# CRITICAL INFRASTRUCTURE RESILIENCE: BRIDGING THE GAP BETWEEN MEASURING AND GOVERNANCE

Hanneke Duijnhoven[1], Albert Nieuwenhuijs[2], Puck van den Brink[3], Dirk Stolk[4] and Theo van Ruijven[5]
1 TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
1 hanneke.duijnhoven@tno.nl, +31(0)88662929
2 TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
2 albert.nieuwenhuijs@tno.nl
3 TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
3 puck.vandenbrink@tno.nl
4 TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
4 dirk.stolk@tno.nl
5 TNO, Research Group Networked Organisations, Lange Kleiweg 137 2288 GJ Rijswijk, The Netherlands
5 theo.vanruijven@tno.nl

**Abstract**

In this paper we seek to explore the challenges regarding governance of critical infrastructure resilience by reviewing the current application of the resilience concept in the domain of critical infrastructure. We broadly discuss the most common categories of approaches towards resilience assessment of critical infrastructure resilience that are currently adopted: performance-based and attribute-based approaches. We then address differences in conceptualization and operationalization of (critical infrastructure) resilience and discuss the implications of these different approaches with regard to their scientific underpinnings and their practical applicability for the field of critical infrastructure governance. This discussion highlights important limitations of these approaches, leading us to argue that a Resilience Engineering perspective may address some of the shortcomings of the performance-based and attribute based approaches. At the same time, the Resilience Engineering work as it stands also has some important limitations (lack of empirical evidence and practical application, as well as insufficient attention for resilience challenges within a multilevel, multi-stakeholder, network-of-networks context.

## 1. Governance of Critical Infrastructure Resilience

There are many definitions of critical infrastructure and the assessment of what the critical infrastructure for a specific society consist of varies between countries. Nevertheless, in general, critical infrastructures are seen as those products, services and underlying processes that, should they fail, have the potential of causing serious societal disruptions, for instance by causing a large number of casualties, extensive economic damages or because there are no realistic alternatives available for products or services that are essential for the continuity of normal societal functions. What makes these infrastructures even more critical is that, together, they form a complex network of processes that are highly interconnected. Failures in one part of the network can cause problems in other parts of the network, potentially causing cascading impact across society that is difficult to predict.

The last decades have witnessed a widespread attention to critical infrastructure protection (and more recently resilience) across nations worldwide. Policies and legislation has emerged in many countries, as well as in the European Union, aimed at cross-border cooperation (Alcaraz & Zeadally, 2015; Klaver et al., 2008; Luiijf, Nieuwenhuijs, Klaver, van Eeten, & Cruz, 2008). In the Netherlands, the first criticality assessment to determine the critical infrastructure for Dutch society took place in 2002. Since then there have been several updates, but all following the same initial structure. In 2014 a new approach for the criticality assessment has been introduced, resulting in a new list of critical infrastructures. Whereas previously the critical infrastructures were listed in sectors and related products and services, the new approach identifies critical processes that deliver those products and services (Hamelink & Mutsaers, 2015). The assessment has been done using a range of different criteria related to the impact (physical, economic, social) of failure on society and the extent to which other processes are critically dependent on a particular process (Schoof, 2015).

As a result of the reassessment a list of processes is defined that constitute the critical infrastructure in The Netherlands. The list distinguishes between two categories of criticality (category A and category B), which has policy implications for the public and private organizations that are involved in operating and maintaining these processes. Moreover, with the reassessment, the orientation for policy is expanding from protecting critical infrastructure towards increasing the resilience of critical infrastructure (Hamelink & Mutsaers, 2015). Given the nature of the domain, with a large number of actors involved and complex networks of dependencies, increasing resilience is not something that is easily achieved. As of yet, there are no adequate governance models to address critical infrastructure resilience enhancement (Bach et al., 2013). In fact, one of the main challenges for the governance of critical infrastructures is the large, varied network of public and private stakeholders involved in combination with the connectivity, complexity and dependencies within the network of infrastructure systems.

