Engineering Resilience in Critical Infrastructures[i]

Prof. Dr. Giovanni Sansavini[1]

[1]Reliability & Risk Engineering Laboratory, Institute of Energy Technology, Dep. of Mechanical and Process Eng., ETH Zurich

Contact: sansavig@ethz.ch

Keywords: Critical infrastructures, Cascading failures, Self-healing, Adaptation, Recovery, Restoration, Robust optimization

Defining Resilience

Resilience has emerged in the last decade as a concept for better understanding the performance of infrastructures, especially their behaviour during and after the occurrence of disturbances, e.g. natural hazards or technical failures. Recently, resilience has grown as a proactive approach to enhance the ability of infrastructures to prevent damage before disturbance events, mitigate losses during the events and improve the recovery capability after the events, beyond the concept of pure prevention and hardening (Woods, Four concepts for resilience and the implications for the future of resilience engineering, 2015).

The concept of resilience is still evolving and has been developing in various fields (Hosseini, Barker, & Ramirez-Marquez, 2016). The first definition described resilience as "a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (Holling, 1973). Several domain-specific resilience definitions have been proposed (Ouyang, Dueñas-Osorio, & Min, A three-stage resilience analysis framework for urban infrastructure systems, 2012) (Adger, 2000) (Pant, Barker, & Zobel, 2014) (Francis & Bekera, 2014). Further developments of this concept should include endogenous and exogenous events and recovery efforts. To include these factors, resilience is broadly defined as "the ability of a system to resist the effects of disruptive forces and to reduce performance deviations" (Nan, Sansavini, & Kröger, 2016).

Assessing and engineering systems resilience is emerging as a fundamental concern in risk research (Woods & Hollnagel, Resilience Engineering: Concepts and Precepts, 2006) (Haimes, 2009) (McCarthy, et al., 2007) (McDaniels, Chang, Cole, Mikawoz, & Longstaff, 2008). Resilience adds a dynamical and proactive perspective into risk governance by focusing (i) on the evolution of system performance during undesired system conditions, and (ii) on surprises ("known unknowns" or "unknown unknowns"), i.e. disruptive events and operating regimes which were not considered likely design conditions. Resilience encompasses the concept of vulnerability (Johansson & Hassel, 2010) (Kröger & Zio, 2011) as a strategy to strengthen the system response and foster graceful degradation

---

[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*

against a wide spectrum of known and unknown hazards. Moreover, it expands vulnerability in the direction of system reaction/adaptation and capability of recovering an adequate level of performance following the performance transient.

Need for Resilience in Critical Interdependent Infrastructures

Resilience calls for developing a strategy rather than performing an assessment. If on the one hand it is important to quantify and measure resilience in the context of risk management, it is even more important that the quantification effort enables the engineering of resilience into critical infrastructures. Especially for emerging, not-well-understood hazards and “surprises” (Paté-Cornell, 2012), resilience integrates very smoothly into risk management, and expediently focuses the perspective on the ex-ante system design process. Following this perspective, risk thinking becomes increasingly embedded into the system design process.

The application of resilience-building strategies look particularly promising for critical interdependent infrastructures, also called systems-of-systems, because of its dynamical perspective in which the system responds to the shock event, adapting and self-healing, and eventually recovers to a suitable level of performance. Such perspective well suits the characteristics of these complex systems, i.e. i) the coexistence of multiple time scales, from infrastructure evolution to real-time contingencies; ii) multiple levels of interdependencies and lack of fixed boundaries, i.e. they are made of multiple layers (management, information & control, energy, physical infrastructure); iii) broad spectrum of hazards and threats; iv) different types of physical flows, i.e. mass, information, power, vehicles; v) presence of organizational and human factors, which play a major role in severe accidents, highlighting the importance of assessing the performance of the social system together with the technical systems.

