

Chapter 6

Engineering Resilience in Critical Infrastructures

Giovanni Sansavini

Abstract This short paper is a result of several intense days of discussion following a talk at the NATO Advanced Research Workshop “Resilience-Based Approaches to Critical Infrastructure Safeguarding”, which took place in Ponta Delgada, Portugal on June 26–29, 2016. This piece elaborates on the definition of resilience, the need for resilience in critical interdependent infrastructures, and on resilience quantification. An integrated metric for measuring resilience is discussed and strategies to build resilience in critical infrastructures are reviewed. These strategies are presented in the context of the research work carried out at the Reliability and Risk Engineering Laboratory, ETH Zurich, namely, (a) planning ahead for resilience during the design phase, (b) carrying out effective system restoration, (c) quickly recovering from the minimum performance level, (d) self-healing, adaptation and control, and (e) exploiting interdependencies among infrastructures. This paper embraces a fundamentally engineering perspective and is by no means an exhaustive examination of the matter. It particularly focusing on technical aspects and does not touch upon the rich work on community resilience and the possible measures to strengthen the response of communities to disasters.

Keywords Critical infrastructures • Cascading failures • Self-healing • Adaptation • Recovery • Restoration • Robust optimization • Resilience

6.1 Defining Resilience

Resilience has emerged in the last decade as a concept for better understanding the performance of infrastructures, especially their behavior 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

G. Sansavini (✉)

Reliability and Risk Engineering Laboratory, Institute of Energy Technology,
Department of Mechanical and Process Engineering, ETH Zurich, Zürich, Switzerland
e-mail: sansavig@ethz.ch

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 2015).

The concept of resilience is still evolving and has been developing in various fields (Hosseini et al. 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 et al. 2012) (Adger 2000) (Pant et al. 2014) (Francis and 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 et al. 2016). Recently, the AR⁶A resilience framework has been proposed based on eight generic system functions, i.e. attentiveness, robustness, resistance, re-stabilization, rebuilding, reconfiguration, remembering, and adaptiveness (Heinimann 2016).

Assessing and engineering systems resilience is emerging as a fundamental concern in risk research (Woods and Hollnagel 2006) (Haimes 2009) (McCarthy et al. 2007) (McDaniels et al. 2008) (Panteli and Mancarella 2015). 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 and Hassel 2010) (Kröger and Zio 2011) as a strategy to strengthen the system response and foster graceful degradation 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.

6.2 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 (Guikema et al. 2015). 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 (Roegel et al. 2014) (Skea et al. 2011).

6.3 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

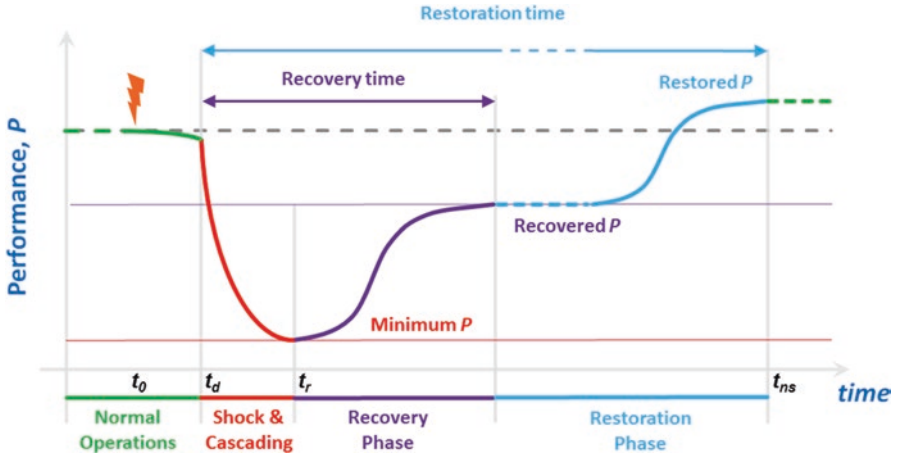


Fig. 6.1 The “resilience curve”, i.e. the performance transient after disturbance, and its phases

capacities overlap and therefore, their combined effects on the system performance are quantified by rapidity and performance loss.