### 1.1. Aim and Outline of the Paper

Given this background, this paper explores the current state-of-the-art of resilience approaches in the critical infrastructure domain in order to specify the gaps that remain. We do not intend to do a meta-analysis of resilience approaches, since there are abundant efforts in that direction. After briefly discussing the shift from CI protection to CI resilience, we will broadly discuss the most common categories of approaches towards resilience assessment of critical infrastructure resilience that are currently adopted: performance-based and attribute-based approaches. We then address differences in conceptualization and operationalization of (critical infrastructure) resilience and discuss the implications of these different approaches with regard to their scientific underpinnings and their practical applicability for the field of critical infrastructure governance. Following this analysis, we argue that a Resilience Engineering perspective may address some of the shortcomings of the performance-based and attribute based approaches, although there are still some important gaps or challenges in adopting such a perspective.

## 2. The Transition Towards Resilience in the Field of Critical Infrastructure

The field of Critical Infrastructure research has traditionally focused on the protection and reliability of infrastructure systems in light of different causes of disturbances (threats). Recently, a shift can be observed from a focus on the protection of critical infrastructures towards a focus on critical infrastructure resilience (Alsubaie, Alutaibi, & Martí, 2015). Risk management has been a dominant orientation and is used to identify potential sources of disturbances, the potential impact of these disturbances and ways to prevent or minimize negative consequences. The increasing complexity of infrastructure systems, their increasing connectivity and network dependencies (partly due to increasing digitalization) make it impractical and perhaps even impossible to assess all risks and take protective measures accordingly (Vugrin, 2016). In addition to this, the threat landscape is also changing, with fast-moving developments such as cyber threats, geopolitical developments and technological innovation, making it ever more difficult to continue with traditional risk management approaches. Thus, it is increasingly recognized that we live in an age of uncertainty and unexpected events will always occur, so it makes sense to focus on being able to deal with unexpected situations rather than trying to prepare for every possible situation (Weick & Sutcliffe, 2007). Hollnagel argues that instead of focusing on all possible things that can go wrong it is important to focus on understanding and increasing “the ability to succeed under varying conditions, so that the number of intended and acceptable outcomes (in other words, everyday activities) is as high as possible”(2013: 8). Resilience has been widely embraced as a promising concept that embodies this shift in orientation (Duijnhoven and Neef 2014; Woods and Hollnagel 2006).

The shift towards resilience thinking is seen across a wide variety of disciplines, with many different conceptualizations and applications of ‘resilience thinking’ as a result. Originating from the field of systems ecology, the wide adoption of resilience is mostly attributed to the work of Holling (1973). From there, the concept, as a “science of complex adaptive systems and an operational strategy of risk management” (Walker & Cooper, 2011: 143) has gained traction in fields such as safety management, disaster management, systems engineering, and natural resource management (Van Ruijven, 2016). Application extends to domains such as climate resilience (resilience of ecological systems against climate change), community resilience (resilience of communities against a wide range of crises), organizational resilience (business continuity in the face of internal and external pressures), cyber resilience (resilience of {digital} systems against cyber threats), and critical infrastructure resilience (resilience of critical infrastructures against disturbances). Between (or even within) all these different approaches, there is no consensus with regard to the definition and

operationalization of resilience. In fact, as Woods (2015) argues, in many studies it is unclearly stated how the concept is used and why. This is problematic as it may stall progress in the field.

## 3. Current Approaches towards Critical Infrastructure Resilience

Definitions of critical infrastructure resilience vary and are usually inspired by the use of the term resilience in other disciplines (Alsubaie et al., 2015; Bach, Bouchon, Fekete, Birkmann, & Serre, 2013). An often cited definition in the field is that from the US National Infrastructure Advisory Council (NIAC): "*the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event*" (2009). Definitions aside, the actual conceptualization of resilience is generally related to the reliability and robustness of the system.

When it comes to resilience analysis, several distinguishing approaches can be identified across the domain of critical infrastructures. Following the classification of resilience assessment approaches in structural, performance-based and hybrid approaches (Biringer et al. (2013) in Alsubaie et al., 2015: 45), Alsubaie et al. present a literature review of 19 approaches towards CI resilience. The majority of approaches (12) can be classified as performance-based approaches. These attempt to "evaluate the system resilience by measuring its performance before and after a disruption" (Alsubaie et al., 2015: 45). Four approaches are classified as structural approaches, meaning that they "use the structure or topology of the system to evaluate its resilience" (Alsubaie et al., 2015: 45). Three approaches are classified as 'hybrid', using a combination of structural and performance-based assessment.