As a key system of interdependent infrastructures, the energy infrastructure is well suited to resilience engineering. In the context of security of supply and security of the operations, resilience encompasses the concept of flexibility in energy systems. Flexibility providers, i.e. hydro and gas-fired plants, cross-border exchanges, storage technologies, demand management, decentralized generation, ensure enough coping capacity, redundancy and diversity during supply shortages, uncertain fluctuating operating conditions and unforeseen contingencies (Roege, Collier, Mancillas, McDonagh, & Linkov, 2014) (Skea, et al., 2011).

Building Resilience in Critical Infrastructures

In the context of critical infrastructures, resilience can be developed by focusing on the different phases of the transient performance following a disturbance (also called resilience curve), and devising strategies and improvements which strengthen the system response.

Focusing mainly on the technical aspects, these strategies can be summarized as:

- Planning ahead during the design phase: robust or stochastic optimization against uncertain future scenarios, i.e. attacks or uncertain future demand in the energy infrastructure, can be used in the system planning or expansion process; uncertain scenarios provide the basis to design resilient systems.

- Self-healing, adaptation and control, i.e. graceful degradation: the system cannot be design with respect to every uncertain scenario, therefore a resilient design should consider how to prevent the disturbance from spreading across the whole system, creating systemic contagion and system-wide collapse. In this respect, cascading failures analysis, and engineering network systems to be robust against outbreak of outages and propagations of cascading failures across their elements are key strategies. Control engineering can provide strategies to create robust feedback loops capable of enabling infrastructures to absorb shocks and avoid instabilities. Designing structures and topologies which prevent failure propagation, and devising flexible topologies by switching elements which allow graceful degradation of system performances after disruptions are also valuable resilience-enhancing techniques.
- Recovering quickly from the minimum performance level: robust or stochastic optimization of the recovery and restoration process in the face of uncertainties in the repair process or in the disruption scenarios.
- Effective system restoration: through the combination of restoration strategies, e.g. repairing the failed elements and building new elements, the infrastructure can achieve a higher performance with respect to the pre-disruption conditions.
- Exploiting interdependencies among infrastructures: interdependencies and couplings in systems operations can foster the propagations of failure across coupled system; on the other hands, interdependencies might also provide additional flexibility in disrupted conditions and additional resources that can facilitate achieving stable conditions of the coupled system.

Quantifying Resilience

Resilience is defined and measured based on system performance. The selection of the appropriate MOP depends on the specific service provided by the system under analysis.

The resilience definition can be further interpreted as the ability of the system to withstand a change or a disruptive event by reducing the initial negative impacts (absorptive capability), by adapting itself to them (adaptive capability) and by recovering from them (restorative capability). Enhancing any of these features will enhance system resilience. It is important to understand and quantify these capabilities that contribute to the characterization of system resilience (Fiksel, 2003). Absorptive capability refers to an endogenous ability of the system to reduce the negative impacts caused by disruptive events and minimize consequences. In order to quantify this capability, robustness can be used, which is defined as the strength of the system to resist disruption. This capability can be enhanced by improving system redundancy, which provides an alternative way for the system to operate. Adaptive capability refers to an endogenous ability of the system to adapt to disruptive events through self-organization in order to minimize consequences. Emergency systems can be used to enhance adaptive capability. Restorative capability refers to an ability of the system to be repaired. The effects of adaptive and restorative capacities overlap and therefore, their combined effects on the system performance are quantified by rapidity and performance loss.

