Designing Dynamic Stress Tests For Improved Critical Infrastructure Resilience

Tina Comes
University of Agder
martina.comes@uia.no

Valentin Bertsch
Karlsruhe Institute of Technology
valentin.bertsch@kit.edu

Simon French
University of Warwick
simon.french@warwick.ac.uk

ABSTRACT

This paper outlines an approach to support decision-makers in designing resilient critical infrastructure (CI) networks. As CIs have become increasingly interdependent disruptions can have far-reaching impacts. We focus on the vulnerability of CIs and the socio-economic systems, in which they are embedded, independent from any initial risk event. To determine which disruptions are the most severe and must be avoided, quantitative and qualitative assessments of a disruption's consequences and the perspectives of multiple stakeholders need to be integrated. To this end, we combine the results of consequence models and expert assessments into stress test scenarios, which are evaluated using multi-criteria decision analysis techniques. This approach enables dynamic adaption of the stress tests in the face of a fast changing environment and to take account of better information about interdependencies or changing preferences. This approach helps make trade-offs between costs for resilient CIs and potential losses of disruptions clearly apparent.

Keywords

Critical infrastructure disruption, robustness, resilience, participatory approaches, stress test, vulnerability, MCDA

INTRODUCTION

Modern societies increasingly depend on critical infrastructures (CIs) (Trucco et al., 2011). CIs encompass physical infrastructures (power plants, road networks, or hospitals) and services that are provided via these infrastructures (electricity supply, transportation of passengers or goods, or health care). While (technical) infrastructures can be defined as complex networks that evolve over time (Star and Ruhleder, 1996; Hanseth, 2010), there is no unanimous definition of which infrastructures are critical and how this criticality is defined (Haemmerli and Renda, 2010). For instance, definitions of CIs vary considerably between the U.S. and Europe (Giannopulos et al., 2012). Despite the diversity of definitions, they all have in common that CIs are defined by their role for society (Rinaldi et al., 2001; Min et al., 2007): they support the services that are vital for life and sustainable economic growth. The definition of CIs therefore depends on what is perceived as essential, and definitions vary with context, risk perception and political and societal goals (Moteff et al., 2003). Consider, for instance, ICT systems: along with their rise over the last decades, their importance has been continuously increasing, and today, they are among the most prominent CIs (Haemmerli and Renda, 2010).

Another important trend is the growing complexity and interdependency of CIs and further socio-economic systems (Wang et al., 2012). The impact of any triggering event causing CI disruptions has two components. The direct impact on the CI itself, and the indirect impacts that propagate through the network. To understand the importance of CIs and the far-reaching consequences of their failure, modelling individual (engineered) CIs is not sufficient any longer: the need arises for comprehensive and participatory approaches for stress testing CIs that integrate socio-economic concerns, local and global trends and technical knowledge.

This paper aims at presenting an approach towards the development of a comprehensive, efficient, iterative and dynamic stress testing methodology for CI disruptions that supports decision-makers in the evaluation of strategies for improved CI resilience. Resilience relates to the ability of a system to adjust or maintain essential functions under stressful and harsh conditions (Ponomarov and Holcomb, 2009). In this sense, it comprises robustness, agility and flexibility. Due to its exceptional role, we focus on electricity supply and present a framework to develop stress tests. Our methodology addresses system-inherent vulnerabilities and is generic in the sense that it goes beyond specific initiating events. As a stepping-stone towards the overall framework, we present an indicator-based vulnerability assessment and present results that were derived for Hurricane Sandy.

BUILDING RESILIENT CRITICAL INFRASTRUCTURES

Industry and economy have become ever more vulnerable to disruptions and crises. Today, failures may have consequences that propagate through global networks causing shortages and business interruptions in distant regions and economic sectors (Jüttner and Maklan, 2011). While socio-economic environment; technologies; human behaviour and expectations are changing at an ever-increasing pace, bringing changing patterns of risk and interdependencies, physical CIs are intended to operate for decades (Giannopulos et al., 2012). It is impossible to predict all potential causes of disruption, and so the design of resilient CIs should include mechanisms to manage failures from unforeseen hazards.

An additional challenge derives from the fact that functioning CIs are of vital importance for emergency management, while at the same time the events that triggered the emergency typically have consequences on the (physical) CI networks. It is essential, therefore, that the design of resilient CIs recognises that fundamental services need be maintained as much as possible during the emergency and full functions need to be reestablished as soon as possible to facilitate fast recovery.

