Resilience – Preparing Energy Systems for the Unexpected[i]

Stefan Gößling-Reisemann[1]

[1]Faculty of Production Engineering; Institute for Advanced Energy Systems; Sustainability Research Center (artec), University of Bremen

Contact: sgr@uni-bremen.de

Keywords: Resilience, Vulnerability, Risk, Resilience management

Introduction: Contrasting vulnerability, risk and resilience

The resilience of energy systems, their vulnerability and the risks stemming from their failure have been recently received increasing attention in the scientific literature[ii]. Still, the discussion on the meaning and interpretation of resilience as a scientific concept is far from settled (Brand & Jax 2010). For infrastructure systems there is a common thread that describes resilience as the ability of a system to withstand and recover from severe stress and extreme events without losing its ability to provide the services it is designed to deliver (see for example Hollnagel 2013). The concrete definitions of resilience, on the other hand, differ and the usage of related terms, like vulnerability, fragility, or robustness is also far from consensual. As an example, the vulnerability of a system in the context of social-ecological systems is defined as the exposure and sensitivity towards certain stressors "minus" the resilience of the system (Berkes, Colding & Folke 2003, Adger 2003). In this particular interpretation, vulnerability and resilience are seen as opposites, which seems self-evident when focusing on well-known stressors. Resilience in this interpretation is a system's ability to actively respond to stressors and recover quickly from them, thus includes a dynamic component. Vulnerability in this context is interpreted as the existence of a stressor acting on the system (exposure) and the potential for damage on the system being caused by the stressor, depending on the system's internal conditions (sensitivity). In the context of homeland security, cyber-security and terrorism, a different understanding of vulnerability and resilience is dominant. Vulnerability in this context is interpreted as a part of risk, where risk is understood as the product of threat likelihood, vulnerability of the threatened system and the consequences of the threat (DHS 2010, Linkov et al. 2014). In this interpretation, a system's vulnerability reflects the existence of a physical or operational weakness which allows a threat to cause damage or loss of functionality. Resilience in this context is interpreted as a "system's ability to prepare for, absorb, recover from and more

[i] This paper is part of the IRGC Resource Guide on Resilience, available at: https://www.irgc.org/risk-governance/resilience/. Please cite like a book chapter including the following information: IRGC (2016). Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center. *v29-07-2016*

[ii] See for example the National Academies Workshop on "The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters" (http://www.nap.edu/catalog/18535/the-resilience-of-the-electric-power-delivery-system-in-response-to-terrorism-and-natural-disasters), the UKERC report "Building a Resilient UK Energy System" (http://www.ukerc.ac.uk/publications/building-a-resilient-uk-energy-system-research-report.html), the special issue of *Energies* on the resilience of energy systems (http://www.mdpi.com/journal/energies/special_issues/resilience), or Molyneaux et al. (2016)

successfully adapt to adverse events" (NRC 2012, Linkov et al. 2014), it thus includes a dynamic and proactive notion of managing potentially harmful stressors.

In view of the largely unknown nature of future stressors, shocks and developments, it makes sense to distinguish the aspects of vulnerability and resilience even further, especially with regard to their scope. When the scope of the possible stressors is widened to include such stressors that are not or only partially known (e.g. the famous "black swans"), vulnerability and resilience reflect different properties of a system. Vulnerability, as it is used in most of the academic and general literature, focuses on the degree to which a system can be harmed by external or internal stressors or events (Adger 2006). The focus usually lies on known stressors. The concept of vulnerability therefore lends itself to analysis, when specific and well-described events or stressors are correlated with the system's sensitivity and adaptive capacity (Gößling-Reisemann et al. 2013). Resilience, on the other hand, can be interpreted even more widely, as the ability of a system to prepare for, cope with and recover from any kind of stressor or event while maintaining the system's service, without necessarily knowing about the specifics of the event or the stressor. If interpreted in this broad way, resilience no longer can be analyzed in the strict sense, since the basis for analysis would have to include all known and unknown (!) stressors, an endeavor that is surely unfeasible. Nevertheless, this definition of resilience can be used as a guiding principle for designing systems and through its vagueness and malleability serve as a boundary object for a diverse range of disciplines, e.g. from sociology to engineering (Brand & Jax 2010, Brand & Gleich 2015).

