From risk management to resilience management in critical infrastructure

Authors: Bjarte Rød[1*], David Lange[2], Marianthi Theocharidou[3], Christer Pursiainen[4]

[1] PhD candidate / MSc, UiT The Arctic University of Norway, Department of Technology and Safety. Postal address: UiT The Arctic University of Norway, Department of Technology and Safety, P.O. Box 6050 Langnes, 9037 Tromsø, Norway.

[2] Dr. / Senior Lecturer, The University of Queensland, School of Civil Engineering, Faculty of Engineering, Architecture and Information Technology. Postal Address: School of Civil Engineering, Building 49 Advanced Engineering Building, Staff House Road, The University of Queensland, St Lucia QLD 4072 Australia. Email: d.lange@uq.edu.au

[3] Dr. / Project Officer, European Commission, Joint Research Centre (JRC), Directorate E – Space, Security and Migration, Technology Innovation in Security Unit. Postal Address: European Commission, Joint Research Centre (JRC), Directorate E – Space, Security and Migration, Technology Innovation in Security Unit, via E. Fermi 2749, 21027, Ispra (VA), Italy. Email: mtheohar@gmail.com.

[4] Professor, UiT The Arctic University of Norway, Department of Technology and Safety. Postal address: UiT The Arctic University of Norway, Department of Technology and Safety, P.O. Box 6050 Langnes, 9037 Tromsø, Norway. Email: christer.h.pursiainen@uit.no

[*]Corresponding author: Email: Bjarte.rod@uit.no, Tel: (+47) 98615331

ABSTRACT: The article discusses critical infrastructure resilience in terms of how it could be incorporated into the existing safety and security practices, namely the ISO 31000 risk management standard. The article starts by outlining the resilience discourse, focusing on the organizational, technological and societal domains of resilience. It goes on to present an approach to how the risk management standard can be extended to a critical infrastructure resilience management framework. Focusing in particular on the organizational and technological resilience domains, which are considered those that can most readily be controlled by critical infrastructure operators, the article presents one of the resilience assessment techniques in some detail to operationalize the overall management framework. In so doing, the article proposes a pre-standardization input for critical infrastructure resilience management, tested in an operational environment. The article concludes with five maxims for this objective: no duplicate practices; tailorability; plurality of assessment techniques; measurability; and relative ease of use.

Keywords: critical infrastructure; organizational resilience; technological resilience; societal resilience; risk management; ISO 31000; resilience measurement; resilience assessment; resilience analysis; resilience evaluation

1 INTRODUCTION

Critical infrastructure resilience (CIR) has been a subject of vibrant scholarly discussion for over a decade. Yet there is no consensus on some fundamental questions, most importantly on how CIR could be assessed, tested and duly enhanced. In other words, a proper approach to CIR management is missing. Such a situation has hindered the development of the concept into a practical tool that could be used by critical infrastructure (CI) operators. The current article seeks to resolve this challenge. Contributing new insights to both the conceptual and the methodological discussion in the field, it focuses on organizational and technological resilience but also takes on board some elements of societal resilience.

While the concepts of CI and CIR will be defined below, management can be understood as a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives (ISO 2015). The main puzzle is whether CIR management can be standardized in the same manner as risk management, providing generic guidelines for operators in their crisis management. Can this be done in a way that is relatively easy to incorporate into the functioning practices of operators, complementing their existing practices rather than duplicating or replacing them?

We propose such a framework for CIR management, originating from the investigations of a recently concluded European Union project (IMPROVER). Some results from the project have been presented earlier in conference papers (Lange et al. 2017; IMPROVER Project 2017a; Pursiainen et al. 2017; Rød et al. 2017). The current article develops our findings further and transforms them into a holistic approach, suitable for further standardization. In short, the article proposes a pre-standardization input for CIR management, tested in an operational environment as presented below.

In filling a clear research gap in the field, the novelty of the current approach is, firstly, that the CIR management framework is largely based on a structure and terminology that are compatible with the existing International Standardization Organization (ISO) 31000 risk management practices. To this end, it builds on them but at the same time creates an easily applicable more holistic scheme related to resilience instead of mere risks. Secondly, it is flexible and does not exclude plurality in choosing between the more detailed techniques to assess CIR within this generic framework. In this way, the framework attempts to overcome the typical 'schools of thought' antagonism in the field, and focuses on the needs of practitioners, in our case CI operators.

We begin by providing some basic definitions of CIR, and an overview of the relevant literature. We then present and justify the proposed framework in terms of how to incorporate CIR into the above-mentioned existing risk management standard. After that, we operationalize the framework, presenting one technique in some detail against a 'test case', thereby illustrating the methodological step-by-step principles of how to use the framework. Lastly, we discuss the main principles that should inform the development of CIR management, and especially CIR assessment, into a more mature, applicable, and easy-to-use tool for CI operators.

2 WHAT IS CIR?

While the concept of resilience was long used mainly in the textile and metal industry to express the elasticity of the material, its current scientific origins can be traced back to the ecosystem theorizing of the 1970s (Holling 1973; Pimm 1984). From the early 2000s onwards, the concept was popularized in many fields, not least in safety and security.

Our emphasis is on CIR as a part of the more generic resilience literature. The resilience concept penetrated the field of CI proper relatively late. Yet by the mid-2010s it had already replaced the earlier focus on mere CI protection (CIP), not only in scientific studies but also in related policy documents (Pursiainen 2009; Pursiainen and Gattinesi 2014; Theocharidou et al. 2018). CIR was needed because it was understood that complete CIP can never be guaranteed. Moreover, achieving the desired level of protection is normally not cost-effective in relation to the actual threats.

2.1 Definitions of CI and CIR

While there are several slightly different national and institutional definitions of CI (CIPedia n.d.), we refer to the one often used in the European context in particular: "An asset, system or part thereof […] 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 […] as a result of the failure to maintain those functions" (European Council 2008).

As for CIR, there are again numerous slightly different definitions of resilience (CIPedia n.d.). In the field of safety and security, ISO defines 'resilience' simply as an "ability to absorb and adapt in a changing environment" (ISO 2018a). The concept remains contested to some extent, however, even in the rather narrow field of so-called resilience engineering, having several different meanings (Woods 2015). A convenient starting point for our purpose, applicable to CI systems, however, is the definition provided by the United Nations Office for Disaster Risk Reduction (UNDRR, formerly UNISDR): "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform 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 through risk management" (UNISDR n.d.b).

Following this definition, there is a certain temporal dimension to CIR (Luiijf 2008; HSSAI 2009; Kozine and Andersen 2015; ANL 2013; Petit et al. 2014; Pursiainen et al. 2016), covering the phases *before*, *during* and *after* an event. This is illustrated in Figure 1, which is an application of the so-called resilience triangle, a common feature in CIR literature in its many forms (Bruneau et al. 2003; Chang and Shinozuka 2004; McDaniels et al. 2007; Wang and Blackmore 2009; Dessavre et al. 2016; Hosseini et al. 2016; Panteli et al. 2017).

Figure 1 depicts three critical systems *A*, *B* and *C*, confronted with an unwanted event, with the vertical axis representing the service level and the horizontal axis representing time. The curves represent different resilience strategies through which organizations deal with hazards and the respective investments in different CIR phases. System *A* is not only less resistant, but when broken it plummets and recovers

slowly. System *C* is resistant but finally collapses altogether. System *B*'s resilience curve resembles the idea of the resilience triangle. The fundamental idea is that reducing the triangle in all of its dimensions would increase resilience. This is in a way the normative dimension of resilience. In some cases, it is also possible and desirable for the system to rebound not to its former state but to a new steady state that is "more secure and resilient" (DHS 2013, p. 19).