Resilience can be quantified through computational experiments in which disruptions are triggered, the system performance is analyzed (Fig. 6.1), and integrated resilience metrics are computed (Nan and Sansavini 2017). 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. The selection of the appropriate *MOP* depends on the specific service provided by the infrastructure under analysis. For generality, it is assumed that the value of *MOP* is normalized between 0 and 1 where 0 is total loss of operation and 1 is the target *MOP* value in the steady phase. As illustrated in Fig. 6.1, the first phase is the original steady phase ($t < t_d$), in which the system performance assumes its target value. The second phase is the disruptive phase ($t_d \leq t < t_r$), in which the system performance starts dropping until reaching the lowest level at time t_r . During this phase, the system absorptive capability can be assessed by identifying appropriate measures. *Robustness* (or *Resistance*) (R) is a measure to assess this capability, which quantifies the minimum *MOP* value between t_d and t_{ns} :

$$R = \min \{ MOP (t) \} \text{ (for } t_d \leq t \leq t_{ns} \text{)} \tag{6.1}$$

where t_d represents the time when the system is in disruptive phase and t_{ns} represents the time when the system reaches the new steady phase. This measure is able to identify the maximum impact of disruptive events; however, it is not sufficient to reflect the ability of the system to absorb the impact. Two additional complementary measures are further developed: *Rapidity* (RAP_{DP}) and *Performance Loss* (PL_{DP})

during disruptive phase. The measure *Rapidity* can be approximated by the average slope of the *MOP* function.

$$RAPI_{DP} = \frac{MOP(t_d) - MOP(t_r)}{t_r - t_d} \quad (6.2)$$

To improve the accuracy of the estimation of *RAPI*, ramp detection is applied to quantify the average slope (Ferreira et al. 2013). According to (Kamath 2010) and (Zheng and Kusiak 2009), a ramp is assumed to occur if the difference between the measured value at the initial and final points of a time interval Δt is greater than a predefined ramping threshold value:

$$\frac{MOP(t + \Delta t) - MOP(t)}{\Delta t} > \Delta X_{ramp} \quad (6.3)$$

where ΔX_{ramp} represents the predefined ramping threshold value. The system rapidity can then be calculated as the average of slope of each ramp:

$$RAPI = \frac{\left| \sum_{i=1}^K \frac{MOP(t_i) - MOP(t_i - \Delta t)}{\Delta t} \right|}{K} \quad (6.4)$$

where K represents the number of detected ramps and $MOP(t_i)$ represents the *MOP* value at the i -th detected ramp. Compared to (2), this method better captures the speed of change in the system performance during disruption and recovery phases. According to this approach, the rapidity during disruptive phase can be calculated as:

$$RAPI_{DP} = \frac{\left| \sum_{i=1}^{K_{DP}} \frac{MOP(t_i) - MOP(t_i - \Delta t)}{\Delta t} \right|}{K_{DP}} \quad (\text{for } t_d \leq t_i < t_r) \quad (6.5)$$

where K_{DP} represents number of detected ramps during the disruptive phase.

The *performance loss* in the disruptive phase (PL_{DP}), using the system illustrated in Fig. 6.1 as an example, can be quantified as the area of the region bounded by the *MOP* curve before and after occurrence of the negative effects caused by the disruptive events, i.e. between t_d and t_r which is referred to as the system impact area:

$$PL_{DP} = \int_{t_d}^{t_r} (MOP(t_o) - MOP(t)) dt \quad (6.6)$$

Where t_o represents the time when the system is in original steady phase. A new measure, i.e. the *time averaged performance loss (TAPL)*, is introduced. Compared to *PL*, *TAPL* considers the time of appearance of negative effects due to disruptive events up to full system recovery and provides a time-independent indication of both adaptive and restorative capabilities as responses to the disruptive events. $TAPL_{DP}$ in the disruptive phase ($t_d \leq t < t_r$) can be calculated as:

$$TAPL_{DP} = \frac{\int_{t_d}^{t_r} (MOP(t_o) - MOP(t)) dt}{t_r - t_d} \quad (6.7)$$

The third phase is the recovery phase ($t_r \leq t < t_{ns}$), in which the system performance increases until the new steady level. During this phase, the system adaptive and restorative capability can be assessed by developing appropriate measures: *rapidity (RAPI_{RP})*, *performance loss (PL_{RP})* and *time average performance loss (TAPL_{RP})*.