The uncertain nature of stressors and the capacity to deal with them

Resilience-building, in the above sense of resilience, can be understood as a strategy to deal with deep uncertainty, i.e. uncertainty that cannot be reduced by statistics or predictive modeling. Resilience-building and other risk management strategies are thus not to be seen as mutually exclusive, they rather complement each other. Resilience-building can help find answers to stressors that cover a wide range of characteristics, and as a strategy has its comparative strengths where the stressors are unknown with respect to their likelihood of occurrence, their potential impact, or even the nature of their impact on the respective system.

We propose to distinguish certain characteristics of stressors and the capabilities a resilient system should possess in order to deal with them. Stressors are characterized by their dynamics and the state of knowledge about their nature, as follows:

- **Known/expected**: stressors that the system has already experienced in the past and where predictions of future occurrence exist
- **Unknown/unexpected**: stressors that the system has never or only very rarely been exposed to and where predictions for future occurrences do not exist
- **Gradual/creeping**: stressors that develop slowly and possibly undetected for some time
- **Abrupt/sudden**: stressors that develop suddenly or abruptly without warning

A system that is capable of preparing for, coping with and recover from stressors with an arbitrary combination of the above attributes needs a diverse set of capabilities. For example, when the stressor develops gradually and is already known to the system or can be expected to occur in the near future, an adaptation of existing structures, components and organizations can be initiated to

better cope with and recover from occurrences of this stressor. On the other extreme, when the stressor is unknown and develops abruptly, the system will not have time to find innovative solutions or build up resistance, so that it has to use existing resources in the most appropriate form possible to deal with the situation, i.e. it needs to improvise. The needed capabilities for a system to cope with these stressors can thus be summarized as robustness, adaptive capacity, innovation capacity and improvisation capacity, see figure 1 (cf Gößling-Reisemann et al. 2013).

Stressor	known	unknown
gradual / creeping	adaptive capacity	innovation capacity
abrupt / sudden	resistance/robustness	improvisation capacity

Figure 1: Characteristics of stressors and needed capabilities

The building up of these capabilities will improve any system's ability to deal with stressors of many kinds. However, these capabilities are also rather abstract and need "spelling out" for specific systems. Some of the capabilities will require similar structure and processes as traditional risk management: monitoring, predictive modeling, system simulation, crisis management, etc. However, with the additional focus on the "unknown" stressors, it will require new mechanisms and processes to deal with surprises and deep uncertainty.

Instruments for resilience management: How to develop resilience within systems and organizations?

The instruments for resilience management, which should be based on the above derived general capabilities, can be grouped into four main phases or managing resilience: prepare and prevent, implement robust and precautionary design, manage and recover from crises, learn for the future. Here, the instruments are exemplified for energy systems[iii].

Prepare and prevent: as a first measure, past crises and near accidents should be transparently documented and examined to learn about the stressors that caused them and the context in which they occurred, or in which they were avoided, respectively. The latter is especially important as a learning tool for resilience engineering (Hollnagel 2007). Further analysis should be directed at stressors that have not yet occurred, but are likely to occur in the near future, e.g. known from trend extrapolation. For the energy system this would include using climate change trends, like trends for extreme weather conditions, in system simulations and planning. The observed trends of converging and coupling of infrastructures (electricity, gas, heat, fuels, IT) in the course of a transition to high shares of renewable energies should also be observed for new threats and vulnerabilities, like hacker attacks, data privacy issues or cascading failures across infrastructures. Furthermore, new threats can stem from social processes, for example increasing non-acceptance of certain technologies or unfair

[iii] This section is partly based on discussions within the working group *Risk and Resilience* as part of the ESYS (Energiesysteme der Zukunft) project organized by the German National Academy of Sciences and Engineering, the Union of German Academies of Science and Leopoldina – National Academy of Sciences (http://www.acatech.de/uk/home-uk/work-and-results/projects/esys-energy-systems-of-the-future-stage-2.html). The text is, however, the sole responsibility of the author and not endorsed by the mentioned project consortium.

cost-benefit distributions in the context of energy transitions leading to protests and delays or halts in necessary system changes. Newly developing stressors can be analyzed by vulnerability assessment methodologies. Results from theses analyses should then be used to adjust the design parameters of energy system components (technology level), develop testing scenarios and design guidelines for coupled infrastructures (system level) and monitor social impacts and responses to technological change with feedback to governance processes (governance level).