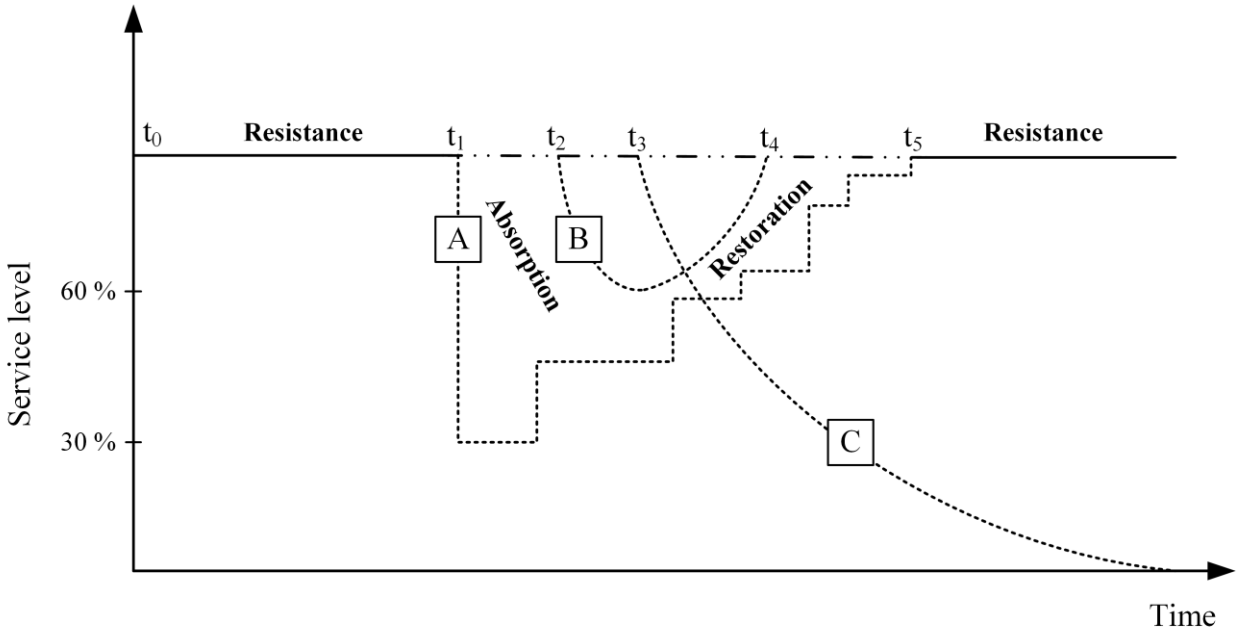


Figure 1.

2.2 Assessment of CIR

If the intention of CIR management is to enable a system to resist, absorb, and recover from unwanted events, in practice this means finding ways to *assess* the existing resilience of a CI in order to *enhance* it (Henry and Ramirez-Marquez 2012; Pursiainen et al. 2016; Rød et al. 2017). Hence the importance of CIR assessment as the basis of CIR management.

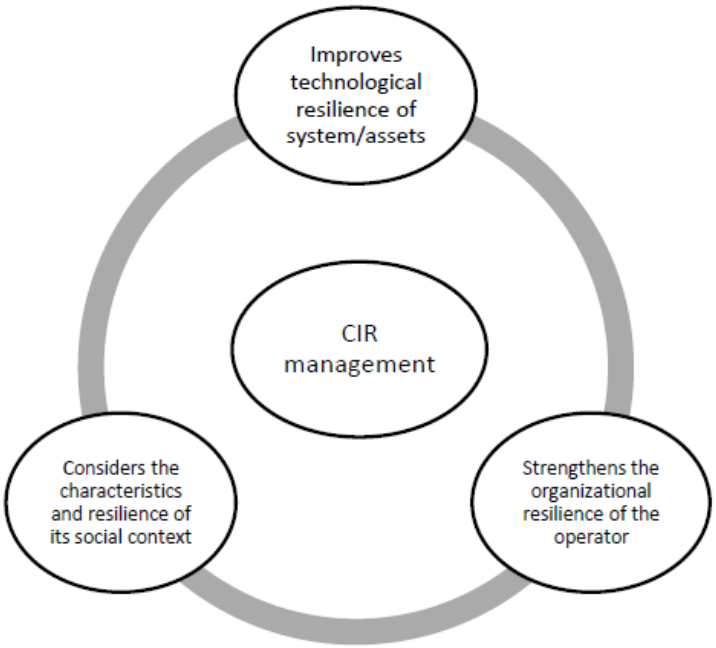
Commonly accepted metrics for CIR are not yet available, although there are many candidates. We have identified twelve CIR assessment techniques that are most promising in the current context (Hollnagel 2010; ANL 2013; Lee et al. 2013; OECD 2014; AIIC 2016; RESILIENS Project 2016a-c; Pursiainen et al. 2016; IMPROVER Project 2017b; Hollnagel 2017; Petersen et al. 2018, IMPROVER Project 2018; Australian Government n.d.). Our review shows that they are usually based on a set of indices, which are then added in a simple cumulative way to form a holistic CIR index. While some remain simple typologies, others have been developed toward software applications already in use. The techniques differ considerably, especially in such issues as their selected domain of resilience (see below), the required resources, ease of use, outcome in terms of quantitative or qualitative results, applicability of the results to create

enhancement strategies, and so forth. In the final analysis, all techniques have their pros and cons. We have summarized the main typological characteristics of these techniques in Appendix 1.

We strongly defend a *plurality of techniques* for CIR assessment. In so doing, we follow the example of the ISO 31000 methodological approach (ISO/IEC 2009; ISO/IEC 2019) on risk assessment. Yet a CIR management standard should also include some basic, generally agreed-upon criteria for a recommended CIR assessment technique. We will discuss some characteristics to this effect below.

2.3 Domains of CIR

While the UNDRR definition above works well as a baseline, the resilience concept remains multifaceted. Consequently, we may differentiate between several domains of resilience in the literature. The *technological*, *organizational* and, in part, *societal* domains are the most relevant for CIR. These domains inescapably influence and overlap with one another, but keeping them analytically separate is nonetheless justifiable; most notably, this is crucial in defining which actor is responsible for a specific action associated with CIR. Figure 2 illustrates this relationship.



<Fig. 2. [Approximately here]>

Technological resilience mainly refers to the physical properties of the CIs, focusing on their ability to resist damage and minimizing any loss of function during a crisis, or quickly repairing the unwanted effect (Bruneau et al. 2003; Kahan et al. 2009; Youn et al. 2011; ANL 2013; Sterbenz et al. 2013; Vlacheas et al. 2013; Francis and Bekera 2014; Linkov et al. 2014; Labaka et al. 2015; Nemeth and Herrera 2015;

Hosseini et al. 2016; Levenberg et al. 2016; Pursiainen 2017; Rød et al. 2017; Ilbeigi and Dilkina 2017; Barabadi and Ayele 2018). A quantitative assessment is appropriate in this domain. Technical analysis often requires modeling and simulation tools, integrating the analyses at the system and component level, and incorporating concepts such as reliability, robustness, maintainability, and recoverability (Lounis and McAllister 2016). For instance, to quantify the recoverability of a system consisting of 'nodes', one could assess the probability of a certain node recovering prior to a specific time, and repeat this process for all nodes in the system. Based on this, the system service recoverability, that is, the probability that full functionality before a specific time will be achieved, is calculated (Barker, Ramirez-Marquez and Rocco 2013).

Organizational resilience refers to the organizations that operate and manage the CIs, including the processes of organizational capacity and capability, planning, training, leadership, communication, and so forth. There is a growing body of literature and certain standards that directly aim at developing indicators to measure organizational resilience (McManus 2008; ANSI/ASIS 2009; Kahan et al. 2009; Gibson and Tarrant 2010; Stephenson 2010; ISO 2011; Linkov et al. 2013; ANL 2013; ISO 2014a-c; Petit et al. 2014; Hosseini et al. 2015; Labaka et al. 2015; Prior 2015; AIIC 2016). Organizational CIR analysis is generally performed qualitatively, but can in some cases be transformed into semi-quantitative scales, which reflect the maturity of processes that support the resilience-related capacities or capabilities.

Societal resilience is important in CIR not only because CI operators are subject to government regulations, but also in relation to the ability of civil society, social groups and individuals to cope with CI contingencies. It is therefore related to the needs and tolerances of the community that is dependent on the service provided by the CI. Having this information to hand can help CI operators to identify the minimum required service levels. While there are infrastructure performance studies that integrate both societal and technical components in their analysis (Choi et al. 2019), most of the efforts have been directed toward development of societal/community resilience indicators (Klein et al. 2003; Chang and Shinozuka 2004; Flint and Luloff 2007; Cutter et al. 2008; McAslan 2010; Sherrieb et al. 2010; Boon et al. 2012; LEDDRA Project 2014; Aldrich and Meyer 2015; IMPROVER Project 2016; Petersen et al. 2017; Rosenqvist et al. 2018). These techniques usually list socio-economic or institutional-political indicators at a very general level. They can, however, be utilized in defining the preconditions (i.e. societal context) for organizational and technological CIR assessment.