The evolution of CIs and their interconnectedness imply that understanding and predicting the consequences of disruptions has become extremely difficult. To illustrate the implications for decision-makers, we focus on electricity supply, which is vital for all other CIs. Figure 1 reveals some of the potential consequences of the disruption of electricity supply for current CI networks (Hiete et al., 2010). The actual complexity of the problem is even greater, as electricity generation portfolios are changing (growing emphasis on renewables and low-carbon generation and the implementation of smart grid technologies), leading to a fundamental rearrangement whose consequences with respect to system stability and resilience are not yet well understood.

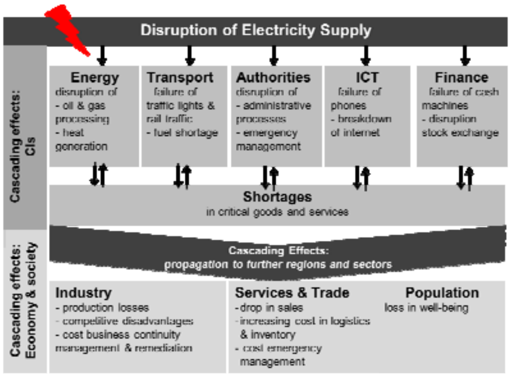
Disruption of Electricity Supply
Cascading effects: CIs
Energy
disruption of
- oil & gas processing
- heat generation
Transport
failure of traffic lights & rail traffic
- fuel shortage
Authorities
disruption of
- administrative processes
- emergency management
ICT
failure of phones
- breakdown of internet
Finance
failure of cash machines
- disruption stock exchange
Shortages
in critical goods and services
Cascading Effects:
propagation to further regions and sectors
Cascading effects: Economy & society
Industry
- production losses
- competitive disadvantages
- cost business continuity management & remediation
Services & Trade
-drop in sales
-increasing cost in logistics & inventory
- cost emergency management
Population
loss in well-being

Figure 1: Impact of disruption of Electricity supply

A DYNAMIC APPROACH TO STRESS TESTING

Following recent crises the EU, among others, has sought to reduce the chance of similar future disasters by '*stress testing*' major systems and infrastructures. Stress tests are targeted at revealing if a system can withstand a shock. To this end, *stress test scenarios* are created that cover a range of factors that together (can) create extraordinary failures. *Vulnerability* refers to the susceptibility of a system to error and failure (Birkmann, 2007) and can be seen as a system-inherent characteristic. While decision-makers can hardly ever influence the hazard events that may occur, stress tests should support decision-making and therefore aim at revealing the most vulnerable parts of CIs and socio-economic systems to enable efficient risk management. So far, stress testing methodologies are typically static: parameters and models are determined before the stress test. For instance, an earthquake of a specific magnitude is supposed to occur in a given region, and the systems are designed to be robust against this known and well-understood hazard (Reason, 1997). However, risks evolve in increasingly fast and unpredicted ways. To our best knowledge, there is currently no approach to dynamically create stress tests that 'attack' the most vulnerable parts of a system. To support decision-makers in designing resilient CIs, a dynamic stress testing methodology is needed that:

- focusses on the vulnerabilities inherent in the system, not on particular external triggering events;
- recognises the interconnectedness of CIs, addresses and evaluates cascading failures;
- is a continuous process that iteratively recognises and adjusts to new information;
- can be adapted to multiple geopolitical scales, socio-economic sectors or groups, time scales and CIs;
- integrates technical, social, economic, environmental, behavioural and organisational perspectives;

- and prioritises strategies to design more resilient CIs and economic networks.

