ETH zürich

Wie wird die digitale Stromversorgung resilienter?

Reflexion der präsentierten Ergebnisse

Dr.-Ing. Wolfgang Kröger, Prof. ETH Zurich
Former Executive Director ETH Risk Center

Berlin, 10. November 2017

Reflexion – auf den Punkt gebracht

- Glückwunsch zu dem Fortschritt und Geschaffenen
- Weitgehende Übereinstimmung mit der Angemessenheit des methodischen Ansatzes und den ausgewiesenen Ergebnissen einschliesslich des „vulnerability ratings“
- Dennoch ein paar „kritische“ Anmerkungen zu:

  Begriffliche Unschärfen

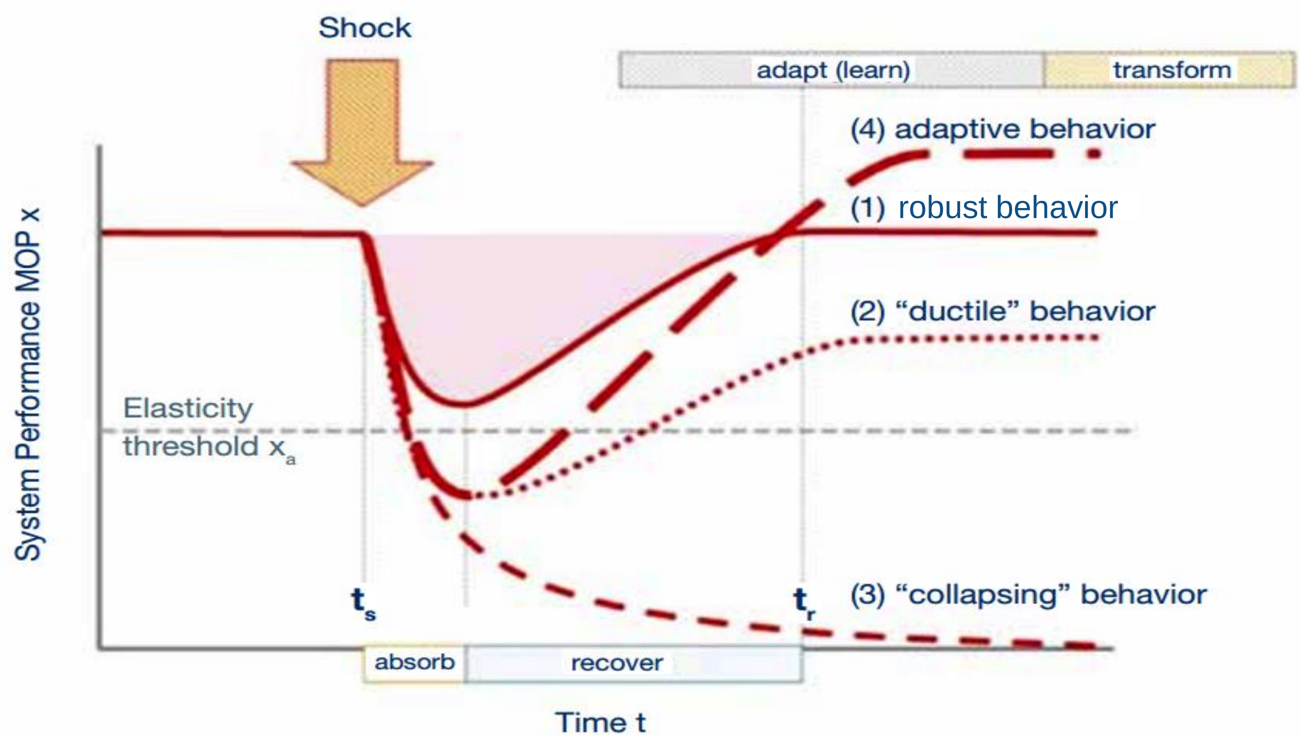
  Qualitativer Ansatz / Stand Analysetechnik