3 INCORPORATION OF CIR INTO THE RISK MANAGEMENT STANDARD

In this paper we will present and exemplify a CIR management framework that is compatible with existing risk management practices. The proposed framework has been developed in close cooperation with CI operators in association with the European Union Horizon 2020 project IMPROVER, using so-called living laboratories to test the framework. In total, eight interactive workshops were organized by the project. Participants included the project associate partners (representatives of CI owners and operators throughout Europe), advisory board members (such as blue light organizations and experts in resilience), CI stakeholders who are part of the European Reference Network for Critical Infrastructure Protection

(ERNCIP), as well as academics and other relevant stakeholders interested in CI and resilience (Petersen et al. 2019). A brief description of each workshop where the data were collected, analyzed and formalized into the current CIR management scheme can be found in Appendix 2. The final implementation of the CIR management framework was presented in two separate pilot implementation or validation workshops. Prior to these two workshops, the data were collected through document analysis and field studies. The evaluation of the performance of the framework, using several CIR assessment techniques, was conducted in a semi-real environment, designed to provide better external validity than traditional laboratory experiments (Rossman and Rallis 2011). Moreover, during the pilot implementation workshops, surveys and focus groups were used to collect data for the critical evaluation of the performance of the framework. By combining two or more data sources, investigators, theoretical perspectives, methodological approaches or analytical methods, one could say that a triangular approach was taken (Denzin 2017; Kimichi et al. 1991), making the implementation, testing and evaluation of the framework more rigorous.

In the current section, we present the proposed CIR management framework (and illustrate how to operationalize it in the subsequent section). While first justifying the use of the ISO 31000 risk management standard as a basis, we then present and define the major elements of the framework. The section concludes with a short discussion on how to select the specific techniques to be used in the CIR assessment in particular.

3.1 The benefits of using ISO 31000 as a basis

Some theorists differentiate between 'risk' and 'resilience' as rather antagonistic schools of thought, but a unified risk-resilience approach is often proposed (Aven 2019). As already implied in the UNDRR definition of resilience above, we see the two processes as enriching and supporting one another. Moreover, we do not attach much importance to the scholastic discourse on whether resilience is part of risk management or the other way around. Our approach is based on mapping CIR against the definitions and concepts already used for risk management in the ISO 31000 international standard (ISO 2009a; ISO 2009b; ISO 2018b; ISO/IEC 2009; ISO/IEC 2019).

This approach has an advantage in that many organizations are already familiar with the standard. True, criticisms have been levelled against ISO 31000 within the risk research community. The original 2009 standard was claimed to be unclear, leading to illogical decisions if followed, impossible to comply with, and not mathematically based, having little to say about probability, data, and models (Leitch 2010; Aven 2011b). By the same token, the revised 2018 version was criticized for its lack of scientific grounding and for being inconsistent (Aven and Ylönen 2019).

While we partially acknowledge this criticism, we contend that the most important achievement of ISO 31000 is its approximation of terminology and its understanding of the basic framework of risk management processes among practitioners. Notwithstanding its shortcomings, it has enhanced the generic risk management level. Indeed, the standard's basic structure is used "in most risk analysis textbooks" (Aven 2016, p. 6), in practical safety and risk work conducted in companies (Aven and Ylönen

2019), as well as by international organizations such as the EU (European Commission 2019 and 2010), the Organization for Economic Co-operation and Development (OECD 2018), and the UNDRR (UNISDR 2017).

This pragmatic argument justifies the effort toward a CIR management system that is aligned with existing widespread practice, rather than proposing a completely new scheme that would probably lead to considerable resistance by practitioners. Thus, we see ISO 31000 as an opportunity to introduce CIR practices into the field.

3.2 ISO 31000 plus CIR management

ISO 31000 divides risk management into a process including 'setting the scope, context and criteria', 'risk assessment', and 'risk treatment', in addition to the cross-cutting functions of 'communication and consultation' and 'monitoring and review' through all of the steps. Risk assessment consists of risk identification, risk analysis, and risk evaluation. Risk treatment in turn comprises measures to prevent or mitigate the risks on the basis of the risk evaluation.

Our approach enhances the current risk management practices by adding the CIR component. In contrast to the pre-event character of risk management, CIR management emphasizes preparedness, response and rapidity of recovery applied during and after the event. In other words, unwanted events and surprises are anticipated to occur, as prevention and mitigation are not always sufficient (Park et al. 2013).

The following definitions of the CIR management components have been proposed (Lange et al. 2017, IMPROVER Project 2017a):

- *CIR management* is the name for all of the coordinated activities undertaken to direct and control an organization with regard to its resilience, including the processes below.
- *Setting the scope, context and criteria* for CIR management is the first phase. It entails identifying the criteria for the subsequent analysis and evaluation, such as a time window and other basic parameters, as well as perceived societal tolerance levels or minimum quality/quantity of service performance for a community to survive.
- *CIR analysis* is the process of determining the level of resilience with one or more appropriate techniques.
- *CIR evaluation* is the process of comparing the results of a CIR analysis with selected criteria to determine whether the level of resilience is acceptable and to identify priority areas for further enhancement.
- *CIR enhancement* is the process of developing and implementing plans for improving resilience, for example by focusing on the absorptive, adaptive or restorative capacity. The enhancement will change the input into the whole process, making CIR management an iterative activity that needs to be constantly revisited by the organization.

Against this backdrop, the framework for parallel and interlinked risk management and CIR management is presented in Figure 3.

<Fig. 3. [Approximately here]>

Risk identification, as a part of typical risk management, only needs to be conducted as a facet of the risk assessment process, as it also feeds into the CIR assessment. Risk assessment also provides important input for the CIR assessment by supplying information about the impact and the vulnerability of the CI to specific hazards. On the other hand, CIR analysis feeds back into the risk management process. The output of the overall framework supersedes a mere CI risk treatment plan, forming a more holistic CIR enhancement plan. The use of the term 'treatment of risks' is duly included in the final result in the iterative process of 'enhancing resilience'.

3.3 Plurality of CIR management techniques

Standards should define the main concepts and goals of a particular activity. By contrast, standards should not define the exact techniques for reaching these goals. Too strict definitions are known to hinder creative developments, yet they should provide guidance (Aven and Ylönen 2019; Brunsson, Rasche and Seidl 2012; Timmermans and Epstein 2010). Rather effective guidelines already exist on how to select risk assessment techniques (ISO/IEC 2009; ISO/IEC 2019). Similar guidance should be provided for choosing between the different CIR assessment techniques.

The decision on which technique(s) to use for CIR assessment should be taken in relation to setting the scope, context and criteria. Any relevant technique could be used in principle, depending on the objectives, needs and requirements, level of ambiguity, information and data availability, and resources of the organization carrying out the assessment.

Moreover, it is essential that the results obtained from the risk analysis are transferable to the CIR assessment and vice versa. For instance, for CI, the risk analysis often reveals that there are vulnerabilities in the system due to tight couplings and interconnection between networks (Vespignani 2010), indicating that such systems should have the ability to bounce back from failures as well.

A technique should provide a transparent and repeatable work process, with results that are verifiable, and be applicable at least for organizational and technological CIR assessment. Appendix 1 presents some of the available techniques. To put these into a comparative perspective in the respective table (but not scoring them), we used certain attributes, aligned with the ISO 31000 practice (ISO/IEC 2009; ISO/IEC 2019), that should be considered, such as: *resources and capability*, for example the financial and staff resources that the organization has, or whether developed modeling and simulation approaches are needed (Banos et al. 2011; Mitra et al. 2009; Ouyang et al. 2012); *uncertainty*, related to data availability and quality (Francis and Bakera 2014; Aven 2011b); the *complexity* of the interdependent systems (Brown et al. 2004); and the ability of the technique to provide *quantitative output*. The latter is not necessarily a requirement, as qualitative approaches also can be used to assess the performance of a CI.

However, if one wants to measure the CI performance over time and compare the results, quantitative output is preferable.

4 OPERATIONALIZATION OF CIR MANAGEMENT

The operationalization of the above CIR management framework is illustrated below by applying one (of many possible) resilience assessment techniques, namely the Critical Infrastructure Resilience Index (CIRI) (Pursiainen et al. 2016). As a test case, we used one of the real-life systems from the pilot implementations, namely a potable water distribution system in the municipality of Barriero in Portugal. The operationalization was presented and validated in two Pilot Implementation Workshops (Appendix 2). Representatives of the current CI took part in the application of the CIRI technique, developing indicators and providing data and relevant information. However, as the real data provided by the operator in this particular 'test-case' is of a sensitive nature, the analysis presented here is entirety fictional, meaning that figures and numbers in the example are given random values for illustrative purposes.

