RESILIENCE ENGINEERING - HOW TO HANDLE THE UNEXPECTED

Stefan Hiermaier, Sandra Hasenstein and Katja Faist[1]

[1] Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, Eckerstr. 4, 79104 Freiburg, Germany

[1]hiermaier@emi.fraunhofer.de

http://www.emi.fraunhofer.de/en.html

Abstract

Resilience engineering is concerned with the design, construction and operation of critical infrastructures aiming at abilities like disaster tolerance, quick recovery and adaptation. Quantitative measures to assess the resilience of a given system refer to this ability via time integrals describing the loss performance after a disruptive event.

There are two characteristics of disruptive events typically challenging the resilient design of critical infrastructure. First uncertainty, they often happen to an unexpected time or in an unanticipated way. Second, due to the ever rising complexity and inter-connectedness of the involved systems, their potential to initiate cascading effects is big. As a consequence, a classical threat-based approach for the resilient configuration of a system potentially misses its design goal if neglected sources of harm lead to a disruption.

Being used to outlay a system based on threats with given loads and boundary conditions, engineers easily find themselves in a dilemma if confronted with the task to deliver a resilient design for the unexpected. This paper discusses an approach utilizing generic damage scenarios as one option to go beyond classical threat-based concepts.

1 INTRODUCTION

Resilience engineering is concerned with the design, construction and operation of critical infrastructures aiming at abilities like disaster tolerance, quick recovery and adaptation. The criticality of an infrastructure is given if a system or a facility is essential for the maintenance of vital societal functions [Council of the European Union (2008)]. Supply chains, communication grids or transport infrastructure as well as financial or security services are typical representatives.

Engineers adopted the resilience concept introduced in the late seventies of the last century by psychologists [Werner, (1977)] in order to extend the classical perception of safety and security. According to Biringer et al. (2013) "… the infrastructure security community in the United States and globally recognized that it was simply not possible to prevent all threats to all assets at all times." The engineering concept for resilience of critical infrastructures takes into account the residual performance of a damaged system after a disruptive event as well as time and efforts needed to recover. As a result, a combination of classical security steps with post-damage activities is provided within the so-called resilience cycle (Figure 1) containing the characteristic phases of prepare-prevent-protect-respond-recover.

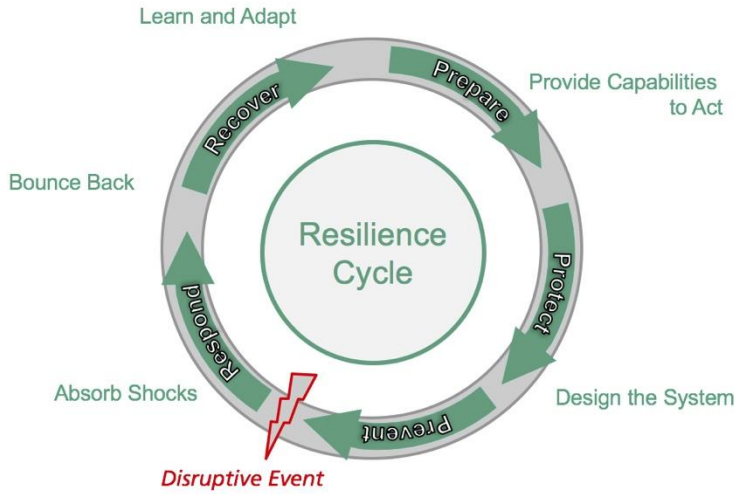

Figure 1. *Five-phases resilience-cycle*

Different measures have been derived to quantitatively assess the resilience of a given system [Tierney & Bruneau (2007), Bruneau & Reinhorn, (2006), Vugrin et al. (2014)]. If a system is expected to deliver a performance at a certain level $P_{initial}$ (see Figure 2), a disruptive event leads to a drop of this performance. The deviation from the expected standard performance, calculated as time-integral and marked as "Performance Loss" in Figure 2, can be used to asses the resilience of the system. The smaller the performance loss, the higher the level of resilience. Moreover, observing the time history of the performance of a system across the initiation of the disruptive event also allows for directly linking the phases of the resilience-cycle to this type of resilience measure.