  Bedeutung des Gestaltungselements „Granularität“

  „Mankos“/Anregungen

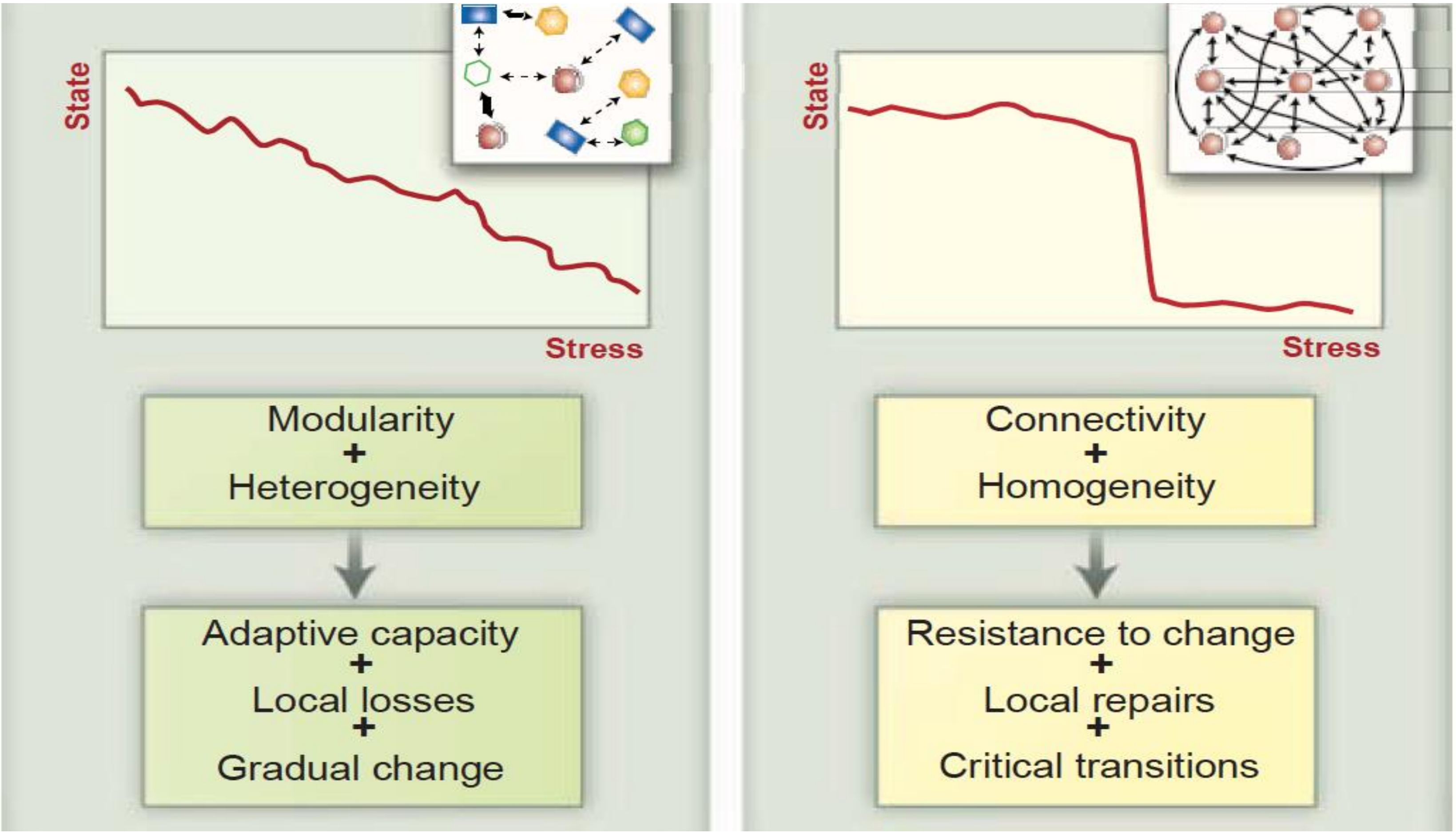
From Pure System „hardening“ to Post-Shock „soft landing“ Resilience Strategy – extentended definition und illustration

Ability of a system to resist/absorb the adverse effects of a disruptive force (either sudden or creeping) with decreasing performance but without collapsing, and the abilitity and speed to recover and return to an appropriate functionality – by adapting through self-organization and learning and eventually bouncing back or transforming into a different state [Kröger, 2017]



Patterns of resilient response behaviors (Courtesy: Heinimann, 2014)

What do we learn from analytical tools?



The connectivity and homogeneity of the units affect the way in which distributed systems with local alternative states respond to changing conditions (“stress”) [Streffer et al., Science, 2012]

„Mankos" und Anregungen

- Put more emphasis on potential „new" (common cause) failure modes within commonly used commercial soft- and hardware and on „manipulation" as cyber attack mode.
- Consider German transmission grid as part of the highly-meshed ENTSO-E grid, governed by the „Operation Handbook", and address more clearly potential effects of fragmented control on grid stability.
- Strive to ensure impact factors by use of quantitative analyses/simulations and contribute to the future development of suitable methods and frameworks.

Additional slides

Defining Key Terms Related to Critical Infrastructure

- Critical infrastructure: Assets that are essential for the functioning of a society and economy /Vatn, Hokstad, Utne, '12/
- Risk: Traditionally, property of a system being analysed comprising the probability whether undesired events (*event scenarios*) will occur or not and the consequences indicating their severity /Vatn, Hokstad, Utne, '12/
- Reliability: Probability that an electric power grid (*technical system*) can perform a required function under given conditions for a given time interval /IEC/
- Vulnerability: Drop in performance when a disruptive event emerges /Ouyang, Kun, '14/
- Resilience: Ability of a system (*or system-of-systems*) to react and recover from unanticipated disturbances and events /Hollnagel et al., '06/…to resist/absorb initial adverse effects of a disruptive (shocking or creeping) internal or external event/force (stressor) and the time/speed at which it is able to return to an appropriate functionality/equilibrium /Kröger, '14; FRS team work in progress/
- Complexity: Inherent characteristic of a system endorsed by tight coupling and interdependencies completed with emergent behavior and self-organization /Wikipedia/

Paradigm Shift from Pure Prevention to Resilience: Some Suggested Guiding Principles

- Seize resource buffers, functional and physical redundancy/diversity
- Ensure robust topology against internal and (areal) external events, stochastic or targeted (balance interconnectedness, identify critical nodes, avoid super spreaders), physcially protect critical components and bottlenecks
- Balance complexity (avoid too little – too high) as well as automation and human control (automation for high reliability, humans-in-loop for unforeseen)
- Prevent them from spreading failures and sudden changes, optimize structure (degree, connectivity, hybrid solutions) against random failures and malicious attacks
- Ensure operation within safety margins, perform decoupling (islanding) strategies
- Span hazards and threats and associated scenarios to all imaginable, strive for “predictability” by applying new knowledge and advance modelling techniques