The objective here is to illustrate the application and usability of the resilience assessment technique, not solely focusing on the output from the assessment itself. Hence, we believe using hypothetical values are justified, which has also been proven to be effective in other studies (Mostafa et al. 2014; Ibbs and Nguyen 2007). Notwithstanding the fictional data and the fictional potable water system, using the well-known Technological Readiness Level (TRL) scale in the form applied by the EU, this represents TRL 7 (of 9) validation, namely a system prototype demonstration in an operational environment.

A step-by-step process for operationalization of the CIR management framework is outlined in Figure 4.

<Fig. 4. [Approximately here]>

Each stage of the operationalization of the CIR management framework is briefly described below, focusing on the CIR assessment (analysis and evaluation). The applied assessment technique, CIRI, is briefly presented, with a more detailed description in Appendix 3.

4.1 Scope, criteria and context

Scope: The above-mentioned 'test case' is a potable water system in a municipality with a population of approximately 100,000 people. The potable water system consists of a number of ground-water intakes from a semi-confined aquifer, 9 reservoirs for treated water storage with the total capacity of 14.250 m^3, 13 licensed ground-water intakes, 8 treatment installations, 4 pumping stations, 7 blowers, 19.3 km of main ducts, and 349 km of meshed distribution pipes. The overall objective of the operator is to be better prepared for future disruptions, with respect to both the technical and the organizational domains, by integrating a CIR management approach with the existing risk management process. The 'operator'

below refers to a focus group, comprising representatives with insights into the current processes and techniques for risk assessment regarding the organization, as well as knowledge of the technical system.

Internal and external context: The internal context is obviously the municipal water operator organization itself, with its structures, procedures and internal relationships. In order to collect data and monitor the system's functions, the operator has a remote management system in place. The external context, in turn, is first of all the population that rely on this service. The external context also includes the (inter)dependencies among external actors, both private and public, such as electricity companies and emergency services.

Risk and resilience criteria: The operator decided to ascertain and measure CIR in a semi-quantitative way, combining the organizational and the technical domains, taking a holistic approach. Considering the organization's capacity and the available data, it was preferable to utilize existing indicators that had already been measured and recorded. Moreover, depending on the resilience assessment technique chosen, the evaluation should be carried out against a recommended initial minimum score. There are of course uncertainties related to such semi-quantitative approaches. However, of paramount importance in this case is finding a pragmatic way to measure resilience on some scale in order to improve the performance of the CI and its organization.

Select CIR assessment technique(s): Appropriate CIR assessment techniques were identified at this stage (as described in Appendix 1). Based on the above-described steps, the Critical Infrastructure Resilience Index (CIRI) (Pursiainen et al. 2016) was identified as a suitable technique in this particular case. While Appendix 3 explains this technique in detail, the main characteristics are outlined below.

CIRI integrates indicators from both the technological and organizational domains, and can therefore be considered a holistic resilience assessment technique. CIRI requires a moderate level of input from the operator and could be used as a self-assessment technique. As described in detail in Appendix 3, CIRI classifies indicators under seven crisis management cycle phases describing the temporal dimensions of resilience, referred to as resilience phases at Level 1 (Risk assessment, Prevention, Preparedness, Warning, Response, Recovery, and Learning), components and processes at Level 2, generic indicators at Level 3, and finally sector-specific and actually addressed indicators at Level 4. Thus, measuring Level 4 indicators first, the measurements accumulate upwards through a scaling process producing comparable results. This is carried out on a semi-quantitative maturity scale inspired by COBIT 4.1 (COBIT 2007), albeit with some applications so as to be able to apply the same scale to indicators in different domains. The scale is summarized in Table 1.

Table 1. Modified maturity scale

Score	Name
0	Non-existent: the indicator is not present or recognized in either the physical infrastructure or the managing organization.

1	Initial / ad hoc: there is awareness of the indicator, but the management of the process is informal and reactive; or the implementation of the technological feature is ad hoc and below standard.
2	Repeatable: the indicator is present, but there is no review of the process or the technological feature is not monitored.
3	Defined: responsibility for monitoring the process is defined, or the technological feature is monitored.
4	Managed: the process is routinely evaluated, or the technological feature is continuously monitored.
5	Optimized: the process is continuously re-evaluated, or the technological feature is subject to continuous monitoring and ongoing preventive maintenance if applicable.

The output from CIRI is either an overall resilience index, representing the accumulated resilience with a maturity scale value, or a breakdown of the maturity in the different phases. Since this is the first time a resilience assessment was conducted for the respective CI facility, and considering that there are no comparable data on record, the operator decided that it would suffice to select a baseline target maturity value, namely a minimum value of 3 for the Level 1 phases and Level 2 components and processes as a starting point. This represents a medium performance.

4.2 CIR assessment

Hazard identification: CIRI is generally hazard independent. However, some of the indicators can be developed based on a perceived vulnerability to a specific hazard. In the case of hazard dependency of the indicators, our chosen example was an earthquake, since this municipality is located on a seismic fault. This is a realistic scenario that may damage potable water supply networks. At this stage, it is also possible to include risks that are normally excluded after the risk identification process in a traditional risk assessment process. In other words, also accounting, to some extent, for possible surprises (or rather their consequences/impact) that have not been identified as risk scenarios.

Feed in information from the risk analysis: The risk analysis results indicate the likelihood of an unwanted event and the potential impact of such an event, also emphasizing the uncertainties in the results. Moreover, through the risk analysis new vulnerabilities in the system and organization could be revealed. This information is fed into the CIR assessment to provide better estimates of the absorptive, adaptive and restorative capacity of the CI (both technological and organizational).

CIR analysis: In the chosen 'test case', a set of indicators was developed for the CI. This was accomplished through a review of indicators for the functioning and vulnerability of the technical system, mainly technical and technological, also including indicators related to cyber. In addition, organizational indicators, found in the literature and relevant standards, were described. The indicators were evaluated according to their relevance and comprehensibility by the CI operator. To ensure objective, consistent, repeatable and representative results, the indicators were defined using unambiguous terms. As long as the

indicators are well described and leave little room for subjectivity, a high number of indicators does not prove to be a problem for the operator. Also, it was important for the operator that a well-defined measurement scale was present to assess the indicators. In the chosen test example, a total of 127 indicators were developed across the seven phases of the crisis management cycle. A total of 69 indicators were applicable to all sectors, and can be considered generic indicators. Fifty indicators were sector-specific to the water system, five indicators were cyber related, and three were related to electricity.

During a series of meetings, the operator's representatives score the indicators. After giving the applicable indicators a score from 0 to 5, the representatives had the opportunity to comment on the overall score to indicate where there was a misrepresentation of the results. The overall CIRI results for the example presented here with illustrative input values is 3.54. This score is further broken down into different resilience phases at Level 1, illustrated in Figure 5 along with the target maturity level 3 identified. Due to the sensitive nature of the actual data, the indicator score in Figure 5 and Figure 6 are fictional. The exact scoring procedure is explained in Appendix 3.

<Fig. 5 [Approximately here]>

CIR evaluation: Where the measured maturity is lower than the target, it represents an opportunity for improvement. The radar chart shows that the score is acceptable for Prevention, Preparedness, Warning, Recovery and Learning, where Recovery has the highest maturity. Risk Assessment and Response have non-satisfactory scores, just below 3. The Level 1 phases can be further broken down in this example into Level 2 components and processes.

Based on Figure 5 it is clear that the overall score and the score of most of the phases of the crisis management cycle exceed the target maturity level. However, the score for the components and processes at Level 2 (beneath those that exceed the target) might still be below the targeted maturity level.

4.3 Enhancement

Feed information from the CIR evaluation into the risk evaluation: The output from the CIR evaluation – in this case it could be a grade on a maturity scale – could be fed back into the risk evaluation process. When applying an acceptance level to evaluate CIR, the processes/areas of the infrastructure that do not reach the acceptance level could be seen as potential risks and should be included in the risk evaluation. The revealed deficiencies could be further analyzed using existing risk evaluation techniques, such as a cost-benefit analysis or the as low as reasonably practicable (ALARP) technique (Melchers 2001; Jones-Lee and Aven 2011a), investigating whether it would be beneficial to treat these processes/areas.

Develop and implement CIR enhancement plan: The final step is the CIR enhancement plan for improvement of the absorptive, adaptive and transformative capacity of the CI. Based on the scores, the components and processes at Level 2 are ranked according to the ratio of the Level 2 to the Level 1 score; hence, those components and processes with a low Level 2 score that contribute to one of the phases of the crisis management cycle with a low rank are prioritized in the enhancement plan. Those components and

processes at Level 2 (with its associated indicators at Level 3 and Level 4) which then have a score of less than the target are selected for enhancement.