Similarly, Vugrin (2016) distinguishes between two broad categories of instruments for critical infrastructure resilience assessment. At one end of the spectrum there is a group of approaches that aim to identify properties or characteristics of a system that contribute to its resilience. There is no widely accepted list of resilience attributes, but they often include attributes such as robustness, redundancy, resourcefulness, adaptability. These attribute-based approaches usually involve a qualitative (or semi-quantitative) assessment of the degree to which the system demonstrates such attributes. According to Vugrin, the benefit of this type of approach is that it is less time- or resource intensive. These approaches, however cannot really predict how resilient the system will be for future (unknown) disruptions and rely heavily on qualitative, subjective assessments. Often, these approaches have a practical orientation and are meant to be used by infrastructure operators and governmental agents to assess the resilience of the systems under their responsibility. Examples are the critical infrastructure resilience index as developed by Argonne National Laboratory (Fisher et al., 2010), approaches developed in European Horizon 2020 projects such as RESILENS[1] and IMPROVER[2], or the approach developed by the Australian government[3] to support organizations (including critical infrastructure operators) in assessing their own resilience. The conceptualization of resilience underlying these approaches is often not explicitly stated or theoretically elaborated.

At the other end of the spectrum there are performance-based approaches that aim to quantitatively measure the degree of resilience of a system by measuring the performance level of the system in case of a specified disruption (Vugrin, 2016). Often, resilience is then presented as a "time dependent ratio of recovery over loss" (Barker, Ramirez-Marquez, & Rocco, 2013). According to Vugrin, a benefit of such approaches is that they are more useful for comparative analyses (bench-marks) because they rely less on qualitative, subjective assessment. Limitations are that such approaches usually require a vast amount of data and complex (computational) modelling which is generally more time- and resource intensive. In addition, the outcome of this type of resilience assessment does not offer much explanatory information about why the system is more or less resilient. The complex models require a lot of knowledge about a system, but the actual calculation of resilience is a black box that does not contribute to a better *understanding* of resilience. This type of approaches has a strong scientific orientation and therefore it seems to be the dominant approach in the scientific literature on critical infrastructure resilience. The scientific orientation and high requirements in terms of data and expertise generally makes these approaches less suitable for practical application in an operational context. Often-cited examples are those by Henry and Ramirez-Marquez (2012), Barker et al. (2013), Filippini and Silva (2014), Francis and Bekera (2014), and Ouyang et al. (2014; 2012; 2015). Both ends of the spectrum offer benefits and limitations, and it is tempting to combine the strengths into hybrid

[1] http://resilens.eu/resilens-outputs/

[2] http://improverproject.eu/category/results/

[3] http://www.organisationalresilience.gov.au/HealthCheck/Pages/default

approaches. However, when taking a closer look at the existing approaches, it becomes clear that many of them are not fully embracing all the concept of resilience has to offer. We argue that the critical infrastructure field could benefit from some of the progress that has been made within the Resilience Engineering field, in particular with regard to the conceptualization of resilience. In the next section we will briefly introduce the Resilience Engineering perspective and argue why this would be a useful lens in the field of critical infrastructures.

## 4. Adopting a Resilience Engineering Perspective

A resilience perspective focuses on how a system performs its/several functions and in what ways it can resist, absorb, respond, or adapt to disturbances. As such it is a fundamentally different mindset than what is common in traditional risk management methods, and it requires different methodological approaches (Vugrin, 2016). Whereas risk assessment has an external orientation, focusing on a set of specific threats that a system may be exposed to, resilience analysis focuses on the dynamic, internal mechanisms that make a system operate and contribute to stable delivery of its products or services. As such, it moves away from anticipation towards "more inclusive strategies that integrate both resistance (prevent, protect) and resilience (respond, recover)" (Longstaff, Armstrong, Perrin, May, & Parker, 2010).

When it comes to resilience analysis, there are many different approaches, with different underlying conceptualizations of what resilience of complex (socio-technical) systems is and how it can be analyzed (Nemeth & Herrera, 2015). Woods (2015), recognizes four basic conceptualizations of resilience that are applied to complex adaptive systems:

1. resilience as the ability to rebound from trauma and return to equilibrium;
2. resilience as a synonym for robustness;
3. resilience as the opposite of brittleness, i.e., as graceful extensibility when surprise challenges boundaries;
4. resilience as network architectures that can sustain the ability to adapt to future surprises as conditions evolve.