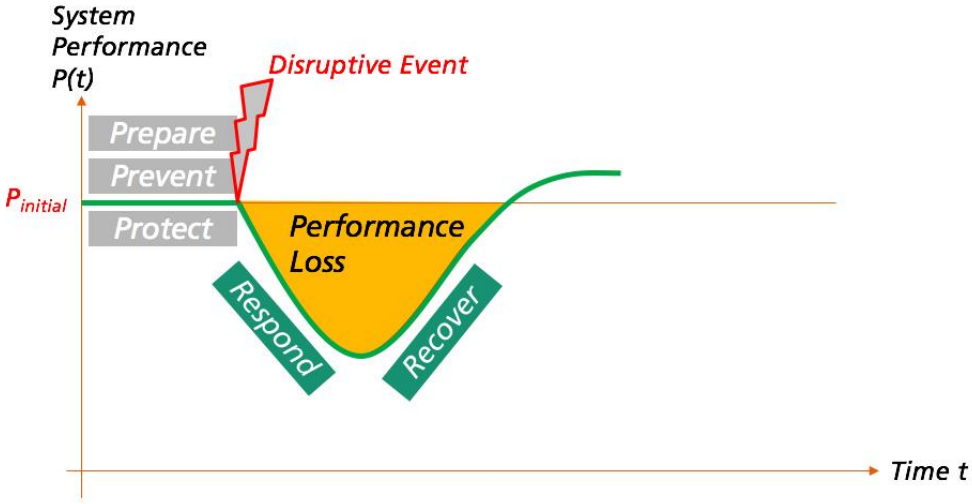

Figure 2. *Time history of system performance and performance loss as measure for resilience.*

The illustrated integration of response- and recovery-phases into engineering design is the novel contribution of resilience ontop of classical safety and security research. The time history of both the response path and the recovery branch allow for a quantitative measure of resilience.

Thus, following the paradigm of the psychologists, engineers for good reason focus on the ability of technical systems to recover from adverse conditions and to adapt based on experience. There are two characteristics of disruptive events typically challenging the resilient design of critical infrastructure.

- First, they often happen to an unexpected time or in an unanticipated way.
- Second, due to the ever rising complexity and inter-connectedness of the involved systems, their potential to initiate cascading effects is big.

As a consequence, a classical threat-based approach for the resilient configuration of a system potentially

misses its design goal if neglected sources of harm lead to a disruption.

Being used to outlay a system based on threats with given loads and boundary conditions, engineers easily find themselves in a dilemma if confronted with the task to deliver a resilient design for the unexpected.

To overcome this dilemma, a modified concept for resilience engineering incorporating the unexpected is needed. This paper discusses an approach utilizing generic damage scenarios as one option to go beyond classical threat-based concepts. Considering the topology of the resilience cycle, the new concept is an approach starting from potential consequences rather than from threats.

2 OBJECTIVES

Modeling software has become an important tool to analyze the multi-physics behavior of complex systems. Pederson et al. (2006) is often cited for their collection of existing modeling tools for interdependent infrastructures as well as for their graphical and matrix-based illustration of interdependencies between grids of different types. Propagation of failure in multi-domain grids is investigated by Hover (2011) where a mathematical methodology for an asymptotic model of cascading failure in two-domain coupled infrastructures is proposed. In his PhD thesis, Rahman (2009) addressed a wide range of grid types with a numerical formulation implemented in his infrastructure modeling and simulation framework called “I2Sim”. A detailed overview on different modeling approaches for critical infrastructure is collected and discussed in Attoh-Okine (2016).