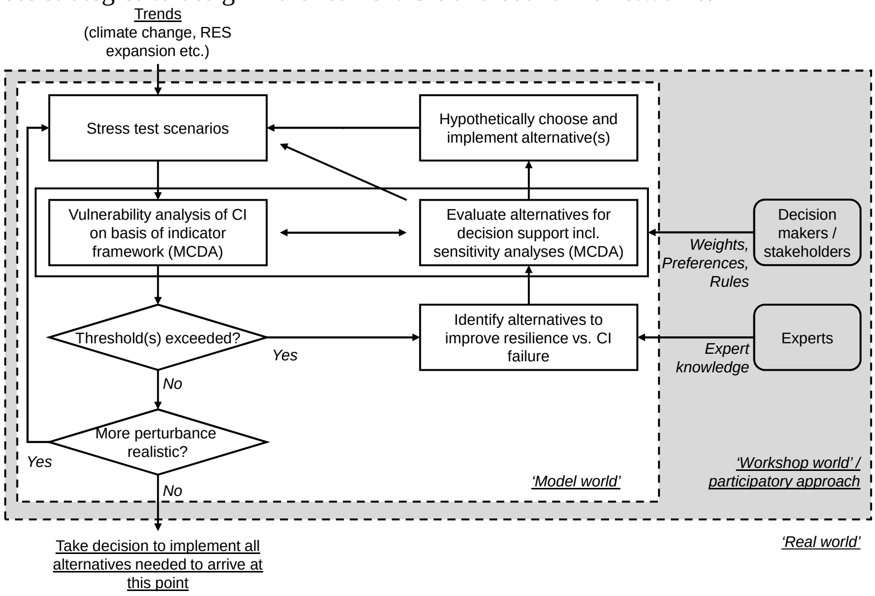
Trends
(climate change, RES expansion etc.)
Stress test scenarios
Hypothetically choose and implement alternative(s)
Vulnerability analysis of CI on basis of indicator framework (MCDA)
Evaluate alternatives for decision support incl. sensitivity analyses (MCDA)
Decision makers / stakeholders
Weights, Preferences, Rules
Threshold(s) exceeded?
Yes
Identify alternatives to improve resilience vs. CI failure
Experts
Expert knowledge
No
More perturbance realistic?
Yes
No
'Model world'
'Workshop world' / participatory approach
Take decision to implement all alternatives needed to arrive at this point
'Real world'

Figure 2: Methodological and decision process framework

In order to address these requirements, we propose an iterative stress test framework as illustrated in Figure 2. The starting point is the design of scenarios that perturb fundamental functions whose disruption lead to the violation of threshold levels (e.g., failure of electricity supply for more than 5 % of customers). It is not our aim to model and simulate all possible worst-case events and scenarios. Credibility is one of the most important aspects in scenario thinking, particularly when extreme scenarios that challenge current mind-sets are presented to the decision-makers (Selin, 2006). To construct scenarios that are plausible and likely to cause significant damage, we propose to start the scenario construction from an analysis of the vulnerability of individual CIs and the socio-economic system. Depending on the focus and scale of the assessment, indicator approaches on sector or regional level (see below), topological analyses, models and simulations can be used to determine vulnerabilities that in turn allow the most critical components of the CIs to be identified, i.e. those components that are prone to failure and whose disruption leads to severe consequences. The stress tests are then designed to disrupt these critical components. By combining results of simulations and models with qualitative expert assessments, insights from different perspectives can be integrated. Expertise from different disciplines is brought together to ensure that each scenario is plausible and justified on scientific grounds. To render the scenarios transparent and understandable, analysis about the adequate aggregation of insights about systems and hazards will be required.

By following the iterative procedure shown in Figure 2, the stress tests are continuously updated to adapt to new insights. In particular, we note two points about the iteration on the stress test scenarios (top left in Figure 2). First, we envisage a growing portfolio of scenarios and that the evaluation is made against a backdrop of all of these. Second, initially we expect each scenario to be very simple: an event that damages one part of the CI, and the most important information to assess the socio-economic vulnerability. The event itself may not even be well defined, but simply stated as an 'event which damages a particular part of the CI'. Exploring such simple events will indicate how the damage propagates. In later iterations, the events can be refined, combined and further environmental or technological factors will be included to understand the interactions of different failures. This approach avoids that CIs are designed only to be robust against well-understood hazards or to satisfy a known set of requirements. Hence, this method helps decision-makers preparing for the integration of emerging risks that may not be known by now, (unexpected) technological changes or socio-economic trends. In this manner, it acknowledges and documents the lack of knowledge from today's perspective. Finally, we emphasize that stress tests should be embedded in the continuous process of risk management to ensure that systems are adapted to emerging risks, new technological developments and changing societal trends.