These four conceptualizations are a testament to the evolution of resilience thinking as the field progresses. The first and second conceptualizations stem from earlier stages of resilience research, although they still prevail in many studies. These two interpretation are rather limited and do not fully embrace the essential notions of the resilience concept as offering an alternative perspective to address the complex, non-linear, stochastic nature of technological systems (Hollnagel, 2006; Woods, 2015).

The third and fourth conceptualizations show the advances in resilience thinking and introduce new concepts such as 'brittleness' and 'sustained adaptability' into the perspective (Woods, 2015). The third conceptualization is where, according to Woods, the state of the art of resilience engineering currently stands. This perspective focuses on "how a system extends performance, or brings extra adaptive capacity to bear, when surprise events challenge its boundaries"(Woods, 2015: 5). The fourth conceptualization is where the field should be progressing towards (Woods, 2015). This conceptualization aims to identify what architectural properties contribute to the capacity of systems to continue adapting to surprises under dynamic and evolving conditions. This means that we need to understand more about what resilience looks like in practice, or more specifically it is necessary to observe empirical instances of adaptability in operational contexts (Nemeth & Herrera, 2015; Woods, 2015). An additional question, that is currently underemphasized within the Resilience Engineering community, would be how to operationalize this conceptualization in the context of dependent networks of a range of different critical infrastructures, with multiple stakeholders and often different or even competing interests. These systems tend to have a long history and many of its properties and characteristics have developed and emerged over a long time (for instance due to technological progress and processes urbanization). The notion of architectural properties seems relevant, but suggests the possibility to deliberately 'design' (engineer) systems. The question is to what extend this is possible in existing infrastructures, and if so, who the designer/engineer is (who can decide)?

In terms of these four conceptualizations that Woods (2015) distinguishes, most of the performance-based approaches and attribute-based approaches that are currently being developed in the field of critical infrastructure resilience seem to come close to the second conceptualization, although often this is not clearly specified. In fact, as Bach et al. argue, (Bach et al., 2013) it seems that the use of the concept of resilience in the field of critical infrastructures is not very well developed yet and the field could benefit from adopting insights from other fields that are further developed in resilience thinking. Precisely because of the *criticality* of

critical infrastructures for society, it is important to come up with effective resilience assessment approaches that utilize the multidisciplinary scientific knowledge for practical, operational applications. The third and fourth conceptualization that Woods describes may provide a good starting point, although it is necessary to further develop these idea to also address the specific challenges of a multi-stakeholder, multi-level, network of networks context such as the field of critical infrastructures.

## 5. Conclusion

The dominant approaches to resilience (as discussed in previous sections) have a rather narrow interpretation of resilience, for instance as the ratio of loss and recovery in the face of a disturbance. The performance-based approaches do not provide pointers for governance of resilience. Other approaches provide lists of attributes of resilience that can give direction as to what type of capacities a system should strive for, but these are rather subjective and do not guarantee that it constitutes sustainable capacity in changing circumstances. What is more, most of these approaches are targeting single organizations or infrastructure systems, while from a governance perspective it is relevant to address resilience at the level of the network or even at the societal level. The conceptualizations of resilience as developed within the Resilience Engineering community offer part of the solution since it is concerned with opening up the 'black-box' of complex systems and understanding where its boundaries are and what the adaptive capacity constitutes (providing concrete insights to decision-makers about how to enhance resilience). It specifically aims to gain an understanding of how to achieve sustained adaptability, yet, until now there are few studies that provide empirical evidence of these conceptualizations. What is more, the literature in the Resilience Engineering community tends to focus on relatively closed systems and it does not explicitly address resilience of networks of systems at a society or intersectoral level. For the challenges in the field of critical infrastructure resilience, a successful approach should address the mutual dependencies and connections between different critical infrastructures. "Rather than focusing on the protection of certain facilities, the safeguarding of the provision of services should be the primary aim" (Bach et al., 2013). This, defining critical processes rather than critical infrastructures, as recently introduced in Dutch policy context, may offer a better starting point to assess the performance and strength of resilience attributes at the level of network-of-networks. But in order to understand how to build more sustainable resilience into these systems requires an approach that explicitly addresses this type of complex context.