$$RAPI_{RP} = \frac{\left| \sum_{i=1}^{K_{RP}} \frac{MOP(t_i) - MOP(t - \Delta t)}{\Delta t} \right|}{K_{RP}} \quad (\text{for } t_r \leq t_i < t_{ns}) \quad (6.8)$$

where K_{RP} represents the number of detected ramps in recovery phase.

$$PL_{RP} = \int_{t_r}^{t_{ns}} (MOP(t_o) - MOP(t)) dt \quad (6.9)$$

$$TAPL_{RP} = \frac{\int_{t_r}^{t_{ns}} (MOP(t_o) - MOP(t)) dt}{t_{ns} - t_r} \quad (6.10)$$

The fourth phase is the new steady state ($t \geq t_{ns}$), in which system performance reaches and maintains a new steady level. As seen in Fig. 6.1, the newly attained steady level may equal the previous steady level or reach a lower level. It should be noted that the new steady state may even be at a higher level than the original one. In order to take this situation into consideration, a simple quantitative measure *Recovery Ability (RA)* is developed:

$$RA = \frac{\left| MOP(t_{ns}) - MOP(t_r) \right|}{\left| MOP(t_o) - MOP(t_r) \right|} \quad (6.11)$$

Different system phases and related system capabilities are summarized in Table 6.1.

Table 6.1 Summary of different resilience phases

Phases	Time scope	Transition point	Capabilities (features)	Measurements
Original steady phase	$t < t_D$		Susceptibility	Susceptibility
Disruptive phase	$t_D \leq t < t_R$	TRNS(D)	Absorptive capability	R
				RAPIDP
Recovery phase	$t_R \leq t < t_{NS}$	TRNS(R)	Adaptive capability	RAPIRP
			Restorative capability	PLRP
New steady phase	$t \geq t_{NS}$	TRNS(NS)	Recovery capability	RA

R Robustness, *RAPIDP* Rapidity in disruptive phase, *PLDP* Performance Loss in disruptive phase, *RAPIRP* Rapidity in recovery phase, *PLRP* Performance Loss in recovery phase, *RA* Recovery ability

6.3.1 The Integrated Resilience Metric

Although the measurements introduced and discussed in Sect. 6.6.3 are useful in assessing the system behavior during and after disruptive events, an integrated metric with the ability of combining these capabilities is needed in order to assess system resilience with an overall perspective and to allow comparisons among different systems and system configurations. The basic idea of incorporating various resilience capacities into one metric has been proposed by Francis and Bekera to develop resilience factor (Francis and Bekera 2014). The idea is also supported by (McDaniels et al. 2008). Therefore, the resilience metric (*GR*) is proposed, which integrates the previous measures:

$$\begin{aligned}
 GR &= f(R, RAPI_{DP}, RAPI_{RP}, TAPL, RA) \\
 &= R \times \left(\frac{RAPI_{RP}}{RAPI_{DP}} \right) \times (TAPL)^{-1} \times RA
 \end{aligned}
 \tag{6.12}$$

where $TAPL_{DP}$ and $TAPL_{RP}$ have been combined into one *TAPL* measure

$$\left(\frac{\int_{t_d}^{t_{ns}} [MOP(t_0) - MOP(t)] dt}{t_{ns} - t_d} \right)$$

in order to incorporate effects of total performance loss during disruptive and recovery phases.

The functional form of the proposed resilience metric assumes that robustness *R*, recovery speed *RAPI_{RP}* and recovery ability *RA* have a positive effect on resilience, and, conversely, performance loss *TAPL* and loss speed *RAPIDP* have a negative effect. To compile the integrated metric (12), no weighting factor is assigned to the measures so that no bias is introduced, i.e. they contribute equally to resilience. *GR* is consistent with the definition proposed in Sect. 6.6.1:

1. If the system is more capable of resisting a disruptive event or force (large *R*, small *RAPIDP*), the system is more resilient (large *GR*).

2. If the system is more capable of reducing the magnitude and duration of deviation of its performance level between original state and new steady state (small $TAPL$, large $RAPL_{RP}$), the system is more resilient (large GR).
3. Additionally GR also incorporate the possibility of improvement of the system performance after the occurrence of the disruptive event. If the new performance level is larger than the original (large RA), the system is more resilient (large GR).