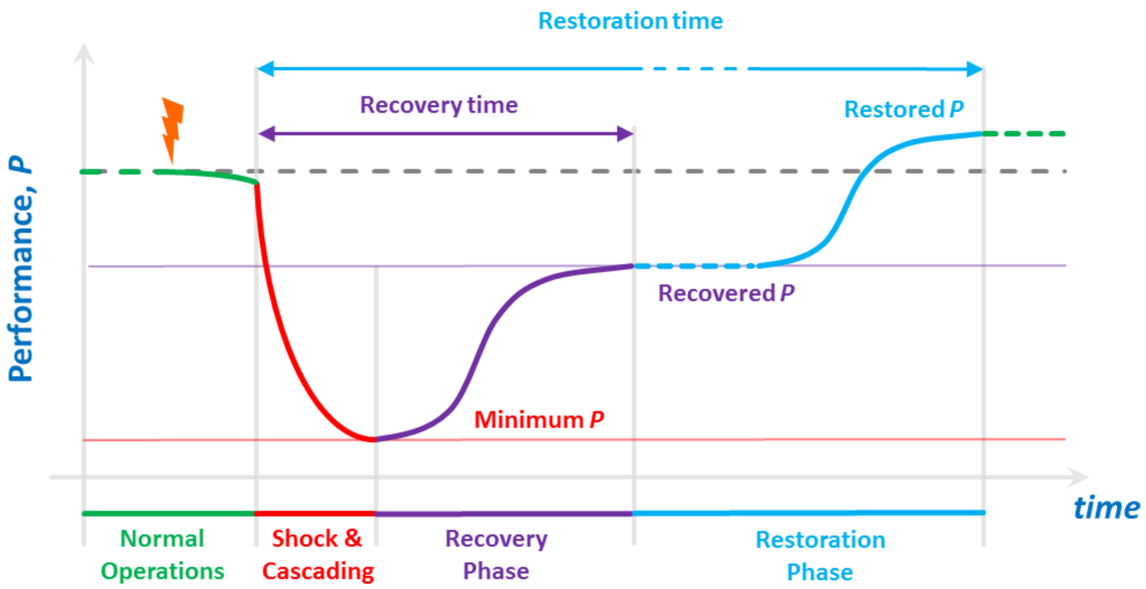

Figure 1: The "resilience curve", i.e. the performance transient after disturbance, and its phases.

Resilience can be quantified through computational experiments in which disruptions are triggered, the system performance is analyzed (Figure 1), and integrated resilience metrics are computed (Nan, Sansavini, & Kröger, 2016). By repeating this process, different system design solutions can be ranked with respect to resilience. By the same token, resilience against various disruptions can be assessed, and resilience-improving strategies compared.

During the last decade, researchers have proposed different methods for quantifying resilience. In 2003, the first conceptual framework was proposed to measure the seismic resilience of a community (Bruneau, et al., 2003), by introducing the concept of Resilience Loss, later also referred to as "resilience triangle".

In recent years, the importance of improving the resilience of interdependent critical infrastructures has been recognised, and research works have developed. Historically, knowledge-based approaches have been applied to improve the understanding of infrastructures resilience (McDaniels, Chang, Cole, Mikawoz, & Longstaff, 2008). Lately, model-based approaches have been developed to overcome the limitations of data-driven approaches, such as System Dynamics (Bueno, 2012), Complex Network Theory (Gao, Barzel, & Barabási, 2016), and hybrid approaches (Nan, Sansavini, & Kröger, 2016).

Approaches to quantify system resilience should be able to

- Capture the complex behaviour of interdependent infrastructures
- Cover all phases of the transient performance following the disruption, and to include all resilience capabilities
- Clarify the overlap with other concepts such as robustness, vulnerability and fragility.

Resilience quantification of interdependent infrastructures is still at an early stage. Currently, a comprehensive method aiming at improving our understanding of the system resilience and at analysing the resilience by performing in-depth experiments is still missing.

Annotated Bibliography

Adger, W. (2000). Social and ecological resilience: are they related? Progress in Human Geography, 347-364.
Discussion about the concept of resilience in different domains.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., & Reinhorn, A. M. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, 733-752.
This paper presents a conceptual framework to define seismic resilience of communities and quantitative measures of resilience that can be useful for a coordinated research effort focusing on enhancing this resilience.

Bueno, N. P. (2012). Assessing the resilience of small socio-ecological systems based on the dominant polarity of their feedback structure. System Dynamics Review, 351–360.
This paper uses loop polarity analysis system dynamics analysis to build a practical procedure for assessing the degree of resilience of socio-ecological systems.