## 6. References


Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66. https://doi.org/http://dx.doi.org/10.1016/j.ijcip.2014.12.002

Alsubaie, A., Alutaibi, K., & Martí, J. (2015). Resilience Assessment of Interdependent Critical Infrastructure. In *International Conference on Critical Information Infrastructures Security* (pp. 43–55). Springer.

Bach, C., Bouchon, S., Fekete, A., Birkmann, J., & Serre, D. (2013). Adding value to critical infrastructure research and disaster risk management: the resilience concept. *SAPI EN.S.Surveys and Perspectives Integrating Environment and Society*, (6.1).

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability Engineering & System Safety*, *117*, 89–97. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.03.012

Duijnhoven, H., & Neef, M. (2014). Framing Resilience. From a Model-based Approach to a Management Process. *Procedia Economics and Finance*, *18*(September), 425–430. https://doi.org/10.1016/S2212-5671(14)00959-9

Filippini, R., & Silva, A. (2014). A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. *Reliability Engineering & System Safety*, *125*, 82–91.

Fisher, R. E., Bassett, G. W., Buehring, W. A., Collins, M. J., Dickinson, D. C., Eaton, L. K., … Lawlor, M. A. (2010). *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program.*

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, *121*, 90–103. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.07.004

Hamelink, S., & Mutsaers, J. (2015). Critical Infrastructure Protection: From Protection to Resilience. *European CIIP Newsletter*, *9*(3), 21–23.

Henry, D., & Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety*, *99*, 114–122. https://doi.org/http://dx.doi.org/10.1016/j.ress.2011.09.002

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 1–23.

Hollnagel, E. (2006). Resilience - the Challenge of the Unstable. In E. Hollnagel, D. Woods, & N. Leveson (Eds.) (pp. 9–17). Aldershot: Ashgate.

Hollnagel, E. (2013). A tale of two safeties. *Nuclear Safety and Simulation*, *4*(1), 1–9.

Klaver, M. H. A., Luiijf, H. A. M., Nieuwenhuijs, A. H., Cavenne, F., Ulisse, A., & Bridegeman, G. (2008). European risk assessment methodology for critical infrastructures. In *Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), 2008 First International Conference on* (pp. 1–5). IEEE.

Longstaff, P. H., Armstrong, N. J., Perrin, K., May, W., & Parker, M. A. H. (2010). Building Resilient Communities: A Preliminary Framework for Assessment. *HOMELAND SECURITY AFFAIRS*, *6*(3).

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., & Cruz, E. (2008). Empirical findings on critical infrastructure dependencies in Europe. In *International Workshop on Critical Information Infrastructures Security* (pp. 302–310). Springer.

National Infrastructure Advisory Council. (2009). *Critical Infrastructure Resilience: Final Report and Recommendations*. US: National Infrastructure Advisory Council.

Nemeth, C. P., & Herrera, I. (2015). Building change: Resilience Engineering after ten years. *Reliability Engineering & System Safety*, *141*, 1–4. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.04.006

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.06.040

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety*, *36–37*, 23–31. https://doi.org/http://dx.doi.org/10.1016/j.strusafe.2011.12.004

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety*, *141*, 74–82. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.03.011

Schoof, D. (2015). Wat is vitaal? *Magazine Nationale Veiligheid En Crisisbeheersing*.

Van Ruijven, T. (2016). *Multidisciplinary Emergency Management. A comparative study of coordination and performance of on-scene command teams in virtual reality exercises*. Delft: Delft University of Technology.

Vugrin, E. D. (2016). Critical Infrastructure Resilience. In IRGC (Ed.) (v. 29-07-20). Lausanne: EPFL International Risk Governance Center.

Weick, K., & Sutcliffe, K. (2007). *Managing the unexpected: resilient performance in an age of uncertainty*. John Wiley & Sons, Inc.

Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5–9. https://doi.org/http://dx.doi.org/10.1016/j.ress.2015.03.018

Woods, D., & Hollnagel, E. (2006). Prologue: Resilience Engineering Concepts. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.) (pp. 1–16). Aldershot, UK: Ashgate Publishing Limited.