GR is a non-negative metric and its value equals zero in the following relevant cases:

1. System performance level drops to zero after the disturbance ($R = 0$).
2. After the disturbance, system performance immediately drops to its lowest level ($RAPL_{DP} \rightarrow \infty$, i.e. no absorptive capability).
3. System performance never increases past the lower level, R , which is the new steady phase ($RAPL_{DP} = 0$, i.e. no adaptive and restorative capability).

GR is dimensionless and is most useful in a comparative manner, i.e. to compare the resilience of various systems to the same disruptive event, or to compare resilience of same system under different disruptive events. This approach of measuring system resilience is neither model nor domain specific. For instance, historical data can also be used for the resilience analysis. It only requires the time series that represents system output during whole time period. In this respect, the selection of the MOP is very important.

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 recognized, and research works have developed. Historically, knowledge-based approaches have been applied to improve the understanding of infrastructures resilience (McDaniels et al. 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 et al. 2016), and hybrid approaches (Nan et al. 2016).

Approaches to quantify system resilience should be able to

- capture the complex behavior 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 analyzing the resilience by performing in-depth experiments is still missing.

6.4 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:

6.4.1 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.

In (Fang and Sansavini 2017), the combination of capacity expansion and switch installation in electric systems that ensures optimum performance under nominal operations and attacks is studied. The planner-attacker-defender model is adopted to develop decisions that minimize investment and operating costs, and functionality loss after attacks. As such, the model bridges long-term system planning for transmission expansion and short-term switching operations in reaction to attacks. The mixed-integer optimization is solved by decomposition via two-layer cutting plane algorithm. Numerical results shows that small investments in transmission line switching enhance resilience by responding to disruptions via system reconfiguration (Fig. 6.2). Sensitivity analyses show that transmission planning under the assumption of small-scale attacks provides the most robust strategy, i.e. the minimum-regret planning, if many constraints and limited investment budget affect

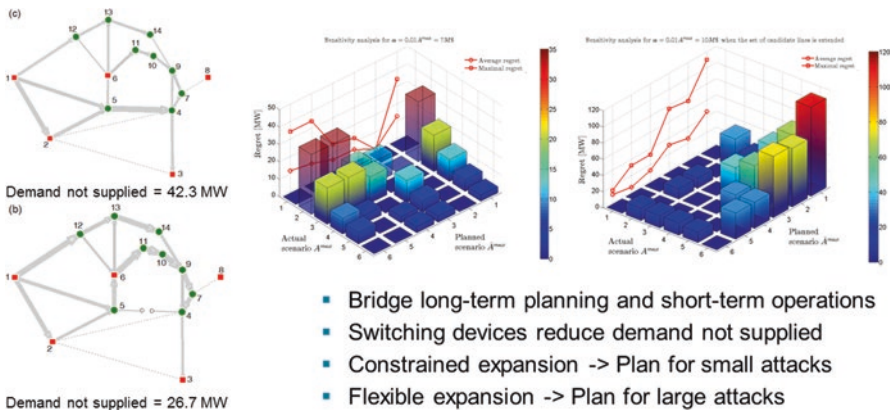


Fig. 6.2 Integrated planning of system expansion and recovery devices against uncertain attack scenarios (Fang and Sansavini 2017)



Fig. 6.3 The heat map of the cumulative economic losses at each canton of Switzerland due to propagation of cascading failures in the electric power system (Li et al. 2015)

the planning. On the other hand, the assumption of large-scale attacks provides the most robust strategy if the planning process involves large flexibility and budget.

6.4.2 Self-Healing, Adaptation and Control

Graceful degradation: the system cannot be designed 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 (Li and Sansavini 2016), 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 (Fig. 6.3).

6.4.3 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.