Fiksel, J. (2003). Designing Resilient, Sustainable Systems. Environ. Sci. Technol., 5330–5339.
This paper proposes a sustainable design approach which encourages explicit consideration of resilience in both engineered systems and the larger systems in which they are embedded.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering & System Safety, 90-103.
They proposed a resilience analysis framework whose implementation is encapsulated within resilience metric incorporating absorptive, adaptive, and restorative capacities.

Gao, J., Barzel, B., & Barabási, A.-L. (2016). Universal resilience patterns in complex networks. Nature, 307–312.
The paper develops analytical tools that identify the natural control and state parameters of a multi-dimensional complex system, and derives effective one-dimensional dynamics that accurately predict resilience.

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. Risk Analysis, 498-501.

Holling, C. S. (1973). Resilience and stability of ecological systems. Annual review of ecology and systematics, 1-23.
One of the first usage if resilience in the context of "systems".

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

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety, 1335–1344.
In the present paper, an approach for modelling interdependent technical infrastructures is proposed, and it is shown how the model can be employed in a vulnerability analysis.

Kröger, W., & Zio, E. (2011). Vulnerable Systems. London: Springer-Verlag.
Vulnerable Systems reflects the current state of knowledge on the procedures which are being put forward for the risk and vulnerability analysis of critical infrastructures.

McCarthy, J., Pommering, C., Perelman, L., Scalingi, P., Garbin, D., Shortle, J. .., . . . 97-109. (2007). Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. Fairfax: George Mason University.
Shifting the paradigm from protection to resilience in infrastructure systems.

McDaniels, T., Chang, S., Cole, D., Mikawoz, J., & Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. Global Environmental Change, 310-318.
This paper develops a conceptual framework for understanding the factors that influence the resilience of infrastructure systems in terms of two dimensions: robustness and rapidity.

Nan, C., Sansavini, G., & Kröger, W. (2016). Building an Integrated Metric for Quantifying the Resilience of Interdependent Infrastructure Systems. In Critical Information Infrastructures Security (pp. 159-171). Springer International Publishing.
In this paper, an integrated metric for resilience quantification with capabilities of incorporating different performance measures is proposed, which can be used to quantify the performance of interdependent infrastructure systems.

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems with a focus on joint restoration modeling and analysis. Reliability Engineering & System Safety, 74-82.
They propose a method to assess resilience of interdependent infrastructure systems and compare the effectiveness of five restoration strategies.

Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. Structural Safety, 23-31.
A multi-stage framework to analyse urban infrastructure system resilience under multiple hazards is developed. The effects of different strategies for resilience improvement are compared.

Pant, R., Barker, K., & Zobel, C. W. (2014). Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. Reliability Engineering & System Safety, 92–102.
This paper proposes quantitative metrics to guide a preparedness decision making framework to promote interdependent economic resilience estimation.

Paté-Cornell, E. (2012). On “Black Swans” and “Perfect Storms”: Risk Analysis and Management When Statistics Are Not Enough. Risk Analysis, 1823–1833.

Roege, P. E., Collier, Z. A., Mancillas, J., McDonagh, J. A., & Linkov, I. (2014). Metrics for energy resilience. Energy Policy, 249–256.
This paper develops a matrix-based approach to generate energy resilience metrics which can be used in energy planning, system design, and operations.

Skea, J., Chaudry, M., Ekins, P., Ramachandran, K., Shakoor, A., & Wang, X. (2011). A Resilient Energy System. In J. S. Paul Ekins, Energy 2050: Making the Transition to a Secure Low-Carbon Energy System (pp. 145-186). Taylor & Francis.
This contributions investigates energy system shocks and possible responses, and reviews resilience indicators for the enrgy network industry.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 5-9.
Review of 4 concepts underlying resilience definition and how they can guide engineering resilience for safety.

Woods, D. D., & Hollnagel, E. (2006). Resilience Engineering: Concepts and Precepts. Boca Raton: CRC Press.