The results of the CIRI calculation, assuming that enhancement results in those indicators in the plan achieve a maturity of 3, are shown in Figure 6. As can be seen, the enhancement plan results in a notable improvement in the results of the CIR evaluation. The new overall resilience score is 3.98, compared to the non-treated 3.54.

<Fig. 6. [Approximately here]>

5 DISCUSSION

The aforementioned case depicts how one could sketch a standardized and operational system for CIR management, using one particular technique. We are aware that this is not a definitive solution. The path toward an approved standard is long, bureaucratic and political, and the techniques, quite rightly, will always remain contested. While the ISO 31000 took years to agree on, and both the 2009 and 2018 editions were both commended and condemned (Aven 2011b; Leitch 2010, Purdy 2010; Lalonde and Boiral 2012; Aven and Ylönen 2019), the same is probably true of CIR management. Yet some serious efforts are being made to this end, both nationally and internationally, for instance at the European Union level, with several resilience projects and approaches joining forces (White Paper 2018).

Some basic principles of these efforts can be highlighted, one of which is *no duplicate practices*. Our experience within the networks in which the current scheme is developed (Appendix 2) clearly shows that CI operators and owners, mostly profit-seeking organizations, while having a self-interest in enhancing their CIR, do not want to change their systems overnight when the scientific discourse changes. The same principle of minimizing duplication is included, for instance, within the first of the 'seven tenets' of the US national regulation on CI (DHS 2013, p. 14). Yet the operators feel the societal pressure and are ready to adapt their practices. This delicate situation should be taken into account. Thus, any CIR management system should be accommodated to the operator's current risk management systems. The above CIR management framework satisfies this criterion.

Secondly, any workable CIR management system should be *tailorable*. No standard should be too rigidly defined. Indeed, the ISO 31000 risk management standard's fate proves this argument. The original version (ISO 2009) is by all accounts more detailed than the renewed one (ISO 2018b). It was simplified on demand. Ostensibly, sectors, companies or organizations do not need too well-defined and detailed frameworks, but they do need some kind of framework to tailor to their needs (Tranchard 2018). In a series of workshops related to the current article (Appendix 2), this was a common viewpoint shared by the CI operators. Hence, the proposed and illustrated CIR management framework was designed to facilitate this.

Thirdly, this is closely related to the idea that a *plurality of assessment techniques* is needed. There is no single technique that would provide all of the answers for all sectors, conditions, situations, needs or

resources for a risk or CIR assessment. While CIR assessment is still presented as something of a contest for the definitive all-encompassing technique (see Appendix 3), in risk assessment it is usually acknowledged that the exact technique should be chosen depending on the task at hand, particular hazards, and other limitations (ISO/IEC 2009; ISO/IEC 2019; Yoe 2012; Pritchard 2015; European Commission 2019).

Fourthly, any CIR management system should be based on *measurability*, that is, on well-defined and weighed-against-each-other indicators. Without measurable indicators, a CI operator would be in the dark about what and how much to enhance. Just as quantitative or semi-quantitative outcomes are preferred in risk assessment, when possible, in order to be useful for stakeholders (European Commission 2019, p. 20), CI operators likewise need quantified data for resilience enhancement.

Finally, CIR management is complex and calls for increased professional skills and resources. Technological interdependencies alone have become such that no group, let alone an individual, can analyze or manage them in their entirety. Yet CIR management should be characterized by relative *ease of use*, preferably computable. As CIR management is too important for any operator to subcontract, the system should be such that it is easy to integrate into the daily activities of the organizations concerned. Yet this also depends on the exact needs, purposes and resources of the operator when engaging in the CIR management process (Rød et al. 2017).

6 CONCLUSION

Focusing in particular on the organizational and technological domains, the current article has presented a way in which CIR can be conceptually and methodologically enhanced. Furthermore, it has shown how this could be achieved by utilizing the often-used practices of risk management, thus modifying the current international risk management standard toward that of CIR management. To this end, it presented a framework that closely follows the standardized risk management typology and terminology, but adapted it to CIR.

With the main emphasis being on CIR assessment rather than enhancement, this study has provided a shortlist of some of the most promising techniques in Appendix 1. It has also presented one assessment technique in some detail. In so doing, the study has nonetheless defended a pluralistic approach, emphasizing the need to adopt several techniques and develop them further.

As a general conclusion, the maxims for a successful CIR management system outlined in the Discussion section should be reiterated: no duplicate practices; tailorability and plurality of assessment techniques; measurability; and relative ease of use.

ACKNOWLEDGEMENTS

Some of the work presented in this article was carried out as a part of the IMPROVER project, which received funding from the European Union's Horizon 2020 research and innovation program under grant

agreement no. 653390. The contents of this article do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

Barreiro municipality is acknowledged for its valuable input and active participation in the operationalization process.

DATA AVAILABILITY

All data, models, or code generated or used during the study are available from the corresponding author on request.

REFERENCES

AIIC (Italian Association of Critical Infrastructures Experts). 2016. *Guidelines for Critical Infrastructures Resilience Evaluation*. Rome, Italy.

Aldrich, D. P., and M. A. Meyer. 2015. "Social capital and community resilience." *American behavioral scientist*, 59(2): 254-269.

ANL (Argonne National Laboratory). 2013. *Resilience measurement index: An indicator of critical infrastructure resilience*. Illinois, US.

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

Australian Government. n.d. "Organisational Resilience HealthCheck." Accessed October 23, 2019. http://www.organisationalresilience.gov.au/HealthCheck/Pages/default.aspx.

Aven, T. 2011a. "On some recent definitions and analysis frameworks for risk, vulnerability, and resilience." *Risk Analysis: An International Journal*, 31(4), 515-522.

Aven, T. 2011b. "On the new ISO guide on risk management terminology." *Reliability Engineering and System Safety*, 96 (7), 719-726.

Aven, T. 2016. "Risk assessment and risk management: Review of recent advances on their foundation." *European Journal of Operational Research*, 253 (1), 1-13.

Aven, T. 2019. "The Call for a Shift from Risk to Resilience: What Does it Mean?" *Risk Analysis*, 39(6), 1196-1203.

Aven, T. and M. Ylönen. 2019. "The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?" *Reliability Engineering and System Safety*, 189, 279-286.

Baños, R., J. Reca, J. Martínez, C. Gil, and A. L. Márquez. 2011. "Resilience indexes for water distribution network design: a performance analysis under demand uncertainty." *Water resources management*, 25(10), 2351-2366.

Barabadi, A., and Y. Ayele. 2018. "Post-disaster infrastructure recovery: Prediction of recovery rate using historical data." *Reliability Engineering & System Safety*, 169, 209-223.

Barker, K., J. E. Ramirez-Marquez, and C. M. Rocco. 2013. "Resilience-based network component importance measures." *Reliability Engineering & System Safety*, 117, pp. 89-97.

Basher, R. 2006. "Global early warning systems for natural hazards: systematic and people-centred. *Philosophical Transactions of the Royal Society*, 364, 2167-2182.

Boon, H. J., A. Cottrell, D. King, R. B. Stevensen, and J. Millar. 2012. "Bronfenbrenner's bioecological theory for modelling community resilience to natural disasters." *Natural Hazards*, 60(2), 381-408.

Brown, T., W. Beyeler, and D. Barton. 2004. "Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems." *International Journal of Critical Infrastructures*, 1(1), 108-117.

Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt. 2003. "A framework to quantitatively assess and enhance the seismic resilience of communities." *Earthquake spectra*, 19(4), 733-752.

Brunsson, N., Rasche, A., Seidl, D. 2012. "The dynamics of standardization: three perspectives on standards in organization studies." *Org Stud*, 33(5–6), 613-632.

Chang, S. E., and Shinozuka, M. 2004. "Measuring improvements in the disaster resilience of communities." *Earthquake spectra*, 20(3), 739-755.

Choi, J., N. Naderpajouh, D. J. Yu, and M. Hastak. 2019. "Capacity Building for an Infrastructure System in Case of Disaster Using the System's Associated Social and Technical Components." *J. Manage. Eng*. 35 (4): 04019013.

CIPedia. n.d.a. "Critical Infrastructure". Accessed 23 October, 2019. https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure.

CIPedia. n.d.b. "Resilience". Accessed 23 October, 2019. https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Resilience.

COBIT. 2007. *Excerpt. Executive Summary Framework.* United States of America: IT Governance Institute, http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cobit-4-1.aspx.

