ETH zürich

Kritische Infrastrukturen: Umgang mit Komplexität, Risiko und Resilienz

Wolfgang Kröger, ETH Zürich

Verein Risiko & Sicherheit, Frühlingsanlass 2019, Luzern

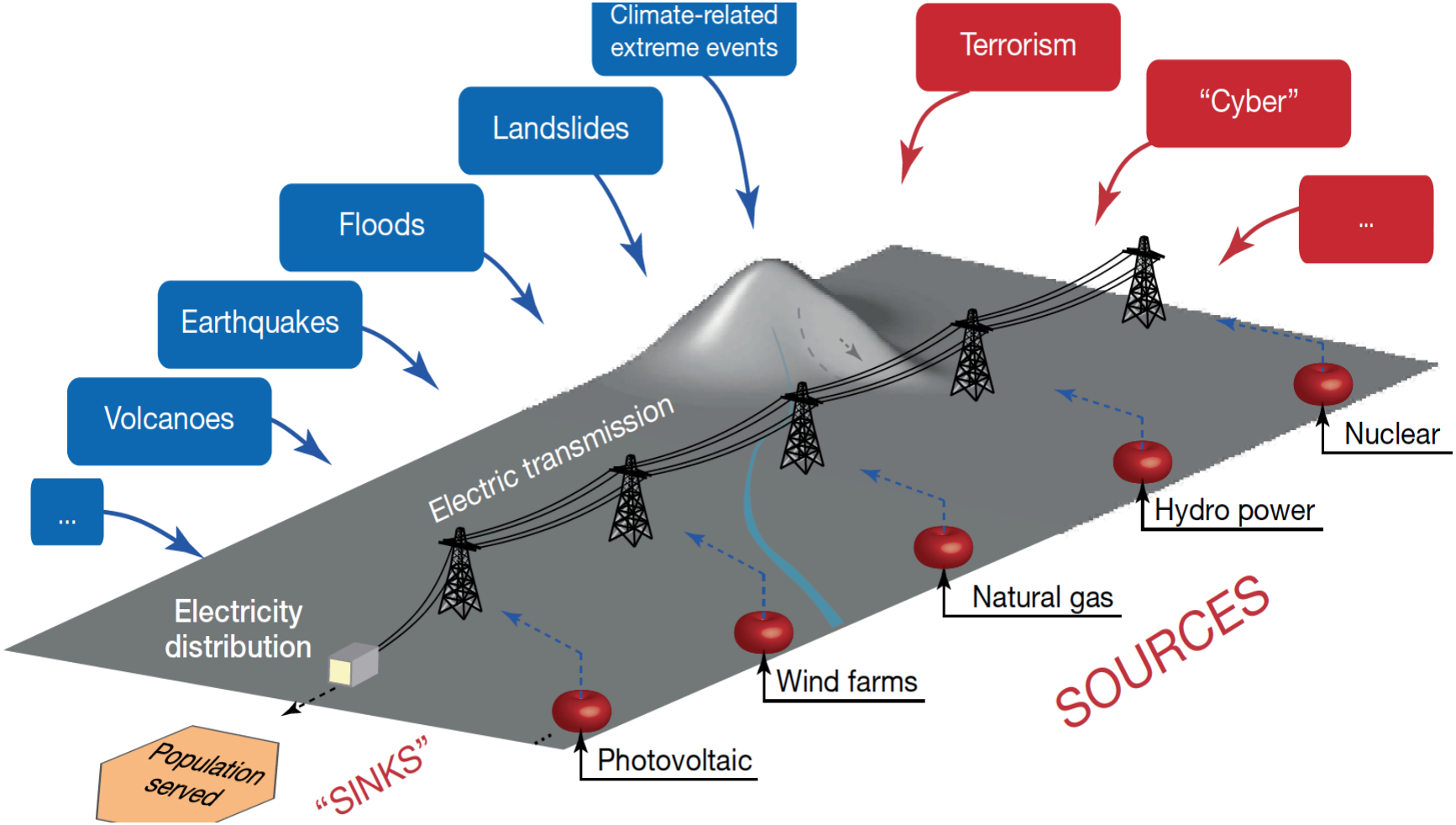
Characteristics of Critical Infrastructures (I)

- Essential for vital societal functions; their debilitation would have impact on our society (well-being) and economy.
- Develop into a „system-of-systems“ due to growing integration and connectedness, mainly driven by digitalization and globalization.
- Must be understood as socio-(ecological)-technical system, characterized by multiple factors, due to strong interactions with humans and the operating environment.
- Mostly developed uncontrolled, were subject to evolution and growth mechanisms, operate beyond their initial design parameters, often close to their limits.