System restoration and its contribution to the resilience of infrastructure networks following disruptions have attracted attention in recent years. Optimization approaches usually guide the identification and scheduling of restoration strategies for rapid system functionality reestablishment under limited resources. Most of the related studies rely on deterministic assumptions such as complete information of resource usage and deterministic duration of the repair tasks. However, restoration activities are subject to considerable uncertainty stemming from subjective expert judgment and imprecise forecasts that may render the scheduling solution obtained by a deterministic approach suboptimal or even infeasible under some uncertainty realizations. Restoration planning and scheduling under uncertainty can be investigated within a credibility-based fuzzy mixed integer programming (PMIP) approach, in which the imprecise parameters are modelled by fuzzy numbers (Fang and Sansavini 2016). To solve the proposed fuzzy optimization problem, an interactive fuzzy solution technique is utilized which provides the decision maker (DM) the flexibility to consider two significant factors when making decision: the degree of achievement of his/her aspiration level and the risk of violation of the constraints. A computational experiment involving the Swiss high voltage electric power transmission network demonstrates the significance and applicability of the developed approach for DM to determine efficient restoration actions aimed to enhancing system resilience. Generally, the system restoration curves, i.e. the system performance levels evolving over time, show that decreasing the degree of feasibility of the constraints results a faster system restoration (Fig. 6.4).

6.4.4 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, and display the anti-fragility property (Taleb 2012; Aven 2015).

A system is anti-fragile if its performance improves as the result of exposure to stressors, shocks or disruptions. This behavior is typical of complex systems and it is not usually exhibited by engineered technical systems. In fact, technical systems can display anti-fragility when new investments are allocated, e.g. after disasters. In post-disaster restoration planning of infrastructure networks, the possibility of combining the construction of new components and the repair of failed ones can lead to anti-fragile behavior. The strategic goal is to determine the optimal target system structure so that the performance of the target system is maximized under the

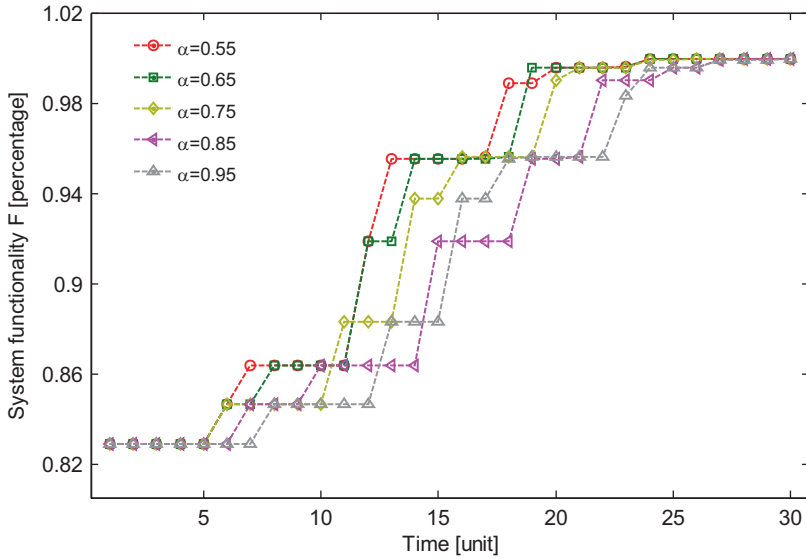


Fig. 6.4 System restoration curves for five different feasibility levels of the solution vector, i.e. the set of decision variables concerning the restoration process

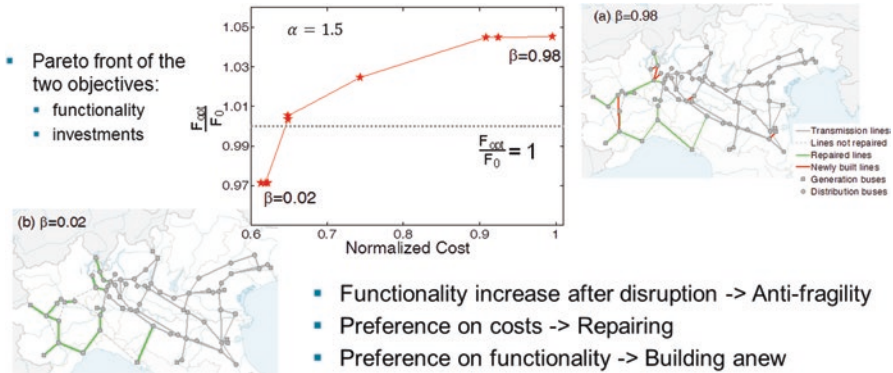


Fig. 6.5 Optimum restoration by repairing and building anew

constraints of investment cost and network connectivity. The problem can be formulated as a mixed-integer binary linear programming (MILP). The preliminary results (Fig. 6.5) show that the restored network can achieve an improved functionality as compared to the original network if new components are constructed and some failed components are not repaired, even when the former is much more expensive than the latter. Therefore, different investment allocations schemes define whether an infrastructure network is fragile or anti-fragile. In particular, the tested infrastructure exhibits anti-fragile behavior even for restoration investments that amount at 62% the cost of complete repair. Furthermore, antifragility provides an opportu-

nity for the system to meet future service demand increase, and a perspective under which disruptions can be seen as chances for system performance improvements.

