Resilience Index* (CIRI) (April 2016, ESREL 2016 conference paper draft, WP2)
- Appendix 14: Bjarte Rød (UiT), Abbas Barabadi (UiT), and Ove T. Gudmestad (UiS), *Characteristics of Arctic Infrastructure Resilience: Application of Expert Judgement*. (April 2016, ISOPE The International Society of Offshore and Polar Engineers conference paper, WP2-related)
- Appendix 15: Myriam Merad and Romuald Salmon (both INERIS), *Methodological insights related to aggregation toward critical infrastructures index* (May 2016, WP2)
- Appendix 16: Daniel Hofi (SP), David Lange (SP), Christer Pursiainen (UiT), and Bjarte Rød, *On the contribution of technological concepts to the resilience of bridges as critical infrastructure assets*, (IABSE 2016 conference paper, May 2016, WP2).

While the above papers draw a much broader picture and discuss multiple dimensions of critical infrastructure resilience, reviewing a huge body of literature and presenting different ways to measure resilience, the current report aims at being as concise as possible. In short, it combines and develops

further the ideas of the above appendices as well as other existing literature on critical infrastructure resilience measurement.

In particular, the report presents a holistic, easy-to-use and potentially computable methodology to evaluate critical infrastructure resilience, called Critical Infrastructure Resilience Index (CIRI). The methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors, facilities and hazard scenarios. The proposed methodology is most suitable for organizational and technological resilience evaluation, but permits including also such elements of societal resilience indicators to the evaluations that are clearly connected to the resilience of a critical infrastructure itself. The aim, and the innovative potential, of the methodology is that it is designed to transfer any quantitative, semi-quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels. This in turn makes it possible to give a specific critical infrastructure or its part an accumulated resilience value on the scale 0-5.

While engaging in total resilience analysis of a critical infrastructure is very time- and resource-consuming, the methodology enables also the evaluation of only some specific individual resilience indicator(s), and can therefore be used as a step-by-step measurement and development tool for resilience.

The user of this methodology is supposed to be the operator of critical infrastructure, or part of it. In case this methodology would be implemented in a wider scale, and the results would be collected together, it would give the authorities a holistic comparative picture about the respective society's critical infrastructure resilience.

It is however considered that in the European Union reality, critical infrastructure operators are reluctant, first, to become compared by an outside authority, and, second, not willing to reveal their detailed resilience level across indicators, which would be the same as to reveal their points of vulnerability. Therefore, at this point, we assume the current methodology to be a self-auditing and self-assessment tool rather than a regulative and control mechanism of the authorities. The methodology is easily transferrable into a self-auditory software with a possibility to tailor it to specific needs.

In this report, we first concisely present the methodology. Second, limiting our focus on a couple of illustrative indicators only, we demonstrate how this methodology could be applied to a specific infrastructure and hazard scenario.

It should be noted that the current report presents a work in progress. The methodology has so far been only illustrated rather than tested, and there are several uncertainties that will be tackled and discussed further in the subsequent phases of the project. One alternative way to deal with the same challenges is presented in a by-product of the current WP2, namely in Myriam Merad and Romuald Salmon's *Methodological insights related to aggregation toward critical infrastructures index* (Appendix 15, May 2016). While some insights from that background paper will be utilized in the current report, and the methodologies resemble greatly each other, at this point it is better not to mix these two different approaches too much but keep them separate for further consideration and comparison.

Remaining challenges aside, the current methodology allows to critically and innovatively discuss the issue of how to measure critical infrastructure resilience and the related indicators, and contributes to the project goal of developing European-wide guidelines for resilience measurement.

The rest of the report is divided into three main parts, first one introducing the reader to the basic definitions and ideas behind the methodology, the second one discussing in some detail the methodology as such, and the third part including several practical and scenario-based illustrations of how the methodology can be used to produce measurable results of resilience. Short conclusions, restating the basic characteristics of the methodology and noting its limits and remaining challenges, are included.

3 What is Critical Infrastructure Resilience?

3.1 Definition of resilience

As well known, the Directive from 2008 (European Council, 2008) defines critical infrastructure as follows: "An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." The Directive focuses on critical infrastructure protection, and it defines 'protection' as "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability.

In the recent years, the focus has however moved from critical infrastructure protection to that of 'resilience'. While there are no established European Union definition of 'resilience' exactly in critical infrastructure context, one can still find several non-official and more official definitions of the concept.[1] A suitable generic definition, applicable also for critical infrastructure, is provided by the UNISDR (2009): "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions."

It is notable that the verb 'resist' implies that protective measures are included in resilience. Resilience can thus be understood as an umbrella concept covering also critical infrastructure protection.

3.2 Resilience domains

Although the concept of resilience has deep roots in many disciplines, in its contemporary meaning it might be correct to trace it back to the ecological debates in the early 1970s (Holling, 1973; for more, see Appendix 1). The concept became popularized in unofficial policy and scientific analyses in the mid-2000s in the context of crisis and disaster management. Rather soon, it also penetrated the field of critical infrastructure, replacing the earlier focus on protection (Pursiainen and Gattinesi, 2014).

The exact boundaries of the resilience discourse in the context of critical infrastructure are still rather obscure. Nevertheless, certain sub-discourses, research fields and partially shared definitions have emerged, and even become institutionalized. Consequently, we can differentiate between at least three separate (though partially overlapping) domains of critical infrastructure resilience: societal, organizational, and technological.

True, in literature one can find more concepts such as economic resilience (Rose 2008; Rose and Krausman. 2013), socio-ecological resilience and planning resilience (Francis and Bekera, 2014, pp.92, Table 1, 94, 95, Appendix A, 100-102), functional resilience and physical resilience (Boone 2014), personal resilience (Bearse 2014), or psychological resilience (Rodriguez-Llanes et al. 2013). However, in most cases these are actually special cases of the above three ones, used in the current report.

We call these overlapping dimensions in this report as *resilience domains*. This is illustrated in *Figure 1*. As these domains are discussed in detail in the appendices – sometimes using a bit different vocabulary – we outline them only briefly below. The main argument in our context is that

[1] Several definitions are collected in CIPedia, a wiki-based application develop within the FP7 project CIPRNet, see: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Resilience

when defining the resilience domain, we can approach the questions of who or which organization or institution is in charge in dealing with a certain critical infrastructure resilience indicator.

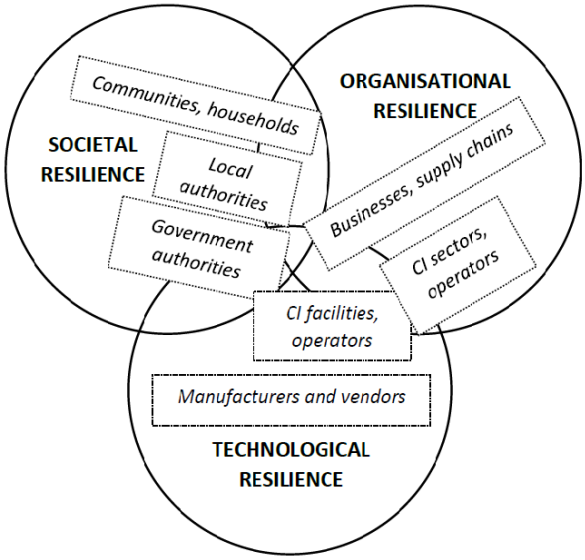


Figure 1: Resilience domains

3.2.1 Societal resilience

There exist many efforts to define societal (or social, sometimes community) resilience, and there can be found many good practices of resilient communities. The focus in societal resilience is on the local community's problems when it faces crises, emergencies or disasters, where critical infrastructure, or its service disruption, may or may not play a crucial role. Yet, even if the source of a disaster is the disruption of critical infrastructure service, the question is not on absorptive but adaptive capacities toward these critical infrastructure disturbances.

There is no one, agreed-upon metrics to evaluate societal or community resilience. Moreover, many of the societal resilience approaches are very generic ones, and thus difficult to operationalise. While quite a few efforts to develop societal resilience indicators and indices exist (e.g. LEDDRA Project, 2014; Boon et al., 2012; Sherrieb et al., 2010; McAslan, 2010a; Cutter et al., 2010; Cutter et al., 2008a; Cutter et al., 2008b; Norris et al., 2008; Flint and Luloff, 2007; Flint and Luloff, 2005; Cumming et al., 2005; Klein et al., 2003; Bruneau et al., 2003; for a review, see Appendix 4), they often only list socio-economic or institutional-political indicators at a very general level.

For instance, Cutter et al. (2010) presents a set of indicators for measuring baseline levels of community resilience in the US. The authors suggested that social resilience could be measured by analysing such indicators as educational equity, age, transportation access, communication capacity, language competency, special needs, health coverage, place attachment, political engagement, social capital in terms of religion, social capital in terms of civic involvement and advocacy, and innovation.

Similarly, LEDDRA Project (2014; cf. Wilson, 2012, pp.4-47) suggests that social resilience could be best measured by evaluating community's identity, cohesiveness and trust, societal relationships, contentment with life, conflicts, communication between stakeholder groups, power, political structures, engagement of young people, responses to and opportunities for influencing change, learning and knowledge, knowledge utility and transfer, learning from experience, participation in decision-making, engagement of community resources, and stakeholder agency.

At best, in terms of concreteness, the literature on societal resilience suggests indicators that reflect the emergency management and self-assistance capacities of the community.

However, from the critical infrastructure operators' point of view, the concept is not very helpful as it is mostly beyond one's influence. Even if critical infrastructure is involved, the focus is on the local community's problems in times of crisis, not on the resilience of a critical infrastructure itself. On the other hand, the concept is very useful from that point of view that its emphasis is on the holistic picture of a society's resilience in times of disasters. In more recent literature, one can find efforts to consider the linkage between infrastructures and social systems (Chang et al., 2014), arguing that there is a need to link physical systems and human communities in order to measure and enhance societal resilience.

3.2.2 Organizational resilience

Organizational resilience connects the resilience concept to that of business continuity, as is revealed by the title of one of the cornerstones of this discourse, namely Sheffi's (2005) monograph *The Resilient Enterprise*. Keeping the business going on is normally the key driver for any enterprise, not to speak about infrastructure operators. A failure of the infrastructure to deliver service could quickly lead to financial disaster for the owner, regardless of the impact on society who might be able to rely on alternative source of service. Thus, it is largely a question about normal risk and crisis management of an enterprise.

In the field of organizational resilience, there is a growing body of literature that literally aims at developing indicators to measure an organizations resilience (Appendices 2, 5, 15; see also e.g. AIIC, 2016; Hosseini et al, 2016; Labaka, Hernates and Sarriegi, 2015; Prior, 2015; Petit et al., 2014; Petit et al., 2013; Linkov et al., 2013; Gibson and Tarrant, 2010; Stephenson, 2010; McAslan, 2010b; Kahan et al., 2009) as well as a number of national and international standards (ISO, 2014a-c; ISO, 2011; cf. ISO, 2007; ISO/IEC, 2005; ISO, 2004; ISO, 2000; ANSI/ASIS, 2012; ANSI/ASIS, 2009; BS, 2014). In fact, the first resilience standards are related to organizational resilience. Thus, the ISO 28002 standard for resilience in the supply chain was approved in 2011, based on the US ANSI/ASIS organizational resilience standard.

The focus of this literature is primarily on organizations that own and manage critical infrastructure facilities. The purpose is to measure the ability of an organization to withstand disturbance of critical infrastructure facilities and maintain or quickly regain function. In practice, this takes place mostly in self-auditing manner, motivated by self-interested profit-seeking in terms of business continuity, although also public good considerations might be taken into account, at least for the sake of possible reputation costs.

To be resilient, organizations must take into account such factors as strong and flexible leadership, an awareness and understanding of their operating environment, their ability to adapt in response to rapid change, and so forth. Yet, while at the first sight, this is a rather straightforward process, and as such suitable for standardization, it becomes more complicated due to the fact that social and cultural differences must be considered (Lee et al., 2013). Also such indicators as innovativeness, creativity and improvisation skills of the organization's leadership are often put forward in this literature (e.g. Stephenson, 2010), which however are rather difficult to measure, except post factum.