Engineers are used to apply numerical and analytical codes to design and optimize technical systems. Given the complexity of critical infrastructures and the wide range of possible consequences after local disruptive events, a software based approach to design a systems and to investigate its behavior under critical loads is desirable.

Ideally, a design and assessment tool for resilient infrastructures would cover a range of capabilities like:

- modelling the physical components of the system including their interactions
- definition of an intended system performance
- calculation of the current system performance and comparison with expected performance
- definition of load cases resulting from specified disruptive events
- definition of generic damage scenarios, i.e. event-independent damage scenarios
- calculation of consequences to the overall system performance
- identification of critical system components and damage scenarios
- assessment of the resilience of the system
- implementation of mitigation strategies towards more resilience
- re-calculation of system resilience including mitigation strategies

With these functionalities implemented, engineers are enabled to design and assess the resilience of complex technical systems. Two characteristics of the software tool are important with respect to the before mentioned dilemma for engineers.

First, the physical and potentially multi-physical domain of the infrastructure is modelled in terms of components for which a well-known set of analytical or partial-differential equations is applicable.

Secondly, an option for event-independent, generic damage scenarios allows to better prepare for the unexpected. The ability to simulate a certain damage effect, regardless of the initiating reason, gives rise to more independence on actual events.

A new software tool, called CaESAR, incorporating some of the above mentioned functionalities has recently been developed at Fraunhofer EMI. It is designated to the simulation of multi-grid systems.

3 METHODOLOGY

3.1 Software Tool CaESAR

CaESAR is a coupled grid simulation tool, which computes cascading effects within grids and across grid borders to assess and enhance the resilience of critical infrastructures in urban areas. The overall target is to find optimized strategies for the mitigation of crisis impact on inter-connected grids. Considered are three

critical grid types – the power grid, the water grid and the mobile phone grid. For this purpose, the CaESAR tool is connected to a dashboard, where the grids are mapped in terms of nodes and arcs in a geo referenced map. From this map CaESAR takes all information to calculate sensitivities, vulnerabilities and levels of resilience of the grid system. A crisis editor is used to define a damage event.

There are two types of damage to be implemented in CaESAR:

- threat-based damage resulting from events like natural disasters and
- generic damage, defining a threat-independent damage scenario, e.g. local or global power grid failure.

Both types of damage scenarios may be defined as single ones or in combination with others. The chronological sequence and interval of single events can be defined in the crisis editor. For every single event an intensity can be set by choosing low, medium or high.

Figure 3 illustrates the major definition and computational steps within the CaESAR tool. Having defined an initial damage scenario, CaESAR simulates its propagation into the grid systems. A standard method for propagating the damage impact inside a supply grid, e.g. within the power grid, is a flow model. CaESAR also provides interfaces to use third-party propagation models. Since these third-party tools are specialized for a specific grid type, their results tend to be more accurate. For propagating the damage impact between different grids, specified physical models are used. These models also utilize geo references and a defined dependency radius estimating possible interaction between different grids.

The damage propagation is used to computationally determine the resulting damage on the entire system of grids. It starts with a sensitivity analysis taking into account probabilities of component failure and is followed by a calculation of related failure mechanisms. The result of both is the residual performance level of the coupled supply grids after the disruptions. And, thus, the input for a later calculation of the resilience level R taking into account the initial and the residual performances, respectively. The analysis is iterated with variations in the probabilities for the sensitivity analysis. With these parameter variations, critical components and failure mechanisms are identified as the ones which happen most often or with most severe consequences.

A resilience value R for the coupled grids is computed in the next step. For the before identified critical components, the CaESAR tool proposes mitigation strategies. To this end, a limited set of predefined mitigation measures is implemented. Its application leads to changes in the performance level of the overall grid system. This new level is not necessarily higher than the one without mitigation strategies. Therefore, the resilience estimation is performed once more based on the mitigated status leading to a resilience value R_M.