6.4.5 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.

Cyber interdependencies are pervasive in critical infrastructures (CIs) and particularly in electric power networks, which are dependent on information and communications technology (ICT), e.g., supervisory control and data acquisition (SCADA) systems, to transmit measurements signals to control centers and to dispatch control signals to actuators. The requirements towards ICT to transmit these signals with tolerable communication delays for timely balancing of power demand and supply have increased due to changes in the operating conditions of electric power networks. On the one hand, its operating conditions are pushed closer to its stability limits due to amplified loading conditions. On the other hand, the increasing share of distributed inverter-connected renewable energy, e.g., wind and PV, on the distribution level has led to a decrease in the inertia and an increase in the volatility in the power grid further reducing its stability margins. Under these conditions, severe consequences, e.g. system-wide blackouts, can be caused by disturbances in the electric grid. In the face of these challenges, ICT is expected to turn the current electric grid into a “smart grid” in order to assure reliable, efficient and secure operations of the electric grid. An application that benefits from the ICT in power systems is grid splitting, also referred to as controlled islanding, which relies on real-time system-wide measurements to enable the detection and recovery from failures in real time, i.e., by applying system topology changes. Grid splitting is a special protection scheme that separates a power system into synchronized islands in a controlled manner in response to an impending instability, i.e., generator rotation desynchronization triggered by a component fault. By appropriately disconnecting transmission lines, severe consequences, e.g., system-wide blackouts, are mitigated through the formation of stable islands. The successful application of grid splitting depends on the communication infrastructure to collect system-wide synchronized measurements and to relay the command to open line switches. Grid splitting may be ineffective if communication is degraded and its outcome may also depend on the system loading conditions. The effects of degraded communication and load variability on grid splitting are investigated in (Tian and Sansavini 2016). To this aim, a communication delay model is coupled with a transient electrical model and applied to the IEEE 39-Bus and the IEEE 118-Bus Test System. Case studies show that the loss of generator synchronism following a fault is mitigated by timely splitting the network into islands. On the other hand, the results show that communication delays and increased network flows can degrade the performance of

grid splitting. The developed framework enables the identification of the requirements of the dedicated communication infrastructure for a successful grid-splitting procedure.

Acknowledgments The author acknowledges the CTI – Commission for Technology and Innovation (CH), and the SCCER-FURIES – Swiss Competence Center for Energy Research – Future Swiss Electrical Infrastructure, for their financial and technical support to the research activity presented in this paper.