3.2.3 Technological resilience

Technological (or technical or engineering) resilience looks the issue at stake from an engineering approach point of view. While technological resilience includes elements of organizational resilience, and these two domains in a way require each other in many cases, the main difference is that resilience is achieved by technological rather than organizational solutions. The main actors in the context of this domain of resilience are critical infrastructure operators, that is, those very facilities that produce the critical services. The authorities' role might be to regulate or control that the technical standards are followed. Furthermore, in most cases, the in-house technological or engineering capacities and capabilities of a service producer are not enough, but one has to rely on manufacturers or vendors for resilience-related technological solutions.

There is no officially approved definition of technological resilience in the context of critical infrastructure in terms of international standard. However, a certain level of consensus has been emerging in the related literature. From the standard definition of resilience, one can already derive the main elements of technological resilience. If a resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored, then there are two key technological concepts in resilience that should be demanded from a resilient critical infrastructure: *resistance* and *restoration capacity*. Resistance could also be described with the term *robustness,* which is the ability of a system to resist or withstand an extreme event of a given level and still maintain some degree of system function.

Every engineering solution is naturally one of its own kind, but already this rather minimalist definition provides us a rather straightforward understanding about what are the general attributes or elements we could measure when we talk about resilient infrastructure especially from a technological perspective.

In literature on technological resilience, one can find more detailed typologies and indicators (e.g. Hosseini et al, 2016; Labaka, Hernates and Sarriegi, 2015; Prior, 2015; Petit et al., 2014; Petit et al., 2013; Vlacheas et al., 2013; Linkov et al., 2013; Strebenz et al., 2011; Youn et al., 2011; McAslan, 2010b; Kahan et al., 2009). In fact, Bruneau et al. (2003) provided already early on a more detailed typology of the resilience aspects of an earthquake that could be applied to critical resilience as well. This typology included four levels: *robustness, redundancy, resourcefulness, and rapidity* (of recovery). This typology, in turn, has been repeated with some variations in most definitions of resilience. For instance, the politically influential definition of Flynn (2008) includes four factors: *robustness*, which is the ability to keep a critical infrastructure operating or stay standing in the face of disaster; *resourcefulness*, which means a skilful management of a disaster once it unfolds; *rapid recovery*, which refers to the capacity to get things back to normal as quickly as possible after a disaster; and, finally, *learning*, that is, the ability to absorb new lessons that can be drawn from a catastrophe.

3.3 The temporal dimension of resilience

Already the above presented UNISDR definition implies that there is a certain temporal dimension of resilience. Resilience is thus a process that has to be present and enhanced before, during and after the crisis or disruption of service. Obviously, this dimension should be taken into account when developing a framework for resilience indicators. Basing the measurement and enhancement strategy on the temporal dimension of resilience helps to identify both *when* and *what* should be done in order to enhance resilience.

This way of thinking is expressed also in official policies, for instance in US cybersecurity strategy (Executive Order, 2013; cf. Appendix 8), which is based on the idea of five functions: identify; protect; detect; respond; and recover. In academic literature, as already mentioned in the previous section, a typical way to express this temporal dimensions is the resilience or performance loss triangle (Chang et al., 2014; Wang and Blackmore, 2009; Bruneau et al., 2003; McDaniels et al., 2007). Increased resilience means that the performance loss triangle will be reduced. By definition, this triangle presupposes the phase before any disruption, that of a downward curve and the upward curve, and last, post-disruption phase when the service level has been restored. In the approach developed by the U.S. Department of Homeland Security (HSSAI, 2009; cf. basically similar Nieuwenhuijs et al., 2008) it is differentiated between three resilience objectives that are interrelated and reinforcing; namely resistance, absorption, and restoration, resistance being the operational mode before and after the disruption.

Following HSSAI (2009) terminology, let us now put the concepts resistance, absorption and restoration into the same picture, and we get *Figure 2* below, illustrating the basic idea of the triangle while somewhat modified with three different scenarios. The figure includes three critical systems

named A, B and C. We consider that the hazard causing the event is similar to all three systems. In the figure, t_0 indicates the time when the stress against the system starts, but one system is more resistance against this stress than another one.

As is seen, the function performance curve A illustrates a system, which is doing worse in resistance, as it partially fails already at t_1 and the performance drops rather immediately around sixty percent. When hit, its service level also drops rather straightforwardly down reaching a rather low point, which means that its absorptive capacity is moderate. Its restoration capacity is also rather moderate as it is restored only gradually by t_5.

Curve B illustrates a system, which is more resistant and withstanding until moment t_2 ($>t_1$) It is also more absorptive as it does not go so low in service level. Furthermore it is able to restore quickly as it is back by t_4 ($<t_5$).

Curve C illustrates a system, which is very resistant, indeed until t_3 ($>t_2>t_1$), but when the damage hits, it leads to a total long-term or permanent functioning failure.

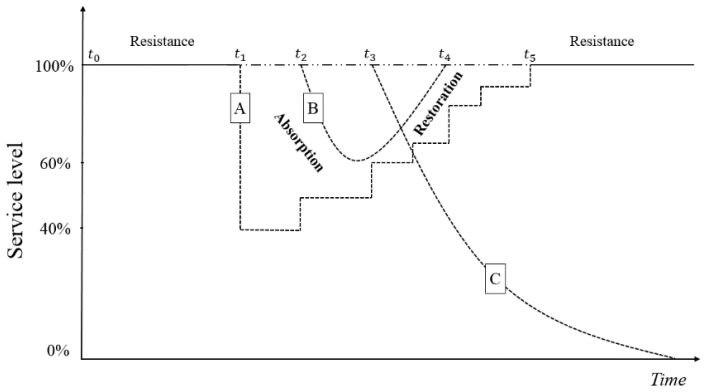


Figure 2: Critical infrastructure performance loss

In a way, *Figure 2* illustrates different resilience strategies through which organizations deal with hazards (cf. Gibson and Tarrant, 2010, p. 11).

Quite often, resilience is approached with the language of crisis management. For instance, McManus suggested rather early to define organizational resilience as "a function of an organization's overall situation awareness, management of keystone vulnerabilities and adaptive capacity in a complex, dynamic and interconnected environment" (McManus, 2008, 82).

Related to this, another way to take into account the temporal dimension, compared to the resilience cycle discussed above, is to understand resilience in relation to the crisis management cycle, sometimes also called emergency management cycle or crisis life-cycle (e.g. Kozine and Andersen, 2015; Petit et al., 2014; Petit et al., 2013).

This cycle, in its standard version, focuses on pre-, during and post-crisis phases, often further divided into subject areas or phases, which are sequential. While the normal presentation of the cycle includes often 'Prevention', 'Preparedness', 'Response' and 'Recovery', we consider that for resilience measurement purposes, it is useful to have rather more than less phases. Therefore, for instance, 'Risk assessment' (usually as part of 'Prevention' in terms of risk management) is separated as its own phase towards which resilience efforts can be targeted. The same goes for adding 'Monitoring and warning' (usually discussed under 'Preparedness' or 'Response') as well as 'Learning' (often omitted) as separate phases or elements, as this

In this report, illustrated in *Figure 3*, we therefore distinguish between the following phases/subject areas: Risk assessment; Prevention (including pre-event mitigation); Preparedness; Monitoring and

warning; Response (including post-event mitigation/damage limitation and consequence management); recovery; and Learning. For most of these crisis management phases, rather clear-cut and generally accepted definitions can be found (e.g. UNISDR, 2009).

Using the crisis management cycle vocabulary is convenient in resilience measurement context as the vocabulary is easily understandable and in many cases already used in practice. For instance, most organizations already make risk assessments and have preparedness plans, and in this sense the current methodology complement and utilises the current practices.

Figure 3: Crisis management circle and resilience

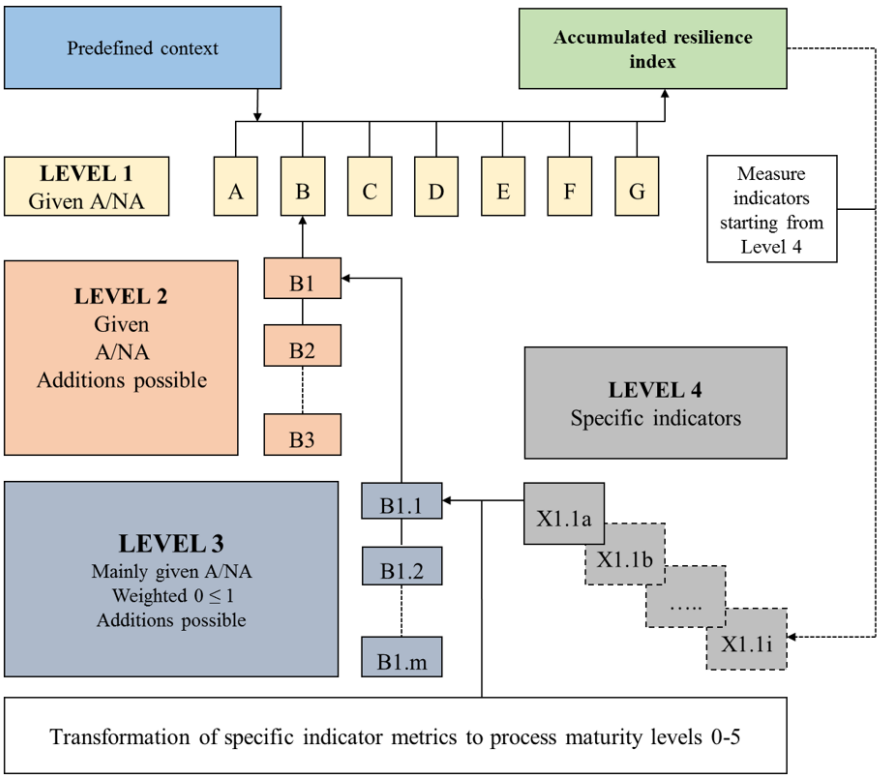
4 Critical Infrastructure Resilience Index

While there already exists a wide range of resilience assessment approaches (for reviews, see Appendices 1, 2, 4, 5, 8, 10, 11, 12, 14; Hosseini 2016), the current report does not aim at reviewing them. Instead, based on the above presented resilience domains and the crisis management cycle, and drawing on existing models, the report develops a set of indicators to measure critical infrastructure resilience and proposes a holistic methodology to that effect, thus making it possible to identify and plan the respective measures to enhance resilience.

4.1 What is an indicator?

'Indicators' are used in many fields – and therefore understood slightly differently – such as economy, chemistry, or health. In more generic terms, an indicator is a sign that shows the condition or existence of something. An indicator is typically understood as a measurable variable used as a representation of an associated factor or quantity.

Related to the metrics that is used in CIRI, to be discussed below, we assume and define indicators, be they originally representing any types of qualitative, semi-quantitative or quantitative metrics, transferrable into *processes, procedures, series of actions, series of operations, schemes, methods, or systems that enable a certain condition or performance*. The scheme of CIRI is presented in *Figure 4*.



A = Applicable, NA = Not applicable

Figure 4: The overall scheme of CIRI

As expressed in *Figure 4*, there is a considerable freedom to tailor the methodology according to the needs of the critical infrastructure operator. Let us in the following explain the elements of the figure.

4.2 Establishing the context

The process of measuring resilience starts with establishing the context. This includes defining three sets of variables: the domain, the hazard type, and situational factors. These variables are illustrated in *Figure 5*.

4.2.1 The domain

Above we have presented the three 'domains' of resilience, that is, societal, organizational, and technological. While to somewhat overlapping, each of the domains have their own sets of indicators. From an operator's point of view, the most important ones are the organizational and technological resilience domains as they are usually in the sphere of direct influence of the operator.

It is reasonable to leave most of the very generic societal resilience indicators (such as socio-economic indicators) outside the task of developing the current CIRI. However, at this point, we keep the societal resilience domain in our analysis to consider whether there might be some indicators that however should be included in this context.