Implement robust and precautionary design: in line with the above detailed characteristic capabilities of resilient systems, the central design elements of resilient energy systems must comprise robustness, adaptive capacity, innovation capacity and improvisation capacity. On the design level of components and systems the resilience-enhancing capabilities can be achieved by first **strengthening** the identified vulnerable elements (see above) by increasing **redundancy, buffer capacity and energy storage**. This will reduce the stress on vulnerable elements in the system and will also act as a precautionary measure for further and yet unknown stressors. In order to prepare for unknown future stressors, it is also advisable to check existing technologies in the energy system for alternative solutions in order to enhance the **diversity**. Diversity should encompass notions of variety, disparity and balance (cf. Stirling 2007 and 2010). Additional analyses should also be directed at components and structures that have not yet been affected by known stressors but are otherwise crucial to the system. As a precautionary measure, they should also be strengthened by increased diversity, redundancy, and buffer and storage capacity. Especially for new couplings between systems (e.g. between electricity and mobility sector) and newly developing technologies (e.g. smart grid and cyber-physical energy systems) special attention on new potential vulnerabilities is needed, since integrating different systems into one also imports the respective vulnerabilities. Resilient coupling of systems should yield additional flexibilities to buffer imbalances in each sub-system, while minimizing the potential for cascading failures (**loose or flexible coupling**, cf. Perrow 2011, Orton and Weick 1990, Beekun and Glick 2001 for loosely coupled organization). It should be obvious that these resilience design measures will cause conflict with other design goals of energy systems, most prominently with technical efficiency and (at least short-term) economic competitiveness. Some conflicts with the ecological sustainability might also be possible, especially in terms of additional equipment and possibly reduced efficiency. These conflicts need to be addressed systematically by **cost-benefit analyses** that include long-term effects and an evaluation of costs due to rare but possibly extremely damaging events.

Manage and recover from crises: If failures of the energy system lead to crises, they should be restricted to the smallest possible area or subsystem and be overcome as quickly as possible. In order to reduce the extent of such crises, emergency planning and respective measures must be implemented on the regional or local level. With the increasing share of renewable energies comes a trend towards decentralization of energy systems, which can be utilized for increased resilience. Currently, the restoration of the electricity supply after blackouts in most industrialized countries is organized in a rather central fashion and dependent on large thermal power plants. A decentral design more in line with increasing decentral renewables and the advent of smart grids would be to organize the energy system in a cellular structure where each cell has the potential to run autonomously for a limited time and inter-cellular synchronization is used to restore overall system performance after blackouts. The adequate size of these cells has still to be determined and will also be dependent on the respective investments necessary to equip cells with restorative functions in relation to the added resilience of the overall system. Flexible coupling between the electricity

system and other energy subsystems (especially gas, heat and fuel networks) will increase the restorative capacity and decrease the need for regional storage capacity.

Learn for the future: mastered or averted crises should be used to learn and increase the adaptive capacity of the system. This can be achieved by documenting and analyzing these crises and events thereby identifying the weaknesses that led to their occurrence (vulnerability store), or, respectively, identify the strengths that led to their avoidance or recovery (solution store). Knowledge about crises and potential solutions should then be used to create simulations and business games for system actors on all levels. Improvisation capacity can be increased by confronting actors in these simulations with unforeseen and unlikely developments, like combined external threats and internal failures of equipment. In the actual operation of the energy system, improvisation capacity can also be improved by allowing a certain amount of unused resources to be maintained in the system, comparable to a strategy called "organizational slack" in business organizations (cf. Cyert & March 1963, Linnenluecke & Griffiths 2010)

Metrics: Criteria or indicators for resilience. Measurement and quantification.

Based on the rather broad definitions of resilience, risk and vulnerability introduced above, it is not possible to truly analyze these aspects of a given energy system, as we can e.g. for aspects like availability. We can, however, derive metrics and measures that capture certain aspects of resilience and combine them into metrics, which can be used in the planning and design of energy systems The system property probably most accessible to measurement and analysis is the vulnerability of the system, as measured by the observed impact of known and observable stressors on the system service. Some indicators might be defined and evaluated that describe a system's performance in and after a crisis, as a basis to analyze its vulnerability (cf. Gößling-Reisemann et al. 2013a). Typically, these will include the energy not delivered, the value of lost load, the duration of outages and the time for recovery of full system operations, the physical damage to equipment, the number or relative share of customers affected, and so on. These indicators are well known from the reliability assessment of energy infrastructures and, when evaluated after stressful events and optionally compared with benchmark systems, indicate the absolute or relative vulnerability of a given energy system[iv].