Further Suggested Readings

- Adger W (2000) Social and ecological resilience: are they related? *Prog Hum Geogr* 24:347–364
- Aven T (2015) The concept of antifragility and its implications for the practice of risk analysis. *Risk Anal* 35(3):476–483
- Bruneau M, Chang SE, Eguchi RT, Lee GC, O’Rourke TD, Reinhorn AM (2003) A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra* 19:733–752
- Bueno NP (2012) Assessing the resilience of small socio-ecological systems based on the dominant polarity of their feedback structure. *Syst Dyn Rev* 28:351–360
- Fang Y, Sansavini G (2016) Optimum post-disruption restoration for enhanced infrastructure network resilience: a possibilistic programming approach. In: *Proceedings of ESREL 2016 European Safety and Reliability Association annual conference*. Glasgow, UK, pp 25–29
- Fang YP, Sansavini G (2017) Optimizing power system investments and resilience against attacks. *Reliab Eng Syst Saf* 159:161–173
- Ferreira C, Gama J, Miranda V, Botterud A (2013) Probabilistic ramp detection and forecasting for wind power prediction. In: Billinton R, Karki R, Verma AK (eds) *Reliability and risk evaluation of wind integrated power systems*. Springer India, India, pp 29–44
- Fiksel J (2003) Designing Resilient, Sustainable Systems. *Environ Sci Technol Environ Sci Technol* 37:5330–5339
- Francis R, Bekera B (2014) A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliab Eng Syst Saf* 121:90–103
- Gao J, Barzel B, Barabási A-L (2016) Universal resilience patterns in complex networks. *Nature* 18:307–312
- Guikema S, McLay L, Lambert JH (2015) Infrastructure Systems, Risk Analysis, and Resilience—Research Gaps and Opportunities. *Risk Anal* 35(4):560–561
- Haimes YY (2009) On the Definition of Resilience in Systems. *Risk Anal* 29:498–501
- Heinimann HR (2016) A generic framework for resilience assessment. In *IRGC (2016). Resource guide on resilience*. Lausanne: EPFL International Risk Governance Center. v29-07-2016
- Holling CS (1973) Resilience and stability of ecological systems. *Annu Rev Ecol Syst* 4:1–23
- Hosseini S, Barker K, Ramirez-Marquez JE (2016) A review of definitions and measures of system resilience. *Reliab Eng Syst Saf* 145:47–61
- Johansson J, Hassel H (2010) An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliab Eng Syst Saf* 95:1335–1344
- Kamath C (2010) Understanding wind ramp events through analysis of historical data. *Transmission and distribution conference and exposition, IEEE PES 2010*; 1–6.
- Kröger W, Zio E (2011) *Vulnerable Systems*. Springer-Verlag, London
- Li B, Sansavini G (2016) Effective multi-objective selection of inter-subnetwork power shifts to mitigate cascading failures. *Electr Power Syst Res* 134:114–125

- Li B, Barker K, Sansavini G (2015) Measuring the societal and multi-industry impact of cascading failures in power systems, Proceedings of ESREL 2015 European Safety and Reliability Association Annual Conference, 7–10 September 2015. Zurich, Switzerland, pp 4445–4453
- McCarthy J, Pommering C, Perelman L, Scalingi P, Garbin D, Shortle, J (2007) Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience. George Mason University, Fairfax, pp 97–109
- 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. *Glob Environ Chang* 18:310–318
- Nan C, Sansavini G (2017) A quantitative method for assessing resilience of interdependent infrastructures. *Reliab Eng Syst Saf* 157:35–53
- Nan C, Sansavini G, Kröger W (2016) Building an integrated metric for quantifying the resilience of interdependent infrastructure systems. In: Panayiotou C, Ellinas G, Kyriakides E, Polycarpou M (eds) Critical information infrastructures security. CRITIS 2014. Lecture Notes in Computer Science, vol 8985. Springer, Cham
- Ouyang M, Wang Z (2015) Resilience assessment of interdependent infrastructure systems With a focus on joint restoration modeling and analysis. *Reliab Eng Syst Saf* 141:74–82
- Ouyang M, Dueñas-Osorio L, Min X (2012) A three-stage resilience analysis framework for urban infrastructure systems. *Struct Saf* 36–37:23–31
- Pant R, Barker K, Zobel CW (2014) Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliab Eng Syst Saf* 125:92–102
- Panteli M, Mancarella P (2015) Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Syst J* 99:1–10
- Paté-Cornell E (2012) On “Black Swans” and “Perfect Storms”: risk analysis and management when statistics are not enough. *Risk Anal* 32:1823–1833
- Roege PE, Collier ZA, Mancillas J, McDonagh JA, Linkov I (2014) Metrics for energy resilience. *Energy Policy* 72:249–256
- Skea J, Chaudry M, Ekins P, Ramachandran K, Shakoor A, Wang X (2011) A resilient energy system. In: Paul Ekins JS (ed) *Energy 2050: making the transition to a secure low-carbon energy system*. Taylor & Francis, Hoboken, pp 145–186
- Taleb NN (2012) *Anti-Fragile*. Penguin, London
- Tian D, Sansavini G (2016) Impact of degraded communication on interdependent power systems: the application of grid splitting. *Electron Spec Issue Smart Grid Cyber Secur* 5(3):49
- Woods DD (2015) Four concepts for resilience and the implications for the future of resilience engineering. *Reliab Eng Syst Saf* 141:5–9
- Woods DD, Hollnagel E (2006) *Resilience Engineering: Concepts and Precepts*. CRC Press, Boca Raton
- Zheng H, Kusiak A (2009) Prediction of wind farm power ramp rates: a data-mining approach. *J Sol Energy Eng* 131:31011