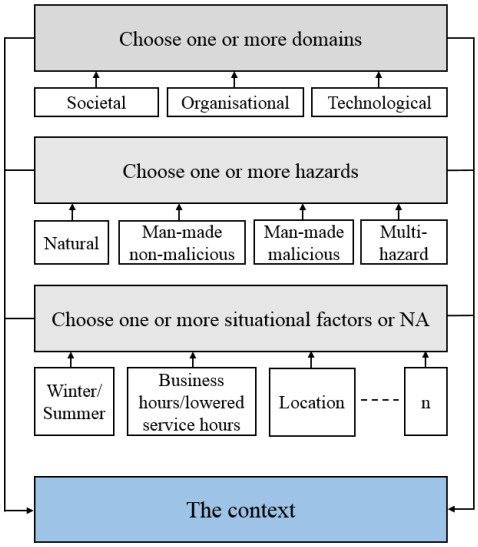


Figure 5: The predefined context

4.2.2 The hazard type

One can argue that resilience is fundamentally dependent on the hazard type, and each hazard type may demand different types of resilience measures. A simply justification of this argument is the obvious notion that a critical infrastructure may be maximally resilient against natural hazards but very vulnerable against malicious attacks.

Therefore we include the definition of hard type into the context variable, with the reservation that one can always omit it by focusing on all-hazard analysis. Following the EU risk assessment summary (European Commission, 2014), we differentiate between natural, non-malicious man-made, malicious man-made, and multi-hazards. Multi-hazard can be understood as a hazard taking into account simultaneous, cascading, domino and other types of causal and non-causal developments.

The user of the methodology can choose one, several or all of these options, and then the accumulated indicator value then reflects the chosen set of hazards.

4.2.3 Situational factors

Resilience depends also on situational factors. Loosing electricity, for instance, is quite a different thing if it takes place in summer time during working hours or if it takes place in cold winter conditions during

banking holidays with minimum staff available for unplanned maintenance and recovery. This set of variable is tailorable (one can add location, weather conditions, location etc.) or it or its elements can be marked as NA (not applicable).

Like in risk assessment, also in resilience evaluation one may need to rely on scenarios to concretise the indicators that we are considering. Scenarios are qualitative and descriptive models of how the future might turn out, which in our case means how the general context established for resilience analysis might materialize.

The scenario may be very simple. For instance, if our operator is a hospital or a district system of hospitals, we may consider the scenario that the external electricity supply is for some reason cut off. Scenario building is however specifically useful to examine complex developments. It is usually only in scenarios one may combine many risk factors in ways to create some surprising events – one of the main characteristics of a crisis – that are difficult to formalize, but which however simulate better the nature of a real-life crisis. In our scheme, the scenario can be included by adding situational factors to describe the more detailed context.

The user of the methodology can tailor the scenario, and then the accumulated indicator values reflect the chosen type of hazard within this particular scenario.

4.3 Levels

In order to operationalise the methodology, we have to differentiate between several hierarchic levels of indicators.

4.3.1 Level 1: Crisis management cycle phases

Level 1 consists of indicators that are the very same crisis management phases already presented above. In Figure A, these phases are represented with symbols A-G.

This level is a generic one and applicable to all types of critical infrastructure. They are not a subject to change, but are given. It is assumed that each Level 1 indicator (cycle phase) is equally important. However, if needed, one can utilise weighting them between 'not applicable' and 1 (NA≤1). Also for practical reasons, one may choose to concentrate only on some of the crisis management phase(s), in which case the others are marked as NA.

4.3.2 Level 2: Generic indicators

Level 2 represents such indicators that are generic applications of some Level 1 indicator. Also this level is applicable to all types of critical infrastructure. Level 2 indicators are relatively few, and represent the most generic indicators usually discussed in resilience literature. Such an indicator would be, for instance, 'Resilient design', which would be located under Level 1 'Prevention'. The methodology however permits to choose some of Level 2 indicators as not applicable (NA). If so, they will not be taken into account when calculating the total resilience value. The methodology also allows adding some new Level 2 indicators, depending on the operator's needs. While the assumption is that the chosen Level 2 indicators are equally important, also here a possibility of weighting (NA≤1) is included.

Combining Levels 1 and 2 into a same matrix, a simple framework for a resilience index emerges, as presented in *Table 1*. For this report, we have not yet populated totally the matrix. While we present a kind of a *blueprint* of the Level 2 indicators, subject for tailoring, the report, puts more emphasis on methodology than on the exact naming or listing of the indicators. For the sake of illustration, however, some indicators are already filled in, highlighted under a variety of titles in the literature dealing with critical infrastructure indicators. We have arrived at this set of Level 2 indicators by reviewing (see Appendices 1, 2, 4, 5, 8, 10, 11, 12, 14; Hosseini 2016) the existing indices and indicators, choosing the most obvious ones into our blueprint. It should be noted that vocabularies may differ, while one still is speaking basically about the same indicator. It is also to be noted that it might not be possible to agree on a set of indicators and their formulations in such a way that would satisfy everyone. This problem is

solved, as already articulated, by leaving a considerable room for tailoring the indicators to the needs of the operator. We limit the table only to the organizational and technological resilience domains.

As mentioned above, the rather detailed definition of the crisis management phases or categories (Level 1) is adopted here with the idea that it enables us to consider the possible indicators more carefully than if we would lump the categories together. This brings some new challenges, however, as these cycle 'phases' are not necessarily easily separable and strictly sequential.

The most problematic category here is, at least at the first look, that of 'Recovery' (Level 1), which is by definition the most central concept in resilience. The problem with the category of recovery is two-fold. First, most of the recovery literature – indeed those very books which bear the concept in their title (e.g. McEntire, 2015; Watters, 2014) – does not really have much to say about recovery but they concentrate on preparedness and response issues that facilitate recovery. As such this is not good or bad. But in order our methodology to work properly, aimed at *measuring* resilience, we should not measure the same indicator twice.

Table 1: Levels 1 and 2 *partially* populated

Risk assessment	**Prevention**	**Preparedness**	**Warning**	**Response**	**Recovery**	**Learning**
Failure data gathering	Safety and security culture	Preparedness plan and crisis organization	Audits	Situation awareness	Downtime	Evaluation
Knowledge of the context	Physical and cyber entrance control	Redundancy plan	Monitoring	Decision-making	Reduced service level	Institutional learning
Risk assessment procedure	Risk treatment plan	Cooperation agreements (external resources)	Early warning and alarm	Coordination (internal and external)	Costs	Implementation of lessons
Monitoring and review	Risk communication	Capability building		Communication (internal and external)	Unplanned maintenance	Technological upgradability
Testing and simulation	Resilience plan	Capacity building		Resource deployment	Restart	
	Resilient design	Technical supportability		Absorption/ damage limitation	Autonomy	
	Planned maintenance	Interoperability (internal and external)		Externalised redundancy	Insurance	
	Information sharing	Stakeholder management				

Second, a great part of the critical infrastructure resilience literature speaks in the language of resilience (or performance) loss triangle, discussed above. In this discourse, the metrics is based (correctly) on the idea that reducing the triangle would increase resilience, and that in turn can be measured with such indicators as time, money, other losses, or considering whether the system was put out of operation completely or not (Moteff, 2012). The same issue has been discussed in terms of 'recoverability' (Barker et al., 2013), which is the speed at which the network recovers.

Others (e.g. Ford et al., 2012) have however noted that considering just performance *outputs* may not be enough. Another parameter to consider is the *capacity* of the system to recover from subsequent failures or attacks.

All this comes to drawing the line between the planned 'Preparedness' for recovery and the actual 'Recovery'. We have resolved the issue by proposing to keep the facilitating plans and preparations for recovery strictly separate from actual recovery. Recovery category in our scheme should therefore be measured *only on the basis of historical incident data*, measuring the real recovery ability of a system. If such data is not available, one should omit (marking it as NA) this category of indicators.

The same challenge is drawing a line between preparedness and response. Like recovery, also response has to be planned. The issues related to planning for response have to be located under preparedness, which makes the evaluation of response indicators a post-crisis exercise measuring the actual performance. Otherwise we would measure the same indicator twice or mix plans and actual performance. Keeping them separate helps to find more vulnerabilities and makes the analysis more detailed and targeted.

4.3.3 Level 3: Generic indicators for selection

Level 3 is a typological application of Level 2, that is, it divides Level 2 indicators into smaller and more easily measurable processes or systems. For instance, should we have chosen 'Resilient design' as a Level 2 indicator, for a technological system on Level 3 this might mean that we separately look such indicators under this theme as 'Physical robustness', 'Cyber robustness', 'Redundancy', 'Modularity', 'Independency/Segregation'. Similarly, under Level 1 'Response', we find Level 2 indicator 'Communication', which should be divided into Level 3 indicators 'External' and 'Internal'.

In *Figure 6*, we have illustrated potential Level 3 indicators under 'Recovery' (Level 1) > 'Unplanned maintenance' (Level 2), with a considerable possible of tailoring.

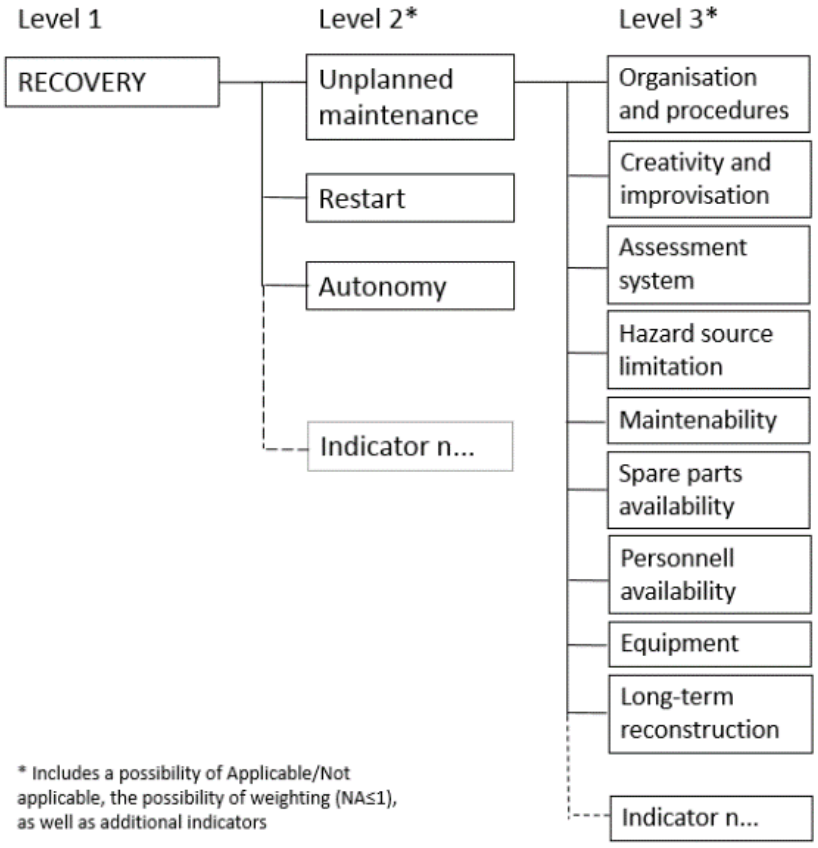


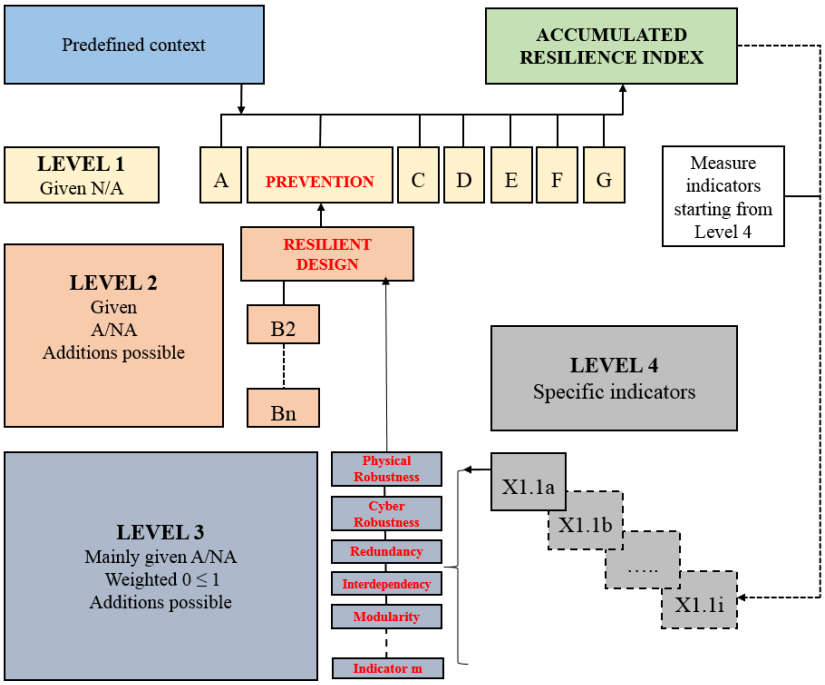
Figure 6: Level 3 application

While also these types of indicators are rather generic, we allow that some of them might be not applicable (NA) for some sectors, some facilities or some hazard scenarios, or they might be of lesser value compared to indicators that are more important. Thus the possibility of weighting (NA≤1) applies also here. Similarly as on Level 2, some tailored indicators can be added by the operator.