For resilience in the more general interpretation as defined above, i.e. based on the capability to prepare for *any* given event, a true measurement of this capability is unfeasible. However, one can assess the degree to which the above-mentioned design components have been implemented. Buffers and storages of various forms can, for example, be evaluated against the overall energy consumption in a given system, or quantified as the storage-based duration of supply at maximum or average load in the system (cf. Chaudry et al. 2011). Couplings with other infrastructures can be qualitatively assessed as to whether and how far an outage in one system (e.g. the IT infrastructure) will generate failures in other systems (e.g. the electricity supply). Threat scenarios (e.g. developed by NESCOR[v] for coupled IT and energy systems) can be used to systematically address these couplings. Also the diversity of energy systems can be assessed by using diversity measures like the

[iv] For a review of resilience metrics which are based on an alternative definition of resilience see (Willis & Loa 2015)

[v] National Electric Sector Cybersecurity Organization Resource: http://smartgrid.epri.com/NESCOR.aspx

Shannon index or more complex measures involving the above-mentioned attributes of variety, disparity and balance (Stirling 2007 and 2010).

In the more restricted context of specific and already known stressors and an energy system's respective resilience, more detailed metrics and indices of resilience can be derived. These metrics usually involve some measure of the stressors' effects on system functionality and the dynamics of these effects during the phases of planning/preparation, absorption of effects, recovery and adaptation (see e.g. Ganin et al. 2015). There has been recent publications on resilience metrics for energy systems that very well summarize the state of the discussion on this topic (see e.g. Roege et al. 2014, Willis & Loa 2015 or Molyneaux et al. 2016).

Annotated bibliography

(by topic)

Adger, W. N. (2003). Building resilience to promote sustainability. IHDP Update, 2(2003), 1-3.

Adger, W. N. (2006). Vulnerability. Global Environmental Change, 16(3), 268-281.

Berkes, F., Colding, J. F., Folke, C. (2003). Navigating social-ecological systems. Building resilience for complexity and change. Cambridge: Cambridge University Press.

Brand, F. S., & Jax, K. (2007). Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. Ecology and Society, 12(1), 23.

Adger and Berkes et al. discuss the general meaning of resilience and how it is related to the concepts of sustainability and vulnerability. The discussion is not focused on energy systems, but very generally touches on topics relevant also for infrastructures as not only technical, but socio-technical systems. Brand and Jax take this discussion one step further in order to show how resilience can be used as either a descriptive concept or as a boundary object, being fruitfully shared as a normative or analytical concept between a multitude of disciplines.

Gößling-Reisemann, S., Wachsmuth, J., Stührmann, S., & Gleich, A. (2013a). Climate change and structural vulnerability of a metropolitan energy system. Journal of Industrial Ecology, 17(6), 846-858.

Gößling-Reisemann, S., Stührmann, S., Wachsmuth, J., Gleich, A. v. (2013b). Vulnerabilität und Resilienz von Energiesystemen. In: J. Radtke, B. Hennig (Ed.): Die deutsche „Energiewende" nach Fukushima – Der wissenschaftliche Diskurs zwischen Atomausstieg und Wachstumsdebatte, Marburg: Metropolis-Verlag.

Brand, U., & Gleich, A. v. (2015). Transformation toward a secure and precaution-oriented energy system with the guiding concept of resilience—Implementation of low-exergy solutions in northwestern Germany. Energies, 8(7), 6995-7019.

Gößling-Reisemann and colleagues discuss the conceptual differences between vulnerability and resilience of energy systems, present an analytical method to assess vulnerability and describe generalizable properties and design elements of resilient energy systems that can be

used to formulate guiding concepts for energy systems. Brand and Gleich describe how the guiding concept of resilience can be used in a socio-technical context for implementing precaution in an energy transformation process and to what extent it can drive innovation.

Stirling, A. (2010). Multicriteria diversity analysis: A novel heuristic framework for appraising energy portfolios. Energy Policy, 38(4), 1622-1634.

Stirling, A. (2007). A general framework for analysing diversity in science, technology and society. Journal of the Royal Society Interface, 4(15), 707-719.