To focus on the most harmful events for the society and to integrate different perspectives, we suggest using methods from the field of multi-criteria decision analysis (MCDA) that allow stakeholders to specify their requirements for good stress tests, e.g., required levels of safety, economic growth or cost of energy. By coupling the stress test design with participatory approaches to assess priorities and stress test requirements, the dynamic design covers not only external trends, but also respects changes in preferences, risk aversion and societal goals. In both decision support and scenario thinking, the importance of co-creation and ownership has been emphasized (Bertsch et al., 2006; Kok et al., 2006). While traditionally, workshops have been used to bring stakeholders and experts together, today ICT systems and social networks offer new possibilities for the collaborative design and interactive exploration of scenarios (Vervoort et al., 2010), which is of particular importance for the assessment of the typically far-reaching CI disruptions.

INDICATOR BASED VULNERABILITY ANALYSIS: HURRICANE SANDY

As highlighted by Figure 2, the multi-criteria indicator approach to vulnerability analysis and the multi-criteria evaluation of alternatives to increase CI resilience constitute the methodological core parts of the framework. For illustrative purposes, this section describes an economic vulnerability analysis conducted for Hurricane Sandy, which hit the east coast of the US in 2012. About 20 million people were affected by power blackouts that occurred in the aftermath of Sandy. Estimates of the direct costs of these power outages assume about $17 billion for the first ten days (Mühr et al., 2012). Indirect economic losses are expected to be much higher.

We use a hierarchical indicator-based approach (Cutter, 2003) to assess the economic vulnerability of industries in different states of the US. Figure 3 (left) shows the dependency dimensions considered; the indicator level is only shown for electricity. This framework is similar to the structures of MADM attribute trees and follows analogous approaches to integrate several vulnerability dimensions. The respective values per economic sector are normalised using vulnerability functions and subsequently aggregated. As the indicators are interdependent (cf. Figure 3, highlighting the interdependence of electricity and further CIs), the results are corrected by using multiplicative weights, derived via the DEMATEL method (Merz et al., 2012). The right part of Figure 3 shows the vulnerability against power blackouts in different states of the US calculated based on 17 indicators derived from 2011 data from the US Bureau of Economic Analysis.

The hierarchical structure of the indicator framework enables efficient updating: revisions can be limited to the affected branches (as opposed to a complete update). Moreover, new information can be added in terms of further branching (e.g., integration of information about specific production sites). Based on the assessed vulnerabilities, the stress test methodology can develop further models and simulations for the most vulnerable regions or economic sector to create more detailed insights (scalability). As these simulations and consequence models can be time consuming to build and run and may be harder to update, the indicator-based approach is a useful approach to support decision-makers in the identification of the most critical parts of the system, which should be stress tested more exhaustively.

CONCLUSION AND OUTLOOK

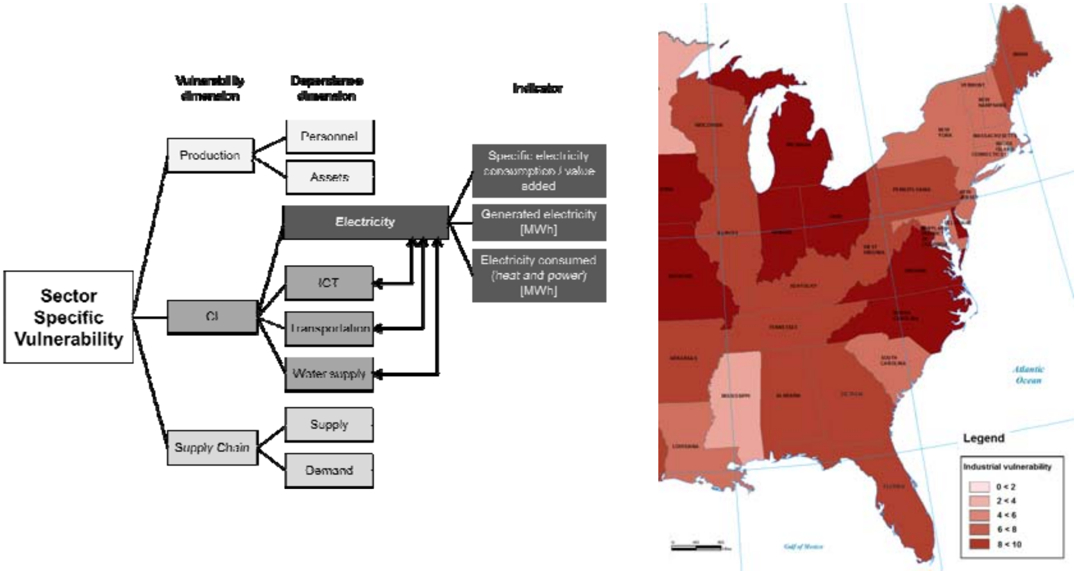

Figure 3: Indicator-based vulnerability assessments and illustrative results for Sandy