4.3.4 Level 4: Sector-specific indicators

Given that we have agreed upon the above levels 1-3 and respective indicators, one has to specify or tailor the indicators at Level 4 according to a certain sector (e.g. health care, electricity grid, rescue services, bridges), preferably focusing on a certain facility or function within these sectors (e.g. a hospital, energy production and distribution in a certain city, municipal tap water distribution, rescue services in a certain administrative area, a certain bridge or a tunnel), perhaps added with a hazard scenario (e.g. 100-year storm, dirty bomb in water treatment facility, complex ITC-SCADA-electricity problem caused by flooding), and so forth. In practice, for instance technological resilience indicators/measures have to be detailed carefully according to the characteristics of the concrete facility.

Level 4 is therefore to specify the indicator depending on the concrete application. One should notice that on Level 4 there are usually several indicators under one of the Level 3 indicators, that is, 4a, 4b, 4c, and so forth. These indicators are always specific and measured by their own metrics. An overall example, using again 'Resilient design' as an example of Level 2 and dividing that into more detailed Level 3 indicators to be represented on Level 4 by respective concrete applications, is presented in *Figure 7*.



A = Applicable, NA = Not applicable

Figure 7: Levels 3 and 4

The challenge then becomes to transform these Level 4 metrics and respective indicators into the commensurable metrics for calculating their Level 3 values. This is achieved by utilising the process maturity scale, as detailed in the next section.

4.4 Maturity level metrics

It is typical that in resilience measurements, be they quantitative, semi-quantitative or qualitative, different resilience characteristics are ranked on some scale and then aggregated to produce a resilience index (Hosseini et al., 2016). We follow the same scheme. Thus, the methodology developed here includes metrics, which makes it possible to come up with a single quantitative value for the selected critical infrastructure's overall resilience, or for resilience of part of it, or for resilience related to a specific hazard scenario.

Imagine that we already have Levels 2 and 3 populated with generic indicators. Then we start from Level 4 and work upwards (or backwards) when defining the system's resilience. This includes two tasks. First, one has to have or define the methodology, usually case- or application-dependent, of how to measure a certain indicator at Level 4. This might include any quantitative, semi-quantitative or qualitative processes. This evaluation methodology might be, and often is, already a fully existing practice in a critical infrastructure facility and the information would then be readily available.

Second, we should put the metrics of resilience of individual indicators so achieved on the same scale, necessitating some qualitative assessment. For this task, we will use the COBIT 4.1 (2007, pp.18, 19; for COBIT, cf. Appendix 8) general maturity model (originally ICT-related, wording here slightly modified) consisting of six maturity levels, as indicated in *Table 2*.[2]

Table 2: COBIT 4.1 process maturity model

Level 3 metrics			**Level 4 metrics**
0	**Non-existing**	Complete lack of any recognisable processes. The organization has not even recognised that there is an issue to be addressed.	Specific metrics of any indicator is transformed into processes, procedures, series of actions, series of operations, schemes, methods, or systems, corresponding one of the maturity levels 0-5.
1	**Initial/Ad Hoc**	There is evidence that the organization has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.	
2	**Repeatable but Intuitive**	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	
3	**Defined Process**	Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.	
4	**Managed and Measurable**	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	
5	**Optimised**	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other organization. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the organization quick to adapt.	

The above standard table might be enough to consider the maturity level of an application, that is, a certain Level 4 indicator's value transformed on the scale 0-5. However, we expect that in many cases it is useful to somewhat tailor the scale descriptions, using an existing standard, best practice, experience, or expert opinions. This does mean that the operator, who is doing the resilience measurement, has always to carefully consider each indicator and its resilience/maturity value. Imagine, for instance, that a hospital will cease to receive electricity from city grid. Then, one part of its redundancy would be to use reserve systems, for instance diesel generators or batteries. There might be a regulation stating that these reserves should be enough for at least x days. The operator then would evaluate, whether this level is, for instance, 3 or 4 on the maturity scale. If they would in practice do even better, say that the reserve energy source would last for $x+n$ days, then one could consider the maturity level as optimised (5).

[2] We are aware of the more recent COBIT 5 (2012), standardised as ISO/IEC 15504, which also could be used. Except that COBIT 5 is not called process maturity but process capability model, and the somewhat different labelling of the maturity levels, the main difference is that the latter combines the two first maturity levels into one and adds a new maturity level 2. The latter also makes a rough distinction between individual and organization knowledge (between levels 2 and 3). However, COBIT 4.1 is very usable due to its descriptive characteristics, whereas COBIT 5 is descriptively shorter and more abstract, and therefore, perhaps, more open to interpretations. In any case, in the current report, we use the older metric.

4.5 Calculating the overall resilience level

The overall CIRI, combining all the Level 1 indicators, is calculated based on the three lower levels of indicators, by simple aggregation. It is up to the operator, whether one wants to do this, or whether one chooses to concentrate on one Level indicator at time, which might be a more informative in terms of identifying the gaps in resilience.

Let us assume that we have done our measurements and evaluations on Level 4. Then we start by aggregating all the Level 4 information to get a score for all the Level 3 indicators, following the maturity model presented in *Table 2* above. Note that one might have to weigh the data according to sector to get the correct picture, depending on the operator's subjective evaluation.

Mathematically we end up with the following algorithm, to calculate the Level 1 indicators, starting from Level 3 and using the same notations as in Figure 5

$$Level\ 2\ indicator = \frac{1}{m} \sum_{i=1}^{m} w_i L3\ indicators$$

Where m is the number of Level 3 indicators. Further, the seven Level 1 indicators are estimated:

$$Level\ 1\ indicator = \frac{1}{n} \sum_{i=1}^{n} v_i L2\ indicators$$

Where n is the number Level 2 indicators. And to produce a final resilience index the seven Level 1 indicators are aggregated into one score

$$CIRI = \sum_{i=1}^{7} u_i\ L1\ indicators$$

Where u_k, v_j and w_i represent the weighting coefficient for individual indicators on respectively level 1, level 2 and level 3, with a value between 0 and 1 corresponding to the indicator's importance.

The methodology allows concentrating on only partial challenges, for instance measuring only two indicators (e.g. resilient design and recovery ability on level 2, with their Level 3 sub-indicators). Its main usefulness is that it enables to measure several indicators and transform them into one metrics, and thus making it possible to define the aggregated level of resilience on the scale 0-5.

The result of an imagined measurement is presented in *Figure 8.*

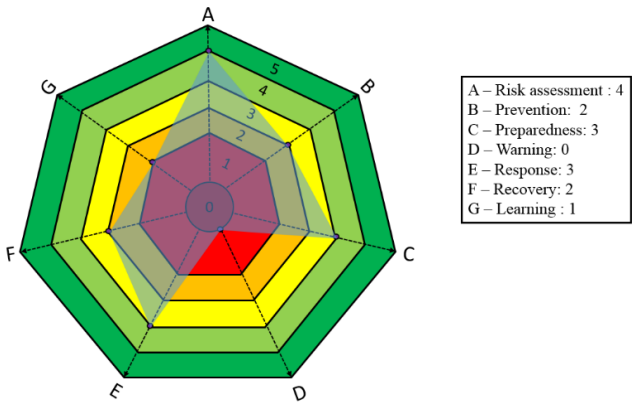


Figure 8: CIRI radar

5 Illustrative case applications

In the following applications, we illustrate the way how one can use the methodology, and especially how to develop meaningful indicators within the methodology and how the process maturity scale can be applied to the Levels 3 and 4.

5.1 Example 1: Oslo Airport Gardermoen fuel logistics[3]

In this example, we have an illustrative scenario applied to one indicator, using concrete Level 4 values.

5.1.1 Context

Imagine the following starting point:

Domain:	Technological
Hazard Type:	Man-Made Non-Malicious
Situational Factors:	Not Applicable

Oslo Airport Gardermoen is the largest airport in Norway and one of three regional hubs for SAS Scandinavian Airlines. All the aviation fuel for Oslo Airport Gardermoen comes from Sydhavna, Oslo. Aviation fuel is stored in an underground cistern at Ekeberg Oil Storage, which is part of the Ekebergåsen Fuel Depot facility at Sydhavna.

A man-made non-malicious incident, i.e., an accident of some kind, has occurred at Sydhavna which prevents aviation fuel being supplied from the Ekebergåsen Fuel Depot facility to Oslo Airport Gardermoen for 3 months.

Due to the nature of the operation, none of the following Situational Factors are considered to be significant for the analysis:

- Time of day (working hours vs. non-working hours)
- Seasonality
- Time of year (vacation vs. non-vacation periods)
- Location

5.1.2 Level 1 – Level 3 indicators

Let us define the levels under consideration as follows:

Level 1:	Prevention and Pre-event Mitigation
Level 2:	Resilient Design
Level 3:	Redundancy

The objective of this example is to develop a quantifiable ‘Redundancy’ metric that can be linked to the length of time of disruption to service (the Impact Metric), in this case the supply of aviation fuel from Sydhavna to Oslo Airport Gardermoen.

5.1.3 Level 4 indicators: Reserve Storage Capacity

Oslo Airport Gardermoen is supplied with aviation fuel from the depot in Ekebergåsen by rail using specially adapted wagons. At the level of activity at Oslo Airport Gardermoen in 2012 of 20 million passengers, 9 train loads of fuel were required per week, with each train carrying approximately 1 150 m^3 of product.

[3] This illustrative case applications has been prepared by Dr. Greg Baker, Chief Scientist at SP Fire Research AS, Norway (Appendix 6).

Over the three month (13 week) period of disruption to aviation fuel supplies from Sydhavna, based on the 2012 consumption figures, a total of 117 train loads of fuel would be required to maintain normal levels of flight/passenger activity at the airport. This equates to a total volume of 134 550 m^3 of aviation fuel.
Oslo Airport Gardermoen does have a small capacity of on-site storage (2-4 days). For the purpose of the analysis there is therefore assumed to be 4 train loads of fuel stored at the airport when the incident occurs, or 4 600 m^3 of fuel. This reduces the required volume of fuel, during the 90 day period of disruption, to 129 950 m^3.

The only alternative way to transport aviation fuel to Oslo Airport Gardermoen is via tank-trucks. At a capacity of 40 m^3 per tank-truck, 30 tank-truck loads are required to match the capacity of one train load. The greatest practical problem will be the availability of tank-trucks that can transport aviation fuel. For the purpose of this analysis, it is assumed that an average of 20 tank-truck deliveries per day, throughout the 3 month period of disruption, are able to be arranged as an alternative to the rail supply system from Sydhavna. During the 90 day period of the disruption, this amounts to 72 000 m^3 of aviation fuel, reducing the total amount of fuel storage required to avoid any disruption to airport services to 129 500 – 72 000 = 57 950 m^3. At a daily consumption rate of approximately 1 440 m^3 per day of normal operation, this equates to 40 days' supply of aviation fuel.