Cutter, S. L., L. Barnes, M. Berry, C. Burton, E. Evans, E. Tate, and J. Webb. 2008. "A place-based model for understanding community resilience to natural disasters." *Global Environmental Change* 18, 598-606.

Denzin, N. K. 2017. *The research act: A theoretical introduction to sociological methods.* New York, US: Routledge.

Dessavre, D. G., J. E. Ramirez-Marquez, and K. Barker. 2016. "Multidimensional approach to complex system resilience analysis." *Reliability Engineering & System Safety*, 149, May, 34-43.

DHS. 2013. *National Infrastructure Protection Plan. Partnering for Critical Infrastructure Security and Resilience*. US: Department of Homeland Security.

European Commission. 2018. *White Paper on Resilience Management Guidelines for Critical Infrastructures. From theory to practice by engaging end-users: concepts, interventions, tools and methods*. Prepared under the Research and Technological Development Crisis Management Topic 7 within European Commission Horizon 2020 Secure Societies Theme. [Online] Available at: http://www.humanist-vce.eu/fileadmin/contributeurs/humanist/white-paper.pdf.

European Commission. 2019. *Recommendations for National Risk Assessment for Disaster Risk Management in EU*. Science for Policy report by the Joint Research Centre (JRC). Luxembourg: Publications Office of the European Union.

European Council. 2008. *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Council Directive 2008/114/EC of 8 December 2008.

Flint, C. G., and A. E. Luloff. 2007. "Community Activeness in Response to Forest Disturbance in Alaska." *Society & Natural Resources*, 20(5), 431-450.

Francis, R., and B. Bekera. 2014. "A metric and frameworks for resilience analysis of engineered and infrastructure systems." *Reliability Engineering & System Safety*, 121, 90-103.

Gibson, C. A., and M. Tarrant. 2010. "A 'conceptual models' approach to organisational resilience." *Australian Journal of Emergency Management, The*, 25(2), 6-12.

Henry, D., and J. E. Ramirez-Marquez. "Generic metrics and quantitative approaches for system resilience as a function of time." *Reliability Engineering & System Safety*, 99, 114-122.

Holling, C. S. 1973. "Resilience and stability of ecological systems." *Annual review of ecology and systematics*, 4(1), 1-23.

Hollnagel, E. 2010. *How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG)*. Sustainable Transformation: Building a Resilient Organization. Toronto, Canada. http://www.organisationalresilience.gov.au/HealthCheck/Pages/default.aspx.

Hollnagel, E. 2017. *FRAM: the functional resonance analysis method: modelling complex socio-technical systems*. Boca Raton, US: CRC Press.

Hosseini, S., K. Barker, and J. E. Ramirez-Marquez. 2016. "A review of definitions and measures of system resilience." *Reliability Engineering & System Safety*, 145, 47-61.

HSSAI (Homeland Security Studies and Analysis Institute). 2009. *Concept Development: An Operational Framework for Resilience*. Arlington, VA.

Ibbs, W., and L. D. Nguyen. 2007. "Alternative for quantifying field-overhead damages." *Journal of Construction Engineering and Managemen*t. 133(10), 736-742.
Ilbeigi, M., and B. Dilkina. 2017. Statistical approach to quantifying the destructive impact of natural disasters on petroleum infrastructures. *Journal of Management in Engineering*, 34(1): 04017042.
IMPROVER Project. 2016. *Social resilience criteria for critical infrastructures during crises*. Project deliverable D4.1.
IMPROVER Project. 2017a. *Framework for implementation of resilience concepts to Critical Infrastructure*. Project Deliverable D5.1
IMPROVER Project. 2017b. *Operationalising organisational resilience to critical infrastructure*. Project deliverable D4.6.
IMPROVER Project. 2018. *Report of technological resilience concepts applied to living labs*. Project deliverable D3.3.
ISO (International Organization for Standardization). 2009a. *Risk management – Principles and guidelines. ISO 31000:2009*. Geneva, Switzerland.
ISO (International Organization for Standardization) 2009b. *Risk management – Vocabulary – Guidelines for use in standards. ISO Guide 73:2009*. Geneva, Switzerland.
ISO (International Organization for Standardization). 2011. *Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use*. ISO 280002:2011. Geneva, Switzerland.
ISO (International Organization for Standardization). 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*.ISO 28004-2:2014. Geneva, Switzerland.
ISO (International Organization for Standardization). 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*. Geneva, Switzerland.
ISO (International Organization for Standardization). 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*. Geneva, Switzerland.
ISO (International Organization for Standardization). 2015. *Quality management systems – Fundamentals and vocabulary. ISO 9000:2015*. Geneva, Switzerland.
ISO (International Organization for Standardization). 2018a. *Security and resilience – Vocabulary. ISO 22300:2018*. Geneva, Switzerland.
ISO (International Organization for Standardization). 2018b. *Risk management – Guidelines. ISO 31000:2018*. Geneva, Switzerland.
ISO/IEC (International Organization for Standardization / International Electrotechnical Commission). 2009. *Risk management – Risk assessment techniques. IEC/FDIS 31010*. Geneva, Switzerland.
ISO/IEC (International Organization for Standardization / Interantional Electrotechnical Commision). 2019. *Risk management - Risk Assessment techniqies*. IEC 31010:2019, Geneva, Switzerland.
Jones-Lee, M., and T. Aven. 2011. "ALARP – What does it really mean?." Reliability Engineering & System Safety, 96(8), 877-882.
Kahan, J. H., A. C. Allen, and J. K. George. 2009. "An operational framework for resilience." *Journal of Homeland Security and Emergency Management*, 6(1), 1-48.
Kimchi, J., B. Polivka, and J. S. Stevenson. 1991. "Triangulation: operational definitions." *Nursing research*, 40(6), 364-366.
Klein, R. J., T., R. Nicholls, and F. Thomall. 2003. "Resilience to natural hazards: How useful is this concept?" *Environmental Hazards*, 5, 35-45.
Kozine, I., and H. B. Andersen. 2015. "Integration of resilience capabilities for critical infrastructures into the emergency management set-up." In *Proc., European Safety and Reliability Conference 2015 European Safety and Reliability conference*. 171-176, CRC Press LLC.
Labaka, L., J. Hernantes, and J. M. Sarriegi. 2015. "Resilience framework for critical infrastructures: An empirical study in a nuclear plant." *Reliability Engineering & System Safety*, 141, 92-105.
Lalonde, C., and O. Boiral. 2012. "Managing risks through ISO 31000: A critical analysis." *Risk management*, 14(4), 272-300.

Lange, D., D. Honfi, M. Theocharidou, G. Giannopoulos, N. K. Reitan, and K. Storesund. 2017a."Incorporation of resilience assessment in Critical Infrastructure risk assessment frameworks." In *Proc., 27th European Safety and Reliability Conference, ESREL 2017,* 1031-1038, CRC Press/Balkema.

LEDDRA project. 2014. *Land & Ecosystem Degradation & Diversification: Assessing the Fit of Responses*. http://leddra.aegean.gr/index.htm.

Lee, A. V., Vargo, and E. Seville. 2013. "Developing a tool to measure and compare organizations' resilience." *Natural Hazards Review*, 14(1), 29-41.

Leitch, M. 2010. "ISO 31000: 2009 – The new international standard on risk management." *Risk Analysis: An International Journal*, 30(6), 887-892.

Levenberg, E., E. Miller-Hooks, A. Asadabadi, and R. Faturechi. 2016. "Resilience of networked infrastructure with evolving component conditions: pavement network application." *Journal of Computing in Civil Engineering*, 31(3): 04016060.

Linkov, I., D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H,... and T. P. Seager. 2013. "Measurable Resilience for Actionable Policy." *Environmental Science and Technology*, 47, 10108-10110.

Linkov, I., T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, and J. Nathwani. 2014. "Changing the resilience paradigm." *Nature Climate Change*, 4(6), 407-409.

Lounis, Z., and T. P. McAllister. 2016. "Risk-based decision making for sustainable and resilient infrastructure systems." *Journal of Structural Engineering*, 142(9): F4016005.

Luiijf, E., A. Nieuwenhuijs, M. Klaver, M. van Eeten, and E. Cruz. 2008. "Empirical findings on critical infrastructure dependencies in Europe." In *Proc., International Workshop on Critical Information Infrastructures Security*, 302-310, Springer, Berlin, Heidelberg.

McAslan, A. 2010. *Community Resilience. Understanding the Concept and its Applications*. Adelaide, Australia.