Stirling gives a detailed description of how to measure and operationalize diversity in the context of energy systems. He makes an important contribution to the question of how to actually measure diversity and thus how to operationalize certain aspects of resilience.

Hollnagel, E., Woods, D. D., & Leveson, N. (2007). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

Hollnagel, E. (Ed.). (2013). Resilience engineering in practice: A guidebook. Ashgate Publishing, Ltd.

Hollnagel and colleagues introduce the concept of resilience engineering as a strategy to improve the resilience of engineered structures and systems. The focus is on learning from successful operations as much as learning from failures. The definition of resilience is very close to the one discussed in this text and focuses on maintaining function or services, not structure, of a system.

Cyert, R. M., & March, J. G. (1963). A behavioral theory of the firm. Englewood Cliffs, NJ, 2.

Linnenluecke, M., & Griffiths, A. (2010). Beyond adaptation: Resilience for business in light of climate change and weather extremes. Business & Society.

Cyert and March have discovered the positive effect of “slack” (here: financial slack), in the meaning of unutilized resources, on the competitive advantage of firms. Linneluecke and Griffiths have extended the notion of slack to include other resources as well and put them in context with the adaptive capacity of business organizations and their resilience towards climate change and extreme events.

Orton, J. D., & Weick, K. E. (1990). Loosely coupled systems: A reconceptualization. Academy of Management Review, 15(2), 203-223.

Beekun, R. I., & Glick, W. H. (2001). Organization structure from a loose coupling perspective: A multidimensional approach. Decision Sciences, 32(2), 227-250.

Perrow, C. (2011). Normal accidents: Living with high risk technologies. Princeton University Press.

Orton and Weick have analysed and re-organized the concept of “loose coupling” for organizations, originally co-developed by Weick, to better explore its explanatory value and make it operational for managing organisations and improve aspects like buffering, adaptability, and effectiveness. Beekun and Glick build a mathematical notation around several defining aspects of loose coupling and apply their framework to case studies from different fields, making the framework operational to assess the specific coupling in

organizations and its implications. Perrow shows how loose coupling in complex socio-technical systems is able to prevent accidents by allowing the system to accommodate shocks, allowing degraded operations and thus generating more time for emergency responses.

Willis, H. H. & Loa, K. (2015). Measuring the resilience of energy distribution systems. Santa Monica, USA: RAND Corporation. http://www.rand.org/pubs/research_reports/RR883.html.

Molyneaux, L., Brown, C., Wagner, L., & Foster, J. (2016). Measuring resilience in energy systems: Insights from a range of disciplines. Renewable and Sustainable Energy Reviews, 59, 1068-1079.

Chaudry, M., Ekins, P., Ramachandran, K., Shakoor, A., Skea, J., Strbac, G. & Whitaker, J. (2011). Building a resilient UK energy system. UK Energy Research Centre, London.

Roege, P. E., Collier, Z. A., Mancillas, J., McDonagh, J. A., & Linkov, I. (2014). Metrics for energy resilience. Energy Policy, 72, 249-256.

Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A. & Linkov, I. (2016). Operational resilience: concepts, design and analysis. Scientific Reports, 6.

Roege et al, Willis and Loa, as well as Molyneaux and colleagues collect and review resilience metrics for energy systems, combining results from different disciplinary approaches to the problem. Chaudry et al. derive and apply some basic resilience indicators for the UK energy system to highlight the potential for decreasing the risk of supply disruptions and Ganin and colleagues derive more generalizable measures for resilience, applicable not only to energy systems but a wider class of complex coupled systems. In the resilience concept as introduced in this text the measurement of resilience does not play an important role, while vulnerability is the analytical category. However, some of the indicators would also work well in a framework for assessing vulnerability.

Department of Homeland Security (DHS) (2010). DHS risk lexicon. Washington DC.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., & Thiel-Clemen, T. (2014). Risking resilience: Changing the resilience paradigm, Commentary to Nature Climate Change.

National Research Council (NRC) (2012). Disaster resilience: A national imperative. The National Academies Press, Washington DC.

The DHS and Linkov et al. describe how resilience, risk and security are linked and the role resilience plays in managing risks in complex and integrated systems which are subjected to highly uncertain stressors. The DHS lexicon provides brief descriptions of the relevant concepts in this context