The Impact metric chosen for this example is length of time of disruption of service, with the range of possibilities tailored to suit the specifics of the incident scenario, i.e., 0 to 90 days. In *Table 4*, the 0 to 5 range of the COBIT Maturity Model is arbitrarily applied to the duration of the period of disruption to service that is applicable to this incident scenario.

Table 4: Impact Metric – Length of Time of Disruption of Service

0	Service disrupted for more than 90 days
1	Service disrupted for 30-90 days
2	Service disrupted for 7-30 days
3	Service disrupted for 3-7 days
4	Service disrupted for less than 3 days
5	No disruption to service

Having quantified the Impact Metric, the chosen mitigation strategy, in addition to the ability to receive 20 tank-truck loads of aviation fuel per day, is to invest in reserve storage capacity of 57 950 m^3, in addition to the 4 600 m^3 that already exists at Oslo Airport Gardermoen. The Redundancy Metric is therefore a volume of reserve storage capacity, where 57 950 m^3 equates to no disruption to service, based on the analysis presented above, and the existing storage capacity of 4 600 m^3 equates to slightly less than 90 days' disruption. This combination of Impact Metric and Redundancy Metric is presented in *Table 5*.

Table 5: Combined Impact Metric and Redundancy Metric

0	Service disrupted for more than 90 days	0 m^3 reserve storage capacity
1	Service disrupted for 30-90 days	38 630 to 4 600 m^3 reserve storage capacity
2	Service disrupted for 7-30 days	53 440 to 38 630 m^3 reserve storage capacity
3	Service disrupted for 3-7 days	56 020 to 53 440 m^3 reserve storage capacity
4	Service disrupted for less than 3 days	57 950 to 56 020 m^3 reserve storage capacity
5	No disruption to service	57 950 m^3 reserve storage capacity

5.2 Example 2: Earthquake and mobile telephone network[4]

In this example, like in the previous one, we have a concrete scenario and we concentrate on one indicator only, illustrating the Level 4 metrics.

5.2.1 Context

Imagine the following starting point:

Domain: Technological
Hazard Type: Natural

The United Nations International Strategy for Disaster Reduction (UNISDR) defines a natural hazard as a "natural process or phenomenon that may cause loss of life, injury or health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage" (UNISDR, 2009, pp. 20-21).

The European Environmental Agency in turn defines two categories for natural hazards: *hydro-meteorological* and *geophysical* (EEA, 2011, p. 19). Hydro-meteorological hazards include storms, extreme temperature events, forest fires, water scarcity and droughts, and floods. Geophysical hazards include snow avalanches, landslides, and earthquakes/volcanoes.

For the purposes of developing Level 4 indicators, no distinction is made as such between different types of natural hazards, although it is acknowledged that different types of hazards may influence the selection of the metrics for Level 4 indicators.

We also has a third variable in the context, namely Situational Factors (Scenario specific). In relation to critical infrastructure resilience, one measure of impact is the length of time that the service provided by the CI asset is below an acceptable level of service (noting that an acceptable level may be below the original level of service). In this context, another measure such as the cost of the disruption is considered to be a secondary measure of impact.

However, the length of time for the disruption is not in itself an absolute measure of impact. There are often, but not always, a number of factors (which we will term Situational Factors) which influence the impact of the disruption for a finite period of time.

Such Situational factors could again include:

- Time of day (working hours vs. non-working hours)
- Seasonality
- Time of year (vacation vs. non-vacation periods)
- Location
- Etc.

An example for item 'Time of the day' could be a four hour disruption to the metropolitan commuter train service at 1 am in the morning has a significantly different impact compared the same four hour disruption at 7 am in the morning – in the former case most commuters would be unaware that the service had been disrupted while they slept at home and they could travel as normal to their place of work, while in the latter case, a four hour disruption to service starting at 7 am would have a severe impact during the morning rush hour and cause chaos for commuters travelling to their place of work.

[4] This illustrative case applications has been prepared by Dr. Greg Baker, Chief Scientist at SP Fire Research AS, Norway (Appendix 6).

For item ‘Seasonality’, the time of year with regards to seasons can be important. For example, a disruption of 72 hours to a reticulated municipal heating system in winter in a cold country would have a major impact, whereas the same length of disruption in summer would go unnoticed. Conversely, a 72 hour disruption to the electricity supply in a tropical country in summer, where there was a heavy reliance on electrical air conditioning systems, could have serious health and wellbeing consequences, whereas the same length of disruption during a cooler part of the year would not be considered significant.

With regard to item ‘Time of the year’, vacation periods can mean low usage for some forms of critical infrastructure, but peak demand for others. For example, airports, roads, etc. are often near capacity during peak holiday periods, while commuter services would have very low patronage at such times. Often maintenance of critical infrastructure in urban areas is scheduled during vacation periods for exactly such reasons.

In relation to item ‘Location’, the location of the event causing the same disruption can have a significant bearing on the societal impact. For example, heavy rainfall upstream from the location of a critical infrastructure asset may mean that there is sufficient time available to implement contingency plans such that service disruption is avoided, whereas the same heavy rainfall in closer proximity to the critical infrastructure asset location may leave insufficient time for the contingency plans to be effective.

The type of critical infrastructure can also have a bearing on the thresholds for the impact (or perhaps more accurately societal tolerance) of disruptions to service levels. Consider the example of an event such as a major earthquake. The event has happened without warning and the immediate reaction of citizens is to try and make contact with immediate family members, relatives and friends, to check on their wellbeing, coordinate reunification efforts, etc. In the event of a major natural disaster of this nature, mobile phones are an essential communication tool for the general public. There is also a growing trend that less and less people have a traditional landline, so therefore the reliance on the mobile phone network is higher than has traditionally been the case, and is expected to increase in the future.

The experience in recent large-scale events has been that the mobile phone networks are immediately jammed as large numbers of users try to contact relatives and friends. This is caused by a combination of the sheer volume of users, as well as reduced capacity due to damage to various network hardware and infrastructure components. If mobile phone coverage was unavailable for say a six hour period, this would be very stressful for the populace, and considered unacceptable. A disruption of the same length, in the same event, to the electricity supply, would have a lesser impact, from the perspective that the majority of public would accept no electricity as manageable for a six hour period.

5.2.2 Level 1 – level 3 indicators

Let us define the levels under consideration as follows:

Level 1: Prevention and Pre-event Mitigation
Level 2: Resilient Design
Level 3: Robustness

5.2.3 Level 4 indicators: Mandatory Structural Design Capacity

The impacts of natural disasters can in some cases be translated into design provisions in building codes and structural loading codes, where mandated levels of structural strength are prescribed, a metric which will be called Mandatory Structural Design Capacity, or MSDC. In such cases critical infrastructure assets can be designed to withstand levels of structural loading that the regulator, on behalf of society, deems to be acceptable.

There are some caveats with regard to MSDC, as follows:

- Mandatory requirements are only applicable to the structural components of the CI asset in question, whereas other non-structural components may not be subject to the same levels of design and hence cause vulnerability in the overall CI asset system;
- Not all types of natural hazards are covered by building and structural loading codes;
- There are also some types of natural hazards where no amount of structural design will suffice for the nature and/or magnitude of the event. An example could be landslides where building foundations are totally undermined, or liquefaction caused by seismic events, where again building foundation are significantly affected. In such cases the choice of location, and hence the vulnerability, can have a major bearing on the impact of the natural hazard;
- Mandatory provisions still do have some level of associated risk, i.e., they are not risk free, and there are situations where the mandated design levels are actually exceeded by the natural event. In limit state design terminology, the ultimate limit sate (ULS) is said to have been exceeded in such cases

To illustrate the application of a Level 4 indicator, structural design of critical infrastructure assets to resist earthquake loading and the mobile telephone network is used as an example. The specific structural element is a free-standing transmission tower.

The Situational Factors component of the Context is noted as being "scenario specific". For this particular example, the situation that is assumed is that the network is swamped with calls as people try to contact family and friends in the immediate aftermath of an event. None of the Situational Factors listed above are considered to be relevant to this example – no matter what the time of day was, the season, the time of year or the location, the situation of the network being swamped is judged to still the same.

The Impact Metric that is used for this example is length of time of disruption to service, with an arbitrary example of the application of the COBIT Maturity Model shown in *Table 6*.

Table 6: Impact Metric – Length of Time of Disruption to Service

0	Service disrupted for more than 48 hours
1	Service disrupted for 24-48 hours
2	Service disrupted for less than 24 hours
3	Service disrupted for less than 12 hours
4	Service disrupted for less than 1 hour
5	No disruption to service

Having quantified the Impact Metric, it is then a case of developing a mitigation strategy (termed the Robustness Metric) that affects the Impact Metric. For this specific example the Robustness Metric is based on the seismic design capacity of the free-standing transmission tower. It is assumed that there is some relationship between length of disruption to service and seismic design capacity, i.e., the more robust the transmission tower the shorter the length of time of disruption to service – in structural engineering terms this relationship would be described as a *fragility curve*.

The methodology for calculating the seismic design capacity may vary between jurisdictions but when response spectral analysis is used the structure will be designed to withstand a certain proportion of gravitational acceleration (g), depending on the period of the structure.

A suitably qualified structural engineer would carry out an assessment and analysis of the free-standing transmission tower to determine the actual structural capacity, or ASC, which would then be compared to the MSDC.

The automatic expectation would be that the tower would comply with the structural strength requirements of the relevant building regulations. However, the age of the installation might mean that the regulations that the tower was originally designed to comply with may have been superseded by more stringent requirements, meaning that the structure no longer meets the current standard. Often

changes to building regulations are not retrospective, meaning that there is no obligation on an owner/operator of critical infrastructure assets to upgrade when new provisions come into effect. The age of the tower might also impact upon its structural strength, due to possible deterioration of materials, etc., over time, and hence reduced performance. It is even possible that the tower was under-designed in the first place.

To provide a simple illustration of this concept, the Impact Metric data from *Table 6* is repeated in *Table 7*, with the addition the ASC, as a percentage of the MSDC, as the Robustness Metric.

An arbitrary scale of risk tolerance has been suggested in *Table 7* where the ASC can be above or below the MSDC. With regard to the former, the owner/operator of the transmission tower may consciously choose to exceed the minimum required by the applicable building regulations in an effort to achieve a greater level of robustness. This situation also exemplifies the potential overlap between Level 3 indicator *robustness* and the associated Level 3 indicator *redundancy*. In could be argued that the COBIT scores of 4 or 5 in *Table 7* should in fact be designated as redundancy metrics.

Table 7: Combined Impact Metric and Robustness Metric

0	Service disrupted for more than 48 hours	ASC < 0.5MSDC
1	Service disrupted for 24-48 hours	0.5MSDC < ASC < 0.75MSDC
2	Service disrupted for less than 24 hours	0.75MSDC < ASC < 1.0MSDC
3	Service disrupted for less than 12 hours	ASC = MSDC
4	Service disrupted for less than 1 hour	1.0MSDC < ASC < 1.25MSDC
5	No disruption to service	1.25MSDC < ASC

The scaling of the metrics in *Table 7* would ultimately depend on the risk tolerance of the CI asset owner/operator and an associated cost-benefit analysis.

5.3 Example 3: Planned maintenance[5]

It goes without saying that maintenance is an important crisis prevention tool in technological systems. Resistance against disturbances can be considerably enhanced by introducing a good maintenance system as part of the organisational routine. According to the European Standard EN13306:2001 (EN, 2001) maintenance is defined as follows: "A combination of all technical, administrative and managerial actions, including supervision actions, during life cycle of an item intended to retain it in, or restore it to, a state in which it can perform the required function." This implies that maintenance also is strongly related to the restoration of a system or an item.