McDaniels, T., S. Chang, K. Peterson, J. Mikawoz, and D. Reed. 2007. "Empirical framework for characterizing infrastructure failure interdependencies." *Journal of Infrastructure Systems*, 13(3), 175-184.

McManus, S. T. 2008. *Organisational resilience in New Zealand*. Doctoral thesis, University of Canterbury, New Zealand.

Mitra, K., R. D. Gudi, S. C. Patwardhan, and G. Sardar. 2009. "Towards resilient supply chains: Uncertainty analysis using fuzzy mathematical programming." *Chemical Engineering Research and Design*, 87(7), 967-981.

Mostafa, M. A., and N. M. El-Gohary. 2014. "Stakeholder-sensitive social welfare-oriented benefit analysis for sustainable infrastructure project development." *Journal of Construction Engineering and Management*. 140(9), 04014038.

Nemeth, C. P., and I. Herrera. 2015. "Building change: Resilience Engineering after ten years." *Reliability Engineering & System Safety*, Volume 141, September, 1-4.

OECD (The Organisation for Economic Co-operation and Development). 2014. *Guidelines for resilience systems analysis*. OECD Publishing. Paris, France.

Ouyang, M., L. Dueñas-Osorio, and X. Min. 2012. A three-stage resilience analysis framework for urban infrastructure systems. *Structural safety*, 36, 23-31.

Rossman, G. B., and S.F. Rallis. 2011. *Learning in the field: An introduction to qualitative research*. California, US: Sage.

Panteli, M., P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou. (2017). "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems." *IEEE Transactions on Power Systems*, 32(6), 4732-4742.

Park, J., T. P. Seager, P. S. Rao, M. Convertino, and I. Linkov. 2013. Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, 33(3), 356-367.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. 2007. A design science research methodology for information systems research. *Journal of management information systems*, 24(3), 45-77.

Petersen, L., L. Fallou, P. Reilly, and E. Serafinelli. 2017. "European Expectations of Disaster Information provided by Critical Infrastructure Operators: Lessons from Portugal, France, Norway and

Sweden." *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 9(4), 23-48.
Petersen, L., E. Lundin, J. Sjöström, D. Lange, and R: Teixeira. 2018. "Creating comparable public tolerances and technical performance measures for critical infrastructure resilience evaluation". In *Proc., Safety and Reliability - Safe Societies in a Changing World*. 1231-1239, CRC press.
Petersen, L., Lange, D., and M. Theocharidou. 2019. "Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators". *Reliability Engineering and System Safety*, forthcoming.
Petit, F., Wallace, K., and Philips, J. 2014. *An Approach to Critical Infrastructure Resilience. The CIP Report*. Center for Infrastructure Protection and Homeland Security. Volume 12 Number 7, 17-20.
Pimm, S. L. 1984. "The complexity and stability of ecosystems." *Nature*, 307(5949), 321-326.
Prior, T. 2015. *Measuring Critical Infrastructure Resilience: Possible Indicators*. Risk and Resilience Report 9. ETH Zürich, Switzerland.
Pritchard, C.L. 2015. *Risk Management. Concepts and Guidance*. Boca Raton: CRC Press.
Purdy, G. 2010. "ISO 31000: 2009 – setting a new standard for risk management." *Risk Analysis: An International Journal*, 30(6), 881-886.
Pursiainen, C. 2009. "The challenges for European critical infrastructure protection." *European Integration*, 31(6), 721-739.
Pursiainen, C. 2017. *The Crisis Management Cycle: Theory and Practice*, Abingdon, Oxon, UK: Routledge.
Pursiainen, C. 2018. Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, Volume 27, pp. 632 - 641.
Pursiainen, C., and Gattinesi, P. 2014. *Towards testing critical infrastructure resilience*. JRC Scientific and Policy Reports. Ispra (VA), Italy.
Pursiainen, C. B. Rød, G. Baker, D. Honfi, and D. Lange. 2016. "Critical infrastructure resilience index." In *Proc., Risk, Reliability and Safety: Innovating Theory and Practice*, 2183-2189, CRC Press.
RESILIENS Project. 2016a. *Preliminary Resilience Maturity Model*. Project deliverable D2.6.
RESILIENS Project. 2016b. "Realising European Resilience for Critical Infrastructure." Accessed 23 October, 2019, http://resilens.eu/.
RESILIENS Project. 2016c. *Resilience Management Matrix and Audit Toolkit*. Project deliverable D2.3.
Righi, A. W., T. A. Saurin, and P. Wachs. 2015. "A systematic literature review of resilience engineering: Research areas and a research agenda proposal." *Reliability Engineering & System Safety*, 141, 142-152.
Rosenqvist, H., N. K. Reitan, L. Petersen, and D. Lange. 2018. "ISRA: Improver societal resilience analysis for critical infrastructure." In *Proc., Safety and Reliability-Safe Societies in a Changing World*, ESREL 2018, 1211-1220, CRC Press.
Rossman, G. B., and S. F. Rallis. 2011. Learning in the field: An introduction to qualitative research. Sage.
Rød, B., C. Pursiainen, G. Baker, D. Honfi, and D. Lange. 2017. "Evaluation of resilience assessment methodologies." In *Proc., Safety and Reliability – Theory and Applications*, edited by M. Cepin, and R. Briš, 1039-1051, CRC Press, Boca, Raton.
Rød, B., A. Barabadi, A. Z. Ayele, D. Lange, D. Honfi,and E. L. Droguett. "Probabilistic metric of infrastructure resilience considering time-dependent and time-independent covariates." In *Proc., Safety and Reliability – Theory and Applications*, edited by M. Cepin, and R. Briš, 1053-1060, CRC Press, Boca, Raton.
Sherrieb, K., F. H. Norris, and S. Galea. 2010. "Measuring Capacities for Community Resilience." *Soc Indic Res*, 99, 227-247.
Stephenson, A. 2011. *Benchmarking The Resilience In Organisations*. Doctoral Thesis. University of Canterbury, New Zealand.
Sterbenz, J. P., E. K. Çetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer. 2013. "Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation." *Telecommunication systems*, 52(2), 705-736.
Theocharidou, M., Galbusera, L., and Giannopoulos, G. 2018. Resilience of critical infrastructure systems: Policy, research projects and tools. In: *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems*, edited by B. D. Trump, M. V. Florin, and I. Linkov. Lausanne, CH: EPFL International Risk Governance Center. Available at: irgc.epfl.ch and irgc.org.

Timmermans, S., and Epstein, S. 2010. "A World of Standards but not a Standard World: Toward a Sociology of Standards and Standardization". *Annual Review of Sociology*, Vol. 36, 69-89.
Tranchard, S. 2018. "Risk management: The new ISO 31000 keeps risk management simple." *Governance Directions*, Vol. 70, No. 4, May, 180-182.
UNISDR (United Nations Office for Disaster Risk Reduction). 2017. *Words into Action Guidelines. National Disaster Risk Assessment*. Geneva, Switzerland.
UNISDR (United Nations Office for Disaster Risk Reduction). n.d. "Terminology on disaster risk reduction", Accessed 23 October, 2019. https://www.unisdr.org/we/inform/terminology.
Vespignani, A. 2010. "Complex networks: The fragility of interdependency." *Nature*, 464(7291), 984.
Vlacheas, P., V. Stavroulaki, P. Demestichas, S. Cadzow, D. Ikonomou, and S. Gorniak. 2013. "Towards end-to-end network resilience." *International Journal of Critical Infrastructure Protection*, 6(3-4), 159-178.
Wang, C. H., and J. M. Blackmore. 2009. "Resilience concepts for water resource systems." *Journal of Water Resources Planning and Management*, 135(6), 528-536.
Woods, D. 2015. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety,* Volume 141 – Sep 1, April, pp. 5-9.
Yoe, C. 2012. *Primer on risk analysis. Decision making under uncertainty*. Boca Raton: CRC Press.
Youn, B. D., C. Hu, and P. Wang. 2011. "Resilience-driven system design of complex engineered systems." *Journal of Mechanical Design*, 133(10): 101011.