Finally the two resilience levels R and R_M are compared and new simulation run can be started if needed.

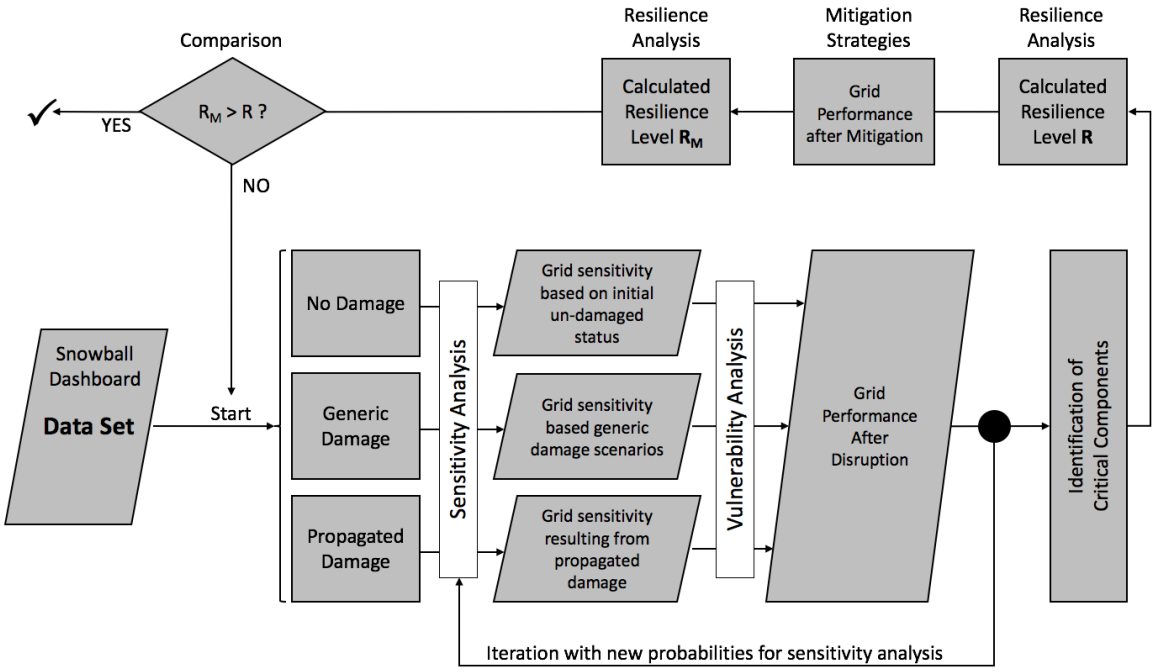

Figure 3. *Flowchart of the CaESAR tool.*

3.2 Set Up of Helsinki Urban Multi-Network Environment

An urban environment near Helsinki was chosen as an example application of the CaESAR tool. For the Helsinki grids shapefiles, which are suitable to share GIS information, were utilized. The shapefiles were attached to and presented in the map on the dashboard (Figure 4).