5.3.1 Context

Imagine the following starting point:

Domain: Technological
Hazard Type: All
Situational factors: Not defined

The simplest way to categorize maintenance is to say that it can either be preventive or corrective. (Barabady and Kumar, 2008) While preventive maintenance (Barabady and Kumar, 2007) means that the maintenance is performed in advance at set intervals to prevent the failure to occur, corrective maintenance (Moubray, 1997) means that components are run until they fail. Corrective maintenance can be both planned and unplanned. For some components with low criticality, it can be desirable to plan to run the components until they fail and then replace them, like for instance a light bulb. In case of an emergency caused by an unknown threat, unplanned maintenance will be scheduled. The effectiveness of unplanned maintenance, and maintenance in general, is highly dependent on the

[5] This illustrative case applications has been prepared by Bjarte Rød, UiT.

maintainability of the system. Maintainability reflects how easy, accurate, effective, efficient, and safe the maintenance action related to the product can be performed (Kumar et al., 2004), and refers to the measures taken during development, design and installation of a manufactured product (Dhillon, 1999). While these issues have been discussed elsewhere in more detail (Appendix 2), below we demonstrate how planned maintenance indicators at level 3 and 4 can be developed (based on the work of Fernandez and Marquez, 2012, as well as on the EFQM-enablers[6]) and combined with the process maturity scale.

5.3.2 Level 1 – Level 3 indicators

Let us define the levels under consideration as follows:

Level 1: Prevention
Level 2: Planned Maintenance
Level 3: Policy and strategy
Leadership
Personnel
Partnership and Resources
Process
Level 4: Process Maturity checklists**

The general characteristics of planned maintenance for utility networks have been defined and discussed by Fernandez and Marquez, 2012. These can in turn be detailed what we here call Level 3, including five separate indicators. We have first the 'Policy and strategy' indicator. The base line is the aim to develop and maintain the missions and vision of the organization via a clear stakeholder-focussed strategy, supported by relevant polices, plans, objectives, target and processes. In terms of maturity scaling, this is illustrated in *Table 8*.

Table 8: Policy and strategy – general attributes

0	Non-existing	Non-existing
1	Initial / Ad Hoc	Reactive execution and on purpose
2	Repeatable but Intuitive	Oriented to customer attending to the management of requirement
3	Defined process	Oriented to customer attending to the integrated performance to accomplish with the requirement. Standardization of the organization.
4	Managed and Measurable	Guide the organization for the statistical analysis with the purpose of improving the objectives, and the customers and internal understanding.
5	Optimized	Innovate in a sustainable way the processes and the technologies for the customers satisfaction and the social perception

The next Level 3 indicator is 'Leadership', which could be characterised as developing and facilitating the achievement of the mission and vision via appropriate actions and behaviour, leading the effective management of the organization and its relationship. Putting Leadership into maturity scales, we get *Table 9.*

Table 9: Leadership – general attributes

0	Non-existing	Non-existing
1	Initial / Ad Hoc	Lack of coordination, without reference nor defined responsibilities
2	Repeatable but Intuitive	Commitment of the interest groups and definition of the responsibilities for the projects
3	Defined process	Identification of personnel involvement and environment preparation for continuous improvement. Assignment of the responsibility based on processes
4	Managed and Measurable	Defining and implementing the mechanisms for the qualitative analysis
5	Optimized	Implement the concepts of continuous improvement and pro-activity

'Personnel', in turn, in this context indicates that the organization develops and manages the knowledge

[6] See http://ww1.efqm.org

and full potential of its people, as an individual as well as team-based, in order to manage its processes effectively according to its policy and strategy. This is scaled in the *Table 10.*

Table 10: Personnel – general attributes

0	Non-existing	Non-existing
1	Initial / Ad Hoc	Reactive and variable execution according to personal initiative, disorganization.
2	Repeatable but Intuitive	Management of the personnel according to the results, monitoring the efficiency and security.
3	Defined process	Development of knowledge and personal skills, facilitating decision-making activities.
4	Managed and Measurable	Quantitatively predict and evaluate the need and improvements of the human resources
5	Optimized	Take the potential of the personnel to optimize the efficiency of the organization

'Partnership and resources' as an indicator refers to planning and managing the organization's external partnership and external resources, in order to manage its processes effectively according to its policy and strategy, as illustrated in *Table 11*.

Table 11: Partnership and resources – general attributes

0	Non-existing	Non-existing
1	Initial / Ad Hoc	Request on demand and without control.
2	Repeatable but Intuitive	Management of partnerships and resources. Specific management of information.
3	Defined process	Unique and integrated definition of the information, attention to maintain the operation of the resources dependent on risks.
4	Managed and Measurable	Quantitatively analyze the operation of the resources, their acquiring and logistics
5	Optimized	Eliminate the causes that produce variations of the operations of the resources

Process as an indicator in this context refers to designing, managing and improving organization's processes in order to generate increasing value for its customers and other stakeholders according to its policy and strategy. This is illustrated in *Table 12.*

Table 12: Processes – general attributes

0	Non-existing	Non-existing
1	Initial / Ad Hoc	Unstable and unpredictable situation
2	Repeatable but Intuitive	Repetitive management and planning according to results.
3	Defined process	Unified and coherent management with process and objectives. Prediction through qualitative techniques.
4	Managed and Measurable	Estimate future efficiency and possible variances from the actual situation of the processes.
5	Optimized	Continuous improvement of the efficiency, through proper adjustment of the processes.

5.3.3 Level 4 indicator – checklists:

In the attachment at the end of the current report (*Tables 17-21*), we present checklists of practices and processes, based on the work of Fernandez and Marquez (2012), which can be tailored and used to evaluate the maturity levels of sector specific indicators.

5.4 Example 4: External interoperability[7]

One of the key indicators of critical infrastructure resilience is the interoperability between the operators and other actors involved in a disaster, most notably the emergency management personnel of the local community (police, rescue service etc.) Especially interoperable information and communication technology becomes important. Interoperability is defined by the European Commission "as the ability of information and communication technology (ICT) systems and the business processes they support to exchange data and to enable the sharing of information and knowledge" (European Commission, 2010).

[7] This illustrative case application has been prepared by Laura Petersen (EMSC), Kerstin Eriksson (SP), and Laura Melkunaite (DBI).

5.4.1 Context

Imagine the following starting point:

Domain: Societal/Organizational/Technological
Hazard Type: All

As a necessary step for increasing resilience between different emergency management agencies, interoperable communications should go beyond just interagency and include critical infrastructure operators as well. Several societal resilience frameworks point to the importance of interoperable communications as being "paramount to ensuring the flow of information is efficient and effective" (O'Sullivan et al., 2013). As the American Presidential Policy Directive on Critical Infrastructure Security and Resilience says, "a secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators" (O'Sullivan et al., 2013). In the case of a disaster affecting a critical infrastructure site, the CI Operators should be able to quickly and effectively communicate with emergency personnel what is happening on the ground, and a predetermined interoperable communication strategy is the best way to achieve this. Indeed, "ensuring [communication systems] are interoperable between organizations is paramount to ensuring the flow of information is efficient and effective" (O'Sullivan et al., 2013).

Furthermore, there needs to be interoperability between critical infrastructure operators themselves. The European Interoperability Framework explains that in order to have "effective cooperation, all stakeholders involved must share visions, agree on objectives and align priorities" (ISA, 2010). Interoperability then is a combination of both governance issues and technology. Technologically, operability involves the use of radios, programmers, and other new technologies to assure that real time communications are not lost during a disaster event. There exist a myriad of different radio and network solutions for this.

5.4.2 Level 1 – Level 3 indicators

Let us define the levels under consideration as follows:

Level 1: Preparedness
Level 2: External interoperability
Level 3: Governance interoperability
Technical interoperability
Common vocabulary
Message contingency

In the current example, we do not take into account any specific Situational factors.

5.4.3 Level 3 indicators

Our first Level 3 indicator under 'External interoperability' is that we call 'Governance interoperability'. To apply our process maturity scale to this indicator, we propose the following descriptions, illustrated in *Table 13*.

Table 13: Impact Metric – Governance interoperability

0	Non-existing	The CI Operator has never recognized interoperability to be an issue.
1	Initial/Ad-hoc	Interoperability is recognized as important in communicating with emergency managers and other CI operators, but no goals have been set and no standard processes exist.
2	Repeatable but Intuitive	Actors have agreed upon an interoperability goal.
3	Defined Process	Actors have agreed upon an interoperability plan, and understand the interoperability plan via training.
4	Managed and Measurable	Interoperability is seen as an ongoing process and the actors meet regularly to evaluate measures taken and update technologies.
5	Optimised	Interoperability, while still seen as an ongoing process, has been achieved among CI operators and emergency management.

Similarly, for 'Technical interoperability', following the USDHS Interoperability Continuum (USDHS, no year), we propose the process maturity scaling as in *Table 14*.

Table 14: Impact Metric – Technical interoperability

0	Non-existing	Data Elements: None Voice Elements: None
1	Initial/Ad-hoc	Data Elements: Swap files "Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, emails, faxes)." Voice Elements: Swap Radios
2	Repeatable but Intuitive	Data Elements: Common Proprietary Applications "The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data." Voice Elements: Gateways "Gateways retransmit across multiple frequency bands, providing an interim interoperability solution as agencies move toward shared systems."
3	Defined Process	Data Elements: Common-Interfaced Applications "Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom "one-off" links or a proprietary middleware application." Voice Elements: Shared Channels "Interoperability is promoted when agencies share a common frequency band or air interface (analog or digital), and are able to agree on common channels. However, the general frequency congestion that exists nationwide can place severe restrictions on the number of independent interoperability talk paths available in some bands."
4	Managed and Measurable	Data Elements: One-way standards-based sharing One-way standards-based sharing enables applications to "broadcast/push" or "receive/pull" information from disparate applications and data sources. However, it does not support real-time collaboration. Voice Elements: Proprietary Shared Systems
5	Optimised	Data Elements: Two-way standards-based sharing "Two-way standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly." Voice Elements: Standards-based Shared Systems

Our third Level 3 indicator 'Common terminology'. Terminology is also an issue in crisis communication and "it should not be assumed that all [involved] subscribe to the same definitions of key terms" (Reilly et al., forthcoming). Moreover, if there is a "lack of a common vocabulary between response organizations and between organizations… [that] adds to the problem" (Baker and Baker, 2007) Furthermore, agreeing to key terms ahead of a disaster helps lead to message consistency between actors (see the following indicator: message consistency).

The Common terminology indicator operationalization would involve agreeing beforehand to key terms to be used in the region to be shared among police, fire, and emergency responders and critical infrastructure operators. Since using previously agreed upon terminology increases societal resilience, the indicator could be the existence of an agreed upon lexicon. It could also be the degree to which the institutions are familiar with the lexicon and the ease with which they understand and employ it. For Common terminology indicator we propose the project maturity scaling as in *Table 15*.

Table 15: Impact Metric – Common terminology

0	Non-existing	Common terminology has not been acknowledged by the organization as an important part of resilience.
1	Initial/Ad-hoc	The need for Common terminology has been noticed; however no document or definitions exist. Instead, there exists an understanding between the people of the terms, but if a person were to change positions or interact with a new comer, terms would not necessarily have the same meaning.
2	Repeatable but Intuitive	NA
3	Defined Process	A lexicon of agreed upon common terminology exists.
4	Managed and Measurable	NA
5	Optimised	People self asses as being familiar with and understanding the common terminology and it is employed in the daily life of the various organizations.

Our last Level 3 indicator in the current cluster is that of 'Message consistency'. Message consistency is a key part to increasing societal resilience, as "the lack of message consistency from key stakeholders may contribute to the cascading effects of natural disasters and public order incidents" (Baker and Baker, 2007).

As such, several studies have shown that "the repetition of the same information through multiple channels during emergencies can help communicate situational urgency to target audiences, thus making it more likely that they will take appropriate action to protect themselves and their family" (Stephens, Barrett, and Mahometa, 2013).