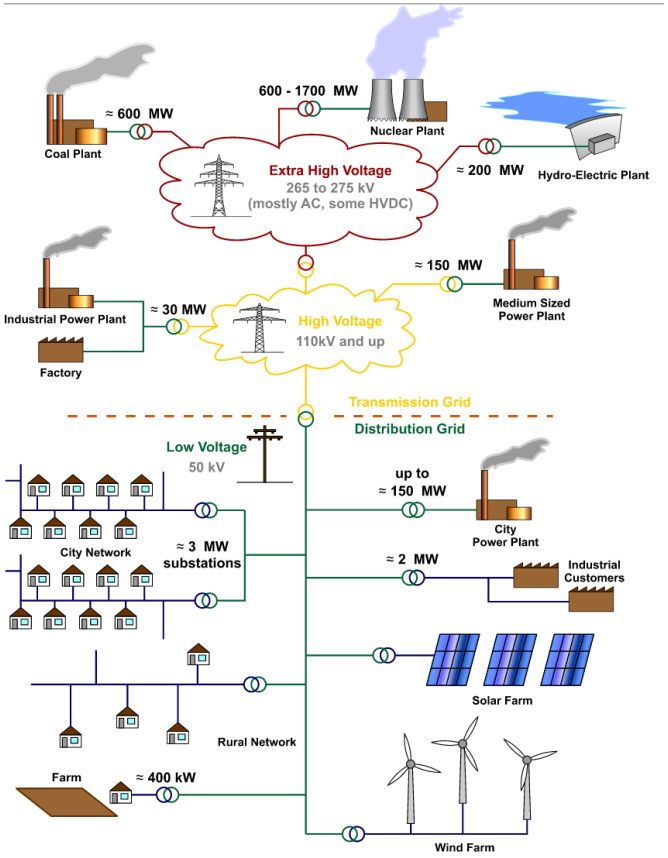
Characteristics of Critical Infrastructures (II)

- Composed of many components, interacting in multiple ways in a non-homogeneous networked structure, which leads to structural and dynamic complexity.
- Large-scale, open systems with critical elements spatially concentrated and loosely protected, exposed to a widening set of hazards/threats of different types including extreme weather, component aging, intentional attacks.
- Subject to ever changing conditions and domains, the „Energiewende“ as most prominent example including replacement of monopolis by intricate market structure.

Representation of the Electricity Supply Network



Einspeiseebenen des heutigen Stromnetzes



- Einspeisung auf unterschiedlichen Spannungsniveaus
- Reduzierung rotierender Massen (Turbogeneratoren) zur Frequenz-kontrolle
- Trennung zwischen Erzeugung und Verbrauch teilweise aufgehoben
- Regionale Sicht sinnvoll, aber als Teil des europäischen Verbundnetzes mit zunehmenden grenzüberschreitenden Flüssen zu verstehen

The European Transmission System: Highly Meshed and Evolving

Key figures (2015):

- 5 synchronous large areas
- Network of 41 TSOs from 34 countries
- Serving 534 million citizens – 3’278 TWh consumption, 15% cross-border
- 314’333 km of high voltage lines

Main goals:

- Security of supply, reliable operation
- Efficient and competitive market
- Optimal management and sound technical evolution of the network

Protection against:

- Cascade tripping
- Voltage or frequency collapse
- Loss of synchronism

Framing Complexity: No Absolute Definition

- Characterization by „something with many components, interacting with each other in multiple ways, culminating in a higher order of emergence greater than the sum of its parts“ (wikipedia).
- Both complex (lat.:woven) and complicated (lat.:folded) systems entail a large number of inerconnected components, organized in a hiercharchy of subsystems – complexity is characterized by <u>interdependencies</u>, a complicated system by its layers.

Framing Complexity: Elements, Attributes, Behaviors

An (adaptive) complex system (stock markets, power grids, www)

- consists of a large but finite number of interrelated parts, that interact with each other in multiple ways; parts can be either physical, human, logical or contextual;
- tends to dynamic and non-linear behavior, triggering disturbances often accelerate and cascade, a change of output is not proportional to change of input;
- often shows emergent behavior, i.e. larger entities exhibiting properties the smaller ones do not have;
- exhibits positive feedback loops, i.e. no damping of instabilities, and possible critical tipping points, depending on topology and structure;
- is influenced by and adapts to its environment and managed by various kinds of actors, often with different rationalities/objectives.