TABLES

Table 2. CIR assessment techniques

Techniques		Resilience assessment process			Resilience domain		Relevance of influencing factors			Can provide quantitative output
Reference	Name	Resilience analysis	Level of resilience	Resilience evaluation	Org.	Tech	Resources and capability	Nature and degree of uncertainty	Complexity	
Pursiainen et al. 2016	Critical Infrastructure Resilience Index (CIRI)	SA	SA	A	SA	A	Medium	High	Medium	Semi
IMPROVER Project 2018; Petersen et al. 2018	IMPROVER Technical Resilience Analysis (ITRA)	SA	SA	SA	A	SA	High	Low	High	Yes
IMPROVER Project 2017b	IMPROVER Organizational Resilience Analysis (IORA)	A	NA	A	SA	NA	High	High	Medium	No
ANL 2013	Resilience Measurement Index	SA	SA	A	A	SA	High	Medium	High	Semi
AIIC 2016	Critical Infrastructure Resilience Evaluation	SA	SA	A	SA	SA	High	High	High	Semi
Lee et al. 2013	Benchmark Resilience Tool (BRT)	SA	A	A	SA	NA	Low	High	Medium	Semi
Australian Government n.d. [Online]	Organizational Resilience Health Check (ORHC)	SA	A	A	SA	NA	Low	High	Medium	Semi
Hollnagel et al. 2010	Resilience Analysis Grid (RAG)	SA	A	A	SA	NA	Low	High	Medium	No
OECD 2014	OECD Guidelines for Resilience System Analysis	SA	SA	A	SA	SA	High	Medium	High	Semi
RESILIENS Project 2016c.	Resilience Management and Matrix Toolkit	SA	A	A	SA	SA	High	High	High	Semi
RESILIENS Project 2016b.	Resilience Maturity Model tool	SA	A	NA	SA	NA	High	High	Medium	No
Hollnagel 2017	The “Fram”	A	NA	NA	SA	NA	Medium	High	Medium	No

SA=Strongly applicable, NA=Not applicable, A=Applicable. Relevance of influencing factors: Low, medium and high

Table 3. List of workshops arranged in association with the IMPROVER project

Date and location	Type of workshop	Topic	Participants
September 25, 2015, Copenhagen, Denmark	Associate partners Workshop I	The definition of resilience and resilience in critical infrastructure	35 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academicians
April 27-28, 2016, Ispra, Italy	Operators Workshop I	Organizational resilience of CI operators, resilience indicators of CI operators, and community resilience	50 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
October 13, 2016, Paris, France	Associate partners Workshop II	How critical infrastructure can meet public expectations in response to a crisis	39 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academicians
May 11-12, 2017, Ispra, Italy	Operators Workshop II	Organizational and community resilience	54 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
September 21, 2017, London, UK	Associate partners Workshop III	Usability and success criteria for the CIR management framework	35 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academicians
January 30-31, 2018, Lisbon, Portugal	Pilot Implementation Workshop I	Implementation, testing and evaluation of the resilience management framework in a semi-real environment (Water Distribution System)	~30 participants: CI operators, local governmental services, associated partners and researchers
May 23-24, 2018, Lisbon, Portugal	Operators Workshop III	Resilience Assessment for Critical Infrastructures: Methods and Tools (Day 1), and Resilience Enhancement for critical infrastructures: Guidelines and Standards (Day 2)	51 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
May 29-30, 2018, Budapest, Hungary	Pilot Implementation Workshop II	Implementation, testing and evaluation of the resilience management framework in a semi-real environment (M1 Highway, Budapest)	~25 participants: CI operators, local governmental services, associated partners and researchers

APPENDIX 1: CIR ASSESSMENT TECHNIQUES

This Appendix, informed by the IEC 31010 *Risk Management – Risk Assessment Techniques* (ISO/IEC 2009; ISO/IEC 2019), presents the main available assessment techniques proposed for organizational and technological CIR assessment. To put these into a comparative perspective, we have evaluated their applicability according to five selected attributes: resources and capability needed; nature and degree of uncertainty; complexity; the ability to provide quantitative output; and two resilience domains, namely organizational and technological.

<Table 2. [Approximately here] >

APPENDIX 2: THE METHODOLOGICAL WORKSHOPS

Table 3 delineates the workshop process with a large number of stakeholders, leading to the negotiated result of the CIR management scheme and its respective operationalization.

<Table 3. [Approximately here]>

APPENDIX 3: CRITICAL INFRASTRUCTURE RESILIENCE INDEX

CIRI is a semi-qualitative index resilience assessment technique inspired by the crisis management cycle (Pursiainen 2017). Since CIRI was introduced in 2016, it has been further developed through demonstrations and evaluations, receiving valuable feedback from several focus groups (including CI operators), using the design research methodology (Peffers et al. 2004).

Structure

CIRI breaks resilience down into seven different phases – risk assessment, prevention, preparedness, warning, response, recovery, and learning – describing the temporal dimensions of resilience, referred to as resilience phases at Level 1 in the hierarchical structure. Each resilience phase is broken down into processes and components, referred to as Level 2, which are further broken down into generic indicators at Level 3. How these are measured will depend on the sector, and thus, sector-specific indicator cards at Level 4 have to be developed, where a Level 3 indicator might have one or several indicator cards, depending on the sector. Figure 7 illustrates the CIRI structure.

<Fig. 7. [Approximately here]>

Level 4 indicators are transformed into a semi-quantitative scale, ranging from 0 to 5 (COBIT 2007) (see Table 1). After assessing the Level 4 indicators, results are aggregated up the hierarchy, and the generic indicators (Level 3), components and processes (Level 2), and resilience phases (Level 1) receive a score from 0 to 5.

Calculation algorithm

Let us assume that we have conducted our measurements and evaluations at Level 4. We then begin by aggregating all the Level 4 information to obtain a score for all the Level 3 indicators, following, for instance, a maturity scale like the one presented in Table 1. Note that the data may have to be weighed according to sector to obtain 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:

$$L2\ component\ or\ process = \frac{1}{\sum_{i=1}^{m} w_i} \sum_{i=1}^{m} w_i\ \ L3\ indicator_i \quad (1)$$

where m is the number of Level 3 indicators and w_i represent the weighting coefficient. Further, the seven Level 1 indicators are estimated as:

$$L1\ phase = \frac{1}{\sum_{i=1}^{n} v_i} \sum_{i=1}^{n} v_i\ \ L2\ (component\ or\ process)_i \quad (2)$$

where n is the number of Level 2 indicators and v_i represent the weighting coefficient. In order to produce a final resilience index, the seven Level 1 indicators are aggregated into one score:

$$CIRI = \frac{1}{7} \sum_{i=1}^{7} L1\ phase_i \quad (3)$$

Indicator cards and work process

In order to address the need for proper descriptions and definitions of sector-specific indicators, indicator cards have been developed for the technological and organizational resilience indicators at the lower CIRI level (Level 4). Each individual resilience indicator card provides a detailed description of the sector-specific indicator subject to assessment. The cards consist of the following information:

- A list of the assessed indicator and its parent indicators.
- Detailed information about the context. The resilience domain (technological or organizational), hazard types (natural, non-malicious man-made, malicious man-made and multi-hazards) and

situational factors (e.g. temporal, geographical or conceptual considerations for taking such an indicator into account) are indicated. Information about the societal resilience domain, such as regulative limits or public tolerance toward CI disturbances (if available) can be added. Lastly, the applicable sector is highlighted and whether the indicator is generic or scenario-specific.

- A description of the indicator and guidance for assessing the maturity level is provided, including a rationale for the indicator. Moreover, a question is provided, which the operator can be asked for the purpose of measuring the indicators in a clear and explicit manner with the six different maturity levels described (on a scale of 0–5) and a reference for describing the indicator.

In order to obtain a transparent and replicable process, it is important to have clear guidelines describing the working methodology. The main steps are described below:

1. Establishing the context.
2. Identification, development, and population of an initial set of indicators (Level 3 and Level 4).
3. Ranking the indicators according to how well they are understood and perceived by the operator.
4. Development of sector-specific indicator cards.
5. Analyzing the indicators and completing the analysis.
6. Review and discussion with the operator.
7. Identification of missing or out-of-context cards.
8. Evaluation and review of the final analysis results (for a further CIR enhancement plan).

If missing or out-of-context information is identified in Step 7, then the process is restarted at Step 4. This process can then be considered iterative.

The overall CIRI, combining all of the Level 1 phases, is, as previously described, calculated based on the three lower levels of indicators by simple aggregation. It is up to the operator whether or not to adopt this approach, or to choose to concentrate on one phase, process, component, or indicator at a time, which might be more informative in terms of identifying the gaps in resilience. The technique allows for concentrating on only partial challenges, such as measuring only two components (e.g. resilient design and recoverability at Level 2, with their Level 3 sub-indicators). The main advantage is that it enables the measurement of several indicators and transforms them into one metric, thereby making it possible to define the aggregated level of resilience on the scale of 0–5.