Our proposed approach to a comprehensive, efficient and dynamic stress testing methodology aims at supporting risk management for CIs. As we propose focussing on the most harmful consequences (as assessed by using participatory approaches to derive stress test requirements), stress tests can be generated that address system-inherent vulnerabilities rather than starting from specific hazard events determined a priori, which do not necessarily reveal the most harmful consequences. By following the iterative procedure as shown in Figure 2, we enable a dynamic stress test design that enhances robustness against unrecognised and unexpected hazards. The indicator framework for vulnerability analysis recognises the interconnectedness of CIs and enables the assessment of cascading failures. Its hierarchical structure facilitates the integration of new information, which may become available later, and adaptation to more fine-grained scales. The use of multi-criteria techniques allows the integration of different perspectives in both the vulnerability assessment and the prioritisation of strategies for improving CI resilience. The approach, which was illustrated for electricity supply in this paper, is transferrable to all other CIs.

However, the approach needs further development and refinements as well as validation. Inter alia, future research includes the adaptation and use of energy systems models for the provision of quantitative input data to the multi-criteria evaluation of mitigation strategies, quantitative analysis of cascading effects, application of the developed models to hypothetical test regions and the conduction of participatory stakeholder workshops.

REFERENCES

1. Bertsch, V. et al. (2006) Multi-criteria decision support and stakeholder involvement in emergency management. *International Journal of Emergency Management*. 3 (2--3), 114–130.
2. Birkmann, J. (2007) Risk and vulnerability indicators at different scales: Applicability, usefulness and policy implications. *Environmental Hazards*. 7 (1), 20–31.
3. Cutter, S. L. (2003) GI Science, Disasters, and Emergency Management. *Transactions in GIS*. 7 (4), 439–446.
4. Giannopulos, G. et al. (2012) *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. JRC- IPSC (ed.). Luxemburg: European Commission.
5. Haemmerli, B. & Renda, A. (2010) *Protecting Critical Infrastructure in the EU*. Brussels: Centre for European Policy Studies.
6. Hanseth, O. (2010) *Industrial Informatics Design, Use and Innovation*. Jonny Holmström et al. (eds.). Hershey: IGI Global.
7. Hiete, M. et al. (2010) *Krisenhandbuch Stromausfall Baden-Württemberg*. Stuttgart: Innenministerium Baden-Württemberg, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
8. Jüttner, U. & Maklan, S. (2011) Supply chain resilience in the global financial crisis: an empirical study. *Supply Chain Management: An International Journal*. 16 (4), 246–259.
9. Kok, K. et al. (2006) Multi-scale narratives from an IA perspective: Part II. Participatory local scenario development. *Futures*. 38 (3), 285–311.
10. Merz, M. et al. (2012) A composite indicator model to assess natural disaster risks in industry on a spatial level. *Risk Research*. in press.
11. Min, H.-S. J. et al. (2007) Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions*. 39 (1), 57–71.
12. Moteff, J. et al. (2003) *Critical Infrastructures: What Makes an Infrastructure Critical?*
13. Mühr, B. et al. (2012) *CEDIM FDA-Report on Hurricane Sandy*. Karlsruhe / Potsdam: CEDIM.
14. Ponomarov, S. Y. & Holcomb, M. C. (2009) Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*. 20 (1), 124–143.
15. Reason, J. T. (1997) *Managing the Risks of Organizational Accidents*. Farnham, Surrey: Ashgate Publishing Company.
16. Rinaldi, S. M. et al. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*. 21 (6), 11–25.
17. Selin, C. (2006) Trust and the illusive force of scenarios. *Futures*. 38 (1), 1–14.
18. Star, S. L. & Ruhleder, K. (1996) Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research*. 7 (1), 111–134.
19. Trucco, P. et al. (2011) Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures. *Reliability Engenieering & System Safety*. 10551–63.
20. Vervoort, J. M. et al. (2010) Stepping into futures: Exploring the potential of interactive media for participatory scenarios on social-ecological systems. *Futures*. 42 (6), 604–616.
21. Wang, S. et al. (2012) Vulnerability analysis of interdependent infrastructure systems: A methodological framework. *Physica A: Statistical Mechanics and its Applications*. 391 (11), 3323–3335.