Framing Complexity: Boundaries, Influencing Factors

- Boundaries need to be defined, together with the granularity of the system, can reach to micro (local/components), macro (areal/ entire system) or large-scale (global/system-of-systems) level.
- There is a variety of key influencing factors, ranging from purely technical (quality, stress, age) to contextual (operational, organizational, human behavioral, political), at different levels and time scales.

Testing Theory with Reality: Evaluation of Major Blackouts and Revealed Patterns

Blackout		Loss [GW]	Duration [h]	People affected	Main causes
Aug. 14, 2003	Great Lakes, NYC	~ 60	~ 16	50 Mio	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighbouring TSOs
Sep. 28, 2003	Italy	~ 30	up to 18	56 Mio	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs
Nov. 4, 2006	Western Europe (planned line cut off)	~ 14	~ 2	15 Mio. Households	High load flow D-NL-maintenance, violation of the N-1 rule, poor inter-TSO coordination
Mar. 11, 2011	Northern Honshu, Japan	~21	days	40 Mio.	Grid destruction by earthquake & tsunami/ supply gap/rolling blackouts
Jan. 26, 2015	Pakistan	~ 9	up to 8	140 Mio.	*Militant attack

- Failures/disruptions may accelerate and cascade into other infrastructure, causing costs of a few percent of GDP
- “Soft factors”, notably organizational and contextual, prevail over technical failures and deserve special attention
- Crucial role of natural hazards (extreme weather, geological), expected to increase due to climate change; increasing concern about malicious physical or cyber attacks

Testing Theory with Reality: 4 Nov 2006 System Split and Associated Complexity

Background

- TSOs not aware of different protection settings on the two sides of the line
- Busbar Borken splitted (maintenance)
- High wind infeed in northen Germany, high load flow to the Netherlands.
- Rescheduled line outage, neighbouring TSOs not informed, congestion forecast not updated.

Sequence of events

Conneford-Diele lines switch off

↓ 21:39

No N-1 security; no load flow calculation by TSO

↓

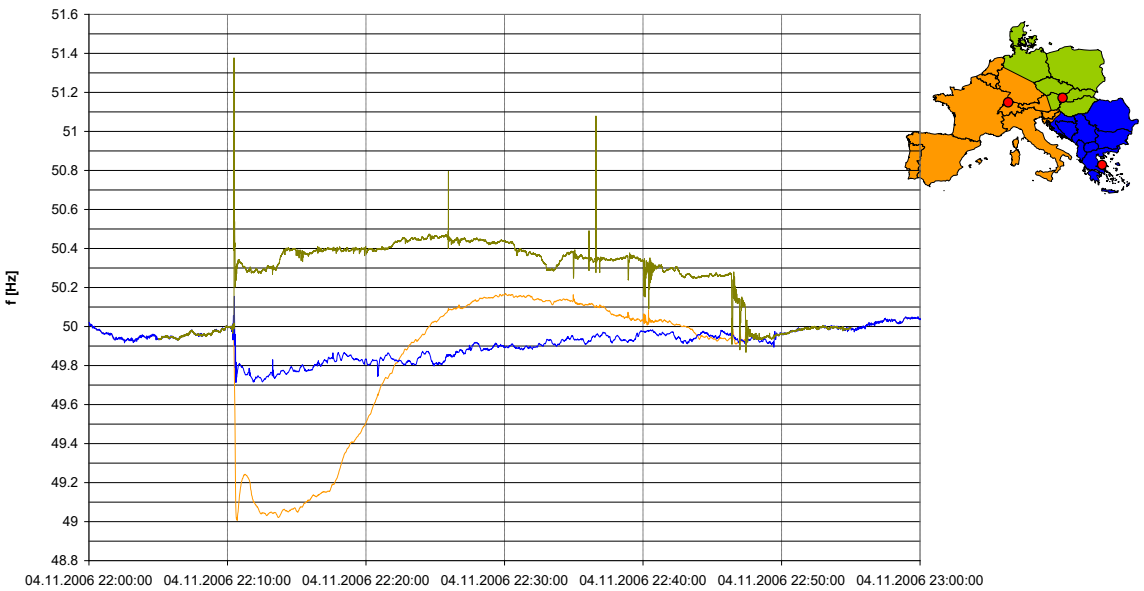
TSO couples busbars in Landesbergen, unexpected increase of the load flow