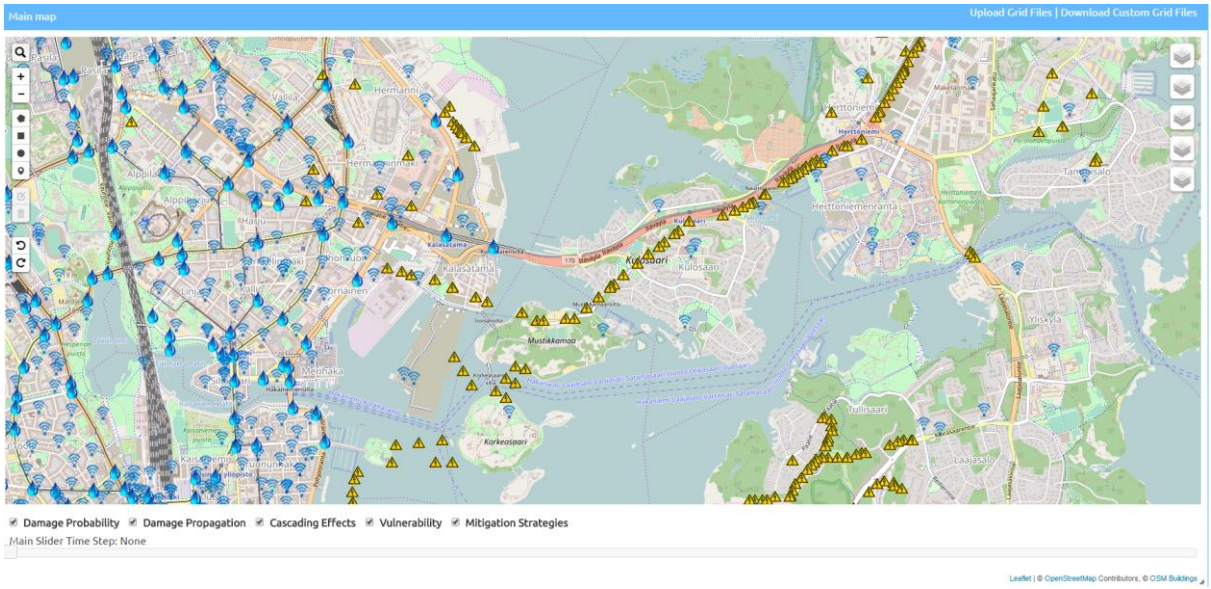

Figure 4. *Helsinki model including grids for power supply (yellow flash symbol), water (blue drop symbol) and mobile communication (blue radio symbol).*

With the dashboard, damage scenarios including threat-based and generic damage can be implemented. Illustrated in Figure 5 is the damage scenario resulting from a storm on the south coast of Finland. Using the map, the location of the storm, its start and end time as well as its impact strength are defined. Based on the grid data and the damage definition the calculation run of CaESAR starts.