The Red Cross has found that "if messages are contradictory, inconsistent or unclear, the result is confusion, apathy, mistrust and inaction" (IF RC & RC, 2013). In New Zealand, the Ministry of Civil Defense & Emergency Management found that "when we consistently give the same messages, we reinforce each others' advice and generate better public confidence and promote faster, better co-ordinated and informed actions by the public" (NZ MCDEM, 2010).

Message consistency has been operationalized by the Red Cross and the New Zealand Ministry of Civil Defense & Emergency Management via the publication of a set of key messages which are free to use and are intended to be duplicated by people working in disaster and emergency management. The New Zealand document "should be consulted when developing public information related to an event or regional hazard … and [for] any other medium in which emergency safety is communicated to the public" (NZ MCDEM, 2010). This is presented in terms of maturity scales in *Table 16.*

Table 16: Impact Metric – Message consistency

0	Non-existing	Message consistency has not been acknowledged by the organization as an important part of resilience, and no set of key, repeatable messages exist.
1	Initial/Ad-hoc	The need for message consistency has been noticed; however no document or set of key messages exist.
2	Repeatable but Intuitive	NA
3	Defined Process	Set of key messages have been agreed upon by all actors
4	Managed and Measurable	NA
5	Optimised	People self asses as being familiar with and understanding the key message and they are employed in the daily life of the various organizations.

6 Conclusions

We have above presented the Critical Infrastructure Resilience Index (CIRI), developed within IMPROVER project WP2 as its deliverable D2.2, and demonstrated how the related methodology works with a few illustrations. We argue that the methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors, facilities and hazard scenarios. The proposed methodology is suitable for organizational and technological resilience evaluation, but permits including also elements of societal resilience indicators to the evaluations. The user of the methodology is supposed to be the critical infrastructure operator in terms of self-auditing. The innovative potential is that with CIRI one is able to transfer the quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels. Its main usefulness is that it enables to measure several indicators and transform them into one metrics, and thus making it possible to define the aggregated level of resilience on the scale 0-5. It can also be used as a check-list kind of toll, not necessarily immediately preparing evaluations across all the indicators, but evaluating individual indicators in a structured way and in step-by-step fashion.

The methodology is also suitable to be developed into a computable or software based application. The next logical steps could be to develop this software and put the methodology into test with selected critical infrastructure operators. Should this to be done, one should aim at least for technology readiness level TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies), or even TRL 7 – system prototype demonstration in operational environment.

References

AIIC (2016) *Guidelines for Critical Infrastructures Resilience Evaluation*. Published by Italian Association of Critical Infrastructures' Experts (AIIC) in February.

ANSI/ASIS (2009) *Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use*. ANSI/ASIS.SPC.1:2009.

ANSI/ASIS (2012) *Maturity Model for the Phased Implementation of the Organizational Resilience Management System*. ANSI/ASIS.SPC.4-2012.

BAKER, M. and BAKER, H. (2007) Communication challenges in emergency response, March. [Online] Available from: https://www.researchgate.net/profile/Manoj_Bs3/publication/228966616_Challenges_in_using_distributed_wireless_mesh_networks_in_emergency_response/links/560a64de08ae840a08d55ae5.pdf. Accessed 8 February 2016.

BARABADY, N.N and KUMAR, R. (2008) Reliability characteristics based maintenance scheduling: A case study of a crushing plant. *Reliability Engineering and System Safety*, 93(4), pp.647- 653.

BARABADY, N.N. and KUMAR (2007) Reliability analysis of mining equipment: A case study of a crushing plant at Jajarm bauxite mine in Iran. *Journal of Performability Engineering* 3(3), pp.319-328.

BARKER, K., RAMIREZ-MARQUEZ, J.E., and ROCCO, C.M. (2013) Resilience-based network component importance measures,. *Reliability Engineering & System Safety*, Volume 117, September 2013, pp. 89-97

BEARSE, R. (2014) The Return on Investing in Personal resilience. *The CIP Report*, Center for Infrastructure Protection and Homeland Security, Volume 12 Number 7, January 2014, pp.21-24.

BOON, H.J. et al. (2012) Bronfenbrenner's bioecological theory for modelling community resilience to natural disasters. *Natural Hazards*, 60(2), pp.381–408.

BOONE, W. (2014). Functional Resilience: The 'Business End' of Organizational Resilience, *The CIP Report*, Center for Infrastructure Protection and Homeland Security, Volume 12 Number 7, January 2014, pp.5-8.

BRUNEAU, M. et al. (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectre*, 2003 19(4), pp.733-752.

BS (2014) *Guidance on organizational resilience*. BS 65000. 2012.

CHANG, S.L. et al. (2014) Establishing Disaster Resilience Indicators for Tan-sui. *Soc Indic Res,* Volume 115, pp.387-418.

CUMMING, G.S. et al. (2005) An exploratory framework for the empirical measurement of resilience. *Ecosystems*, 8(8), pp.975–987.

CUTTER, S.L. et al. (2008a) *Community and Regional Resilience: Perspectives from Hazards, Disasters, and Emergency Management*. CARRI Research Report 1. [Online] Available from: http://www.resilientus.org/library/FINAL_CUTTER_9-25-08_1223482309.pdf

CUTTER, S.L. et al. (2008b) A place-based model for understanding community resilience to natural disasters. *Global Environmental Change* 18(2008), pp.598–606.

CUTTER, S.L., BURTON, C.G. and EMRICH, C.T. (2010) Disaster Resilience Indicators for Benchmarking Baseline Conditions. *Journal of Homeland Security and Emergency Management, 7(1)*.

COBIT (2007) *Cobit 4.1 Excerpt. Executive Summary Framework*. United States of America: IT Governance Institute. [Online] Available from: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

COBIT (2012). *Cobit 5. A Business Framework for the Governance and Management of Enterprise IT*. USA: ISACA.

DHILLON, N.N. (ed.) (1999) Engineering Maintainability- Houston: Gulf Professional Publishing.

EEA. (2011) *Mapping the impacts of natural hazards and technological accidents in Europe: An overview of the last decade*, European Environment Agency. Luxembourg: Publications Office of the European Union, DOI: 10.2800/62638.

EN (2001) *Maintenance - Maintenance terminology*. European Standard, EN 13306:2001.

EUROPEAN COMMISSION (2016) *What is semantic interoperability?* [Last updated 18 February 2016.] [Online] Available from: https://joinup.ec.europa.eu/asset/page/practice_aids/what-semantic-interoperability..

EUROPEAN COMMISSION (2014). *Overview of natural and man-made disaster risks in the EU*. Commission Staff Working Document. Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience. Brussels, 8.4.2014. SWD(2014) 134 final.

EUROPEAN COUNCIL (2008) *Council Directive 2008/114/EC of 8 December 2008 on the identification and*

designation of European critical infrastructures and the assessment of the need to improve their protection.
EXECUTIVE ORDER (2013) *Executive Order 12636 - Improving Critical Infrastructure Cybersecurity*. Federal Register, T. P. o. t. U. S. o. America.
FERNÁNDEZ J. F.G. and MÁRQUEZ, A.C. (2012) *Maintenance Management in Network Utilities*. Springer Series in Reliability Engineering. London: Springer-Verlag.
FLINT, C.G. and LULOFF, A.E. (2005) Natural Resource-Based Communities, Risk, and Disaster: An Intersection of Theories. *Society & Natural Resources*, 18(5), pp.399–412.
FLINT, C.G. and LULOFF, A.E. (2007) Community Activeness in Response to Forest Disturbance in Alaska. *Society & Natural Resources*, 20(5), pp.431–450.
FLYNN, S.E. (2008) America the Resilient: Defying Terrorism and Mitigating Natural Disasters. *Foreign Affairs*, vol. 83, no. 2, (March/April), 2008.
FORD, R, CARVALHO, M, MAYRON, L. and BISHOP, M. (2012) *Towards Metrics for Cyber Security*, 21st EICAR Annual Conference Proceedings, May, pp.151–159.
FRANCIS, R. and BEKERA, B. (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering and System Safety* 121 (2014), pp.90-103.
GIBSON, C.A. and TARRANT, M. (2010) A 'Conceptual Models' Approach to Organisational Resilience. *The Australian Journal of Emergency Managemen*t 25(2), pp.6–12.
HOLLING, C.S. (1973) Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4, 1–23.
HOSSEINI, S., BARKER, K., and RAMIREZ-MARQUEZ, J.E. (2016) A Review of Definitions and Measures of System Resilience. *Reliab Eng Syst Safe*, 145, pp. 47 -61.
HSSAI (2009) *Concept Development: An Operational Framework for Resilience*. Homeland Security Studies and Analysis Institute. August 27, 2009.
IF RC & RC (2013) Public awareness and public education for disaster risk reduction: key messages. International Federation of Red Cross and Red Crescent Societies. [Online] Available from: http://www.ifrc.org/PageFiles/103320/Key-messages-for-Public-awareness-guide-EN.pdf. Accessed 24 February 2016.
ISA (2010) European Interoperability Framework (EIF) for European public services. Interoperability Solutions for European Public Administrations.16 December. [Online] Available from: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf. Accessed 24 February 2016.
ISO (2007) Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. 28004:2007.
ISO (2011) *Security management systems for the supply chain – Development of resilience in the supply chain*. 28002:2011.
ISO (2014a) *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations*. 28004-2:2014.
ISO (2014b) *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 3: Additional specific guidelines for adopting ISO 28000 for use of medium and small businesses (other than marine ports).* 28004-3:2014.
ISO (2014c) *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 4: Additional specific guidelines for adopting ISO 28000 if compliance with ISO 280001 is a management objective.* 28004-4:2014.
ISO/IEC (2009) *Risk management — Risk assessment techniques*. IEC/FDIS 31010.
ISO/PAS (2007) *Societal security - Guideline for incident preparedness and operational continuity management*. ISO/PAS 22399:2007.
ISO/IEC (2005) *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC 27001:2005.
ISO (2004) *Environmental management systems — Requirements with guidance for use*. ISO 14001:2004.
ISO (2000) *Quality management systems — Requirements.* ISO 9001:2000.
KLEIN, R.J.T., NICHOLLS, R.J. and THOMALL F. (2003) Resilience to natural hazards: How useful is this concept? *Environmental Hazards* 5 (2003), pp.35–45.
KAHAN, J.H, ALLEN, A.C, and GEORGE, JK (2009). An Operational Framework for Resilience. *J Homel Secur Emerg*, 6(1), pp.1 -48.
KOZINE I., and ANDERSEN, H.B. (2015) Integration of resilience capabilities for Critical Infrastructures into the Emergency Management set-up. In. Podofillini et al. (Eds), *Safety and Reliability of Complex Engineered Systems*. London: Taylor & Francis Group, London, pp.172-176.
KUMAR, R., MARKESET, T., KUMAR, U. (2004) Maintenance of machinery: Negotiating service contracts in