↓ 22:10:11

Tripping of Landesbergen-Wehrendorf line

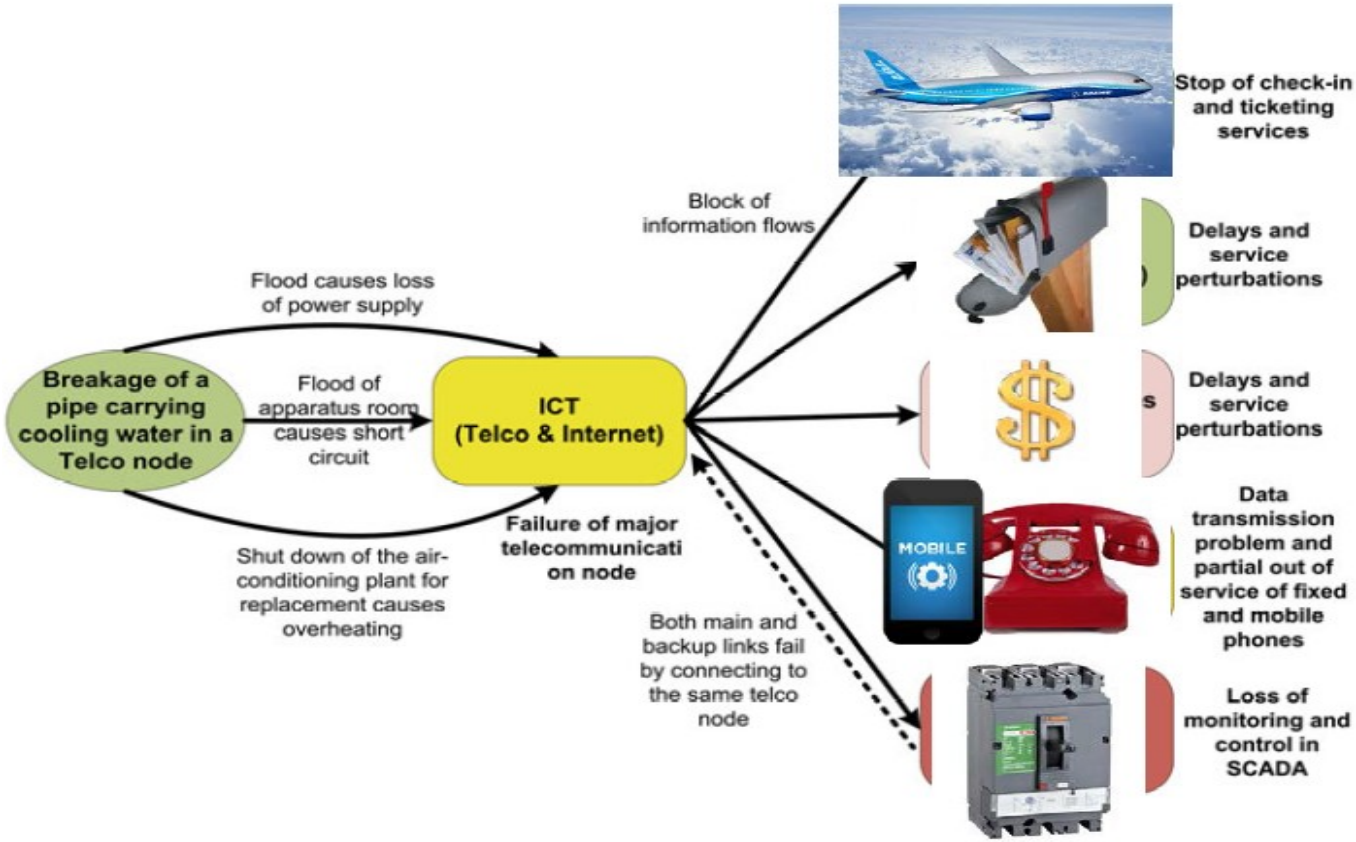
↓

Cascading line tripping leads to 3 separated areas



Wide area frequency measurements, synchronized by GPS, prior to the disturbance and up to the resynchronisation
Source: Final Report – System Disturbance on 4 November 2006, UCTE

Testing Theory with Reality