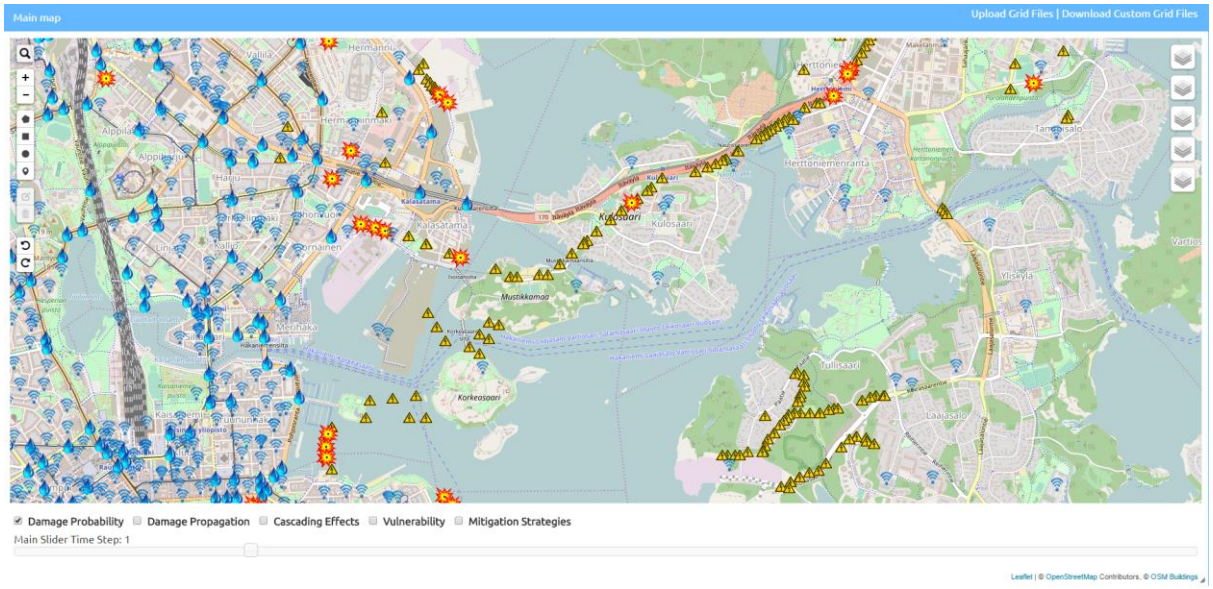

Figure 5. *Damage scenario resulting from coastal storm (red-yellow marked).*

4 RESULTS

Applied to the Helsinki scenario, the CaESAR tool provided a variety of critical components as well as mitigation strategies to increase the resilience level for the envisaged damage scenarios.

In general, there are now three major results to be gained using the CaESAR tool:

- A resilience measure for interconnected supply grids resulting from threat-based or generic damage scenarios
- Identification of the most critical components within the supply grids
- Assessment of mitigation strategies to increase the resilience of interconnected supply grids

The damages and the damage propagation based on the pre-defined chronological sequence and interval of single events during the crisis can be displayed on the map on the dashboard in several time steps.

Currently, a limited set of mitigation strategies can be applied to grid components. There are three different mitigation strategies implemented in the CaESAR tool: structural strengthening, installation of redundant components and an integration of an uninterrupted power supply. Structural strengthening and the installation of redundant components are applicable to all of the three grids. An uninterrupted power supply can be applied to water and mobile phone grid components, only.

5 DISCUSSION AND CONCLUSION

With the development of CaESAR, complex interconnected supply grid systems can be modelled. A quantitative resilience assessment based on system performances before and after a disruptive event is performed. The disruptions to the grid system can be defined as threat-based or generic.

With this approach, a first step towards damage-based and threat-independent design for resilient performance is achieved. The unexpected nature of many resilience-critical disruptive events can, thus, be addressed.

Still, CaESAR has its current short-comings. One of the next steps should be the implementation of more types of grids as components of critical infrastructure. Another field of further development is identified in more and more flexible mitigation strategies.

REFERENCES

Attoh-Okine, N.O., (2016). Resilience Engineering. Models and Analysis. Cambridge University Press, NY.

Biringer, B., Vugrin, E. & Warren, D. (2013). Critical Infrastructure System Security and Resiliency. New York: CRC Press.

Bruneau, M. & Reinhorn, A.M. (2006). Overview of the Resilience Concept. In *Proceedings of the 8th US National Conference on Earthquake Engineering*, number 2040, 2-6.

Council of the European Union (2008): COUNCIL DIRECTIVE 2008/114/EC of 8 December 20018 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In Official Journal of the European Union. L345 (pp. 75-82)

Hover, F. (2011). Degree Design of Coupled Infrastructures. International Journal of Critical Infrastructures, 7:2, 141-162.

Pederson, P., Dudenhoeffer, D., Hartley, S. & Permann, M. (2006). Critical Infrastructure Interdependency Modeling: A Survey of US and International Research. Technical report. Idaho National Laboratory, 25, 27.

Rahman, H.M.A., (2009). Modeling and Simulation of Interdependencies Between the Communication and Information Technology Infrastructure and Other Critical Infrastructure. PhD Thesis, The University of British Columbia.

Tierney, K. & Bruneau, M. (2007). A Key to Disaster Loss Reduction. *TR News*, 16-18.

Vugrin, E., Baca, M., Mitchell, M., & Stamber, K. (2014). Evaluating the Effect of Resource Constraints on Resilience of Bulk Power System with an Electric Power Restoration Model. *International Journal of Systems of Systems Engineering,* 5(1), 68-91.

Werner, E. (1977). The Children of Kauai. A longitudinal study from the prenatal period to age ten. University of Hawai'I Press.