business-to-business marketing. *International Journal of Service Industry Management*, Vol. 15, 2004, Iss: 4, pp.400 - 413
LABAKA, L., HERNANTES, J. and SARRIEGI, J.M. (2015) Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant, *Reliability Engineering and System Safety* 141, pp.92-105.
LEDDRA Project (2014) *Land & Ecosystem Degradation & Diversification: Assessing the Fit of Responses*. [Online] Available from: http://leddra.aegean.gr/index.htm.
LINKOV, I. et al. (2013) Measurable Resilience for Actionable Policy. *Environmental Science and Technology*, 47, pp.10108−10110.
LEE, A.V., VARGO, J., and SEVILLE, E. (2013) Developing a Tool to Measure and Compare Organizations' Resilience. *Natural Hazards Review* (February), pp. 29–41.
MCASLAN, A. (2010a) *Community Resilience. Understanding the Concept and its Applications*. [Online] Available from: http://sustainablecommunitiessa.files.wordpress.com/2011/06/community-resilience-from-torrens-institute.pdf
MCASLAN, A. (2010b) *Organisational Resilience. Understanding the Concept and its Application*. [Online] Available from: http://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDoQFjAC&url=http%3A%2F%2Fwww.executiveaccelerators.com.au%2FLiteratureRetrieve.aspx%3FID%3D129836&ei=zSbVUv66GIinyQOGn4GICg&usg=AFQjCNHvoywQ-bRpx-9FZRc5yw6t7oQh5w&bvm=bv.59378465,d.bGQ
MCDANIELS, T. et al. (2007) Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, 13(3), pp.175-184.
MCENTIRE, D.A. (2015), *Disaster Response and Recovery. Strategies and Tactics for Resilience*. Hoboken, New Jersey: John Wiley & Sons.
MCMANUS, S. (2008) *Organisational Resilience in New Zealand*. University of Canterbury. [Online] Available from: http://ir.canterbury.ac.nz/bitstream/10092/1574/1/thesis_fulltext.pdf.
MOTEFF, J.D. (2012) *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, August 23, 2012, Congressional Research Service 7-5700. [Online] Available from: http://www.fas.org/sgp/crs/homesec/R42683.pdf.
MOUBRAY, N.N. (1997) *Reliability-centred maintenance*. Oxford, England: Butter-worth/Heinemann.
NIEUWENHUIJS, A.H., LUIIJF, H.A.M. and KLAVER, M.H.A. (2008). Modeling Critical Infrastructure Dependencies. In MAURICIO, P. and SHENOI, S. (eds.). *IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II*, Boston: Springer, October 2008, pp.205-214.
NORRIS, F.H. (2008) Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology*, 41, pp.127–150.
NZ MCDEM (2010) *Working from the same page: consistent messages for CDEM*. New Zealand Ministry of Civil Defense & Emergency Management.June 2010. [Online] Available from: http://www.civildefence.govt.nz/assets/Uploads/publications/Consistent-messages-complete-June-2015-v2.pdf.
O'SULLIVAN, T.L., KUZIEMSKYB, G.E., TOAL-SULLIVAN, D. (2013) Wayne Corneil *Unraveling the complexities of disaster management: A framework for critical social infrastructure to promote population health and resilience*. Social Science & Medicine, Volume 93, September, pp.238–246
PETIT, F.D. et al. (2013) *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Argonne National Laboratory, U.S. Department of Energy, April.
PETIT, F., WALLACE, K. and PHILLIPS, J. (2014) An Approach to Critical Infrastructure Resilience. *The CIP Report*, Center for Infrastructure Protection and Homeland Security. Volume 12 Number 7, January, pp.17-20.
PRIOR, Tim (2015) *Measuring Critical Infrastructure Resilience: Possible Indicators.* Risk and Resilience Report 9. ETH Zürich: April.
PURSIAINEN, C. and GATTINESI, P. (2014) *Towards Testing Critical Infrastructure Resilience*. Publications Office of the European Union, JRC Scientific and Policy Reports.
REILLY et al. (forthcoming) *A strategy for communication between key agencies and members of the public during crisis situations*. CascEff project, Deliverable 3.3.
RODRIGUEZ-LLANES, J.M., VOS, F. and GUHA-SAPIR, D. (2013) Measuring psychological resilience to disasters: are evidence-based indicators an achievable goal? *Environmental Health*, 12:115, pp.1-10.
ROSE, A.Z. (2009) *Economic Resilience to Disasters*, CARRI Research Report 8, CREATE Research Archive, Published Articles & Papers, 11-1-2009, pp.7-8.
ROSE, A. and KRAUSMAN, E. (2013) An Economic Framework for the Development of a Resilience Index for Business Recovery. *International Journal of Disaster Risk Reduction* 5, pp.73–83.
SHEFFI, Y. (2005) *The Resilient Enterprise - Overcoming Vulnerability for Competitive Advantage*. Cambridge,

MA: MIT Press.
SHERRIEB, K., NORRIS, F.H. and GALEA, S. (2010) 'Measuring Capacities for Community Resilience', *Soc Indic Res* 99, pp.227-247.
STEPHENS, K. K., BARRETT, A. K., and MAHOMETA M. J. (2013) Organizational communication in emergencies: Using multiple channels and sources to combat noise and capture attention. *Human Communication Research*, 39, pp.230-251.
STEPHENSON, A. (2011) *Benchmarking The Resilience In Organisations*. University of Canterbury, PhD Thesis.
STERBENZ, J.P.G., CETINKAYA, E.K., HAMEED, M.A, JABBAR, A., and ROHRER J.P. (2011) Modeling and Analysis of Network Resilience. *Proc the IEEE COMSNETS*, Bangalore, India.
UNISDR (2009) *UNISDR Terminology on Disaster Risk Reduction*, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009. [Online] Available from: http://www.unisdr.org/we/inform/terminology
USDHS (no year) *Interoperability Continuum: A tool for improving emergency response communications and interoperability*. U.S. Department of Homeland Security. [Online] Available from: https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2_1.pdf.
VLACHEAS, P., STAVROULAKI, V., DEMESTICHAS, P., CADOW, S., IKONOMOUR, D., GORNIAK, S. (2013) Towards End-to-end Network Resilience. *Int J Crit Infrastruct Prot* 6(3-4), pp.159 -178.
WANG, C. and BLACKMORE, J. (2009) Resilience Concepts for Water Resource Systems. J*ournal of Water Resources Planning and Management*, 135(6), 528-536
WATTERS, J. (2014) *Disaster Recovery, Crisis Response, & Business Continuity. A Management Desk Reference*. California: Apress.
WILSON, A.G. (2012) *Community Resilience and Environmental Transitions*. UK: Routledge.
YOUN, BD, HU., C., and WANG, P. (2011) Resilience-driven System Design of Complex Engineered Systems. *J Mech Design*, 133(10), pp.10108 -10110.

Attachment 1

Checklists of practices and processes, based on the work of Fernandez and Marquez (2012), which can be tailored and used to evaluate the maturity levels of sector specific indicators for measuring Level 4 indicators in the "(5.3) Example 3: Planned maintenance" above

Table 17: Maturity checklist – Policy and strategy

0	Non-existing	Non-existing
1	Initial /Ad-hoc	Reactive execution and on purpose
2	Repeatable and intuitive	• Establish and maintaining the mission, policy and strategy to plan and perform the processes. • Requirements are identified • Maintaining and validating the requirements with bidirectional communication. • Activities prioritized according to the requirements. • Performance objectives are established (including quality) according to definitions, procedures and standards. • Service agreements are established and maintained for managing and delivering services.
3	Defined process	• Process improvement opportunities are established and maintained. • Essential resources and identified and prioritized. • Plans and need for standard services are established. • Known and tested solutions are defined to solve or prevent the known incidents.
4	Managed and Measurable	• Encourage quantitative process-performance evaluation through benchmarking.
5	Optimized	• Encourage the continuous improvement of processes and technologies towards a world class maintenance.

Table 18: Maturity checklist – Leadership

0	Non-existing	Non-existing
1	Initial /Ad Hoc	Lack of coordination, without reference nor defined responsibilities
2	Repeatable but Intuitive	• Commitment of all involved personnel and groups with the requirements. • Establish and maintain plans for the performance, assign responsibilities. • Review in a high level of management the real state, performance and results. • Establish and maintain the measurements and the objectives, specifying the procedures to manage them.
3	Defined process	• Establish record and maintain the organizational and standardized processes, systems, technologies, procedures and criteria. • Deploy the process along with the organization. Establish the work environment for improvement. • Determine and categorize the risk sources. Establish, validate and analyse the training and service continuity. • Establish and maintain guidelines, methods and criteria to take decisions about formal issues, selection the solutions.
4	Managed and Measurable	• Budgetary analysis and prediction including costs of corrective actions and improvements
5	Optimized	• Assure the continuous improvement and collect potential improvements and innovations of process and technologies systematically. • Evaluate improvement effects including costs analysis. • Elect, develop and implement the improvements and innovation in the organization, fulfilling the objectives. • Evaluate the improvement and innovations effects according to expected, including costs.

Table 19: Maturity checklist – Personnel

0	Non-existing	Non-existing
1	Initial /Ad Hoc	Reactive and variable execution according to personnel initiative, disorganization.
2	Repeatable but Intuitive	• Plan the necessary knowledge, participation and relationships. • Monitor the commitment and performance of the personnel, their security and health. • Notify the real state, performance and results to different hierarchy levels.
3	Defined process	• Establish the rules and guidelines to integrate in teamwork and work environment. Value personnel performance. • Establish, provide and evaluate strategic tools and training need to perform the roles effectively and efficient. • Coordinate and collaborate with interest groups and personnel, controlling the access and solving critical issues and defects. • Develops the change management taking in count the impacts in the services, making necessary corrective actions.
4	Managed and Measurable	• Establish and maintain quantitative process-performance models, objectives, measures and techniques and resources, defining baselines.
5	Optimized	• Take the potential of the personnel to optimize the efficiency of the organization.

Table 20: Maturity checklist – Partnership and resources

0	Non-existing	Non-existing
1	Initial /Ad Hoc	• Request on demand and without control
2	Repeatable but Intuitive	• Estimate and assign costs and reasonable efforts. • Employ techniques more frequently used for planning task such as Critical Path Method (CRM), Programme evaluation review techniques (PERT) and Justin-time (JIT), Criticality analysis, Queuing theory or MRP. • Plan data management and necessary resources in all the life cycle, reconciling plans with real circumstances. • Record monitor and maintain the data traceability of the progress, performance and other issues in a management system. • Select and maintain potential suppliers and external services periodically, including their agreements. • Record, monitor and maintain the quality, performance and other issues, using a monitoring system and techniques more frequently used to evaluate quality such as Quality loss function (QLF), Quality Circles (QC), and Quality function deployment (QFD). • Establish, monitor, record and maintain the configuration and changes management in an inventory system, ensuring integrity. • Obtain and analyse measurement reliable and useful data, and employing techniques more frequently used assess the results such as check-list, histograms, Total productive maintenance (TPM) or Universal maintenance standards (UMS).
3	Defined process	• Establish and maintain the repository of data, process information and experiences in a knowledge management system and using techniques such as Strength, weakness, opportunities, threats (SWOT) and brainstorming. • Define the measurement techniques concerning resources, customers and services, using a geographical information system (GIS) and techniques such as process capability and casual models.
4	Managed and Measurable	• Establish, spread and remote techniques for quantitative modelling such as simulation, deterministic, replacement/renewal and Markovian. • Develop, monitor, record and maintain quantitatively analysis and predictions in a Reliability Cantered Maintenance (RCM) system and knowledge management system using techniques such as Operational reliability analysis (ORA) or Statistics process control (SPC).
5	Optimized	• Establish, spread and promote techniques for optimization such as Game Theory, Risk-cost optimization, Life cycle cost analysis (LCCA) and Optimized production technology (OPT). • Automate, monitor, record and support actions in an expert support system based in symptom-cause reasoning, and using techniques such as fishbone diagram, Failure root cause analysis (FRCA) or 5WH2:Who, what, when, where, whey, how, and how.

Table 21: Maturity checklist – Processes

0	Non-existing	Non-existing
1	Initial /Ad Hoc	All the basic functions are implemented as best efforts.
2	Repeatable but Intuitive	• Monitor and control the performance against the plans periodically and in determined milestones, escalating real state, performance and results. • Identify inconsistency and determine corrective actions. • Establish, monitor, evaluate and maintain the supplier performance. • Ensure the resolution of the performance, determining corrective actions. Operate and maintain the services.
3	Defined process	• Appraise the processes periodically in order to improve them through corrective actions. • Use defined processes and systems to estimate and plan activities, maintaining the global integrity and reviewing according to commitments. • Monitor and effective use of the resources to ensure the performance of processes and services, taking corrective actions. • Evaluate, prioritize and monitor the risks periodically implementing mitigation actions. • Translate the requirements in solutions for the service, ensuring integrity and connectivity.
4	Managed and Measurable	• Develop, monitor, record and maintain analysis and qualitative predictions of performance, deviation and risks. • Manage and analyse performance statistically implementing the necessary corrective actions. • Stabilize the process-performance to achieve the quantitative objectives.
5	Optimized	• Identify and analyse the root-causes of performance, defects and problems systematically determine improvement actions. Implement and monitor the improvement actions of the root causes to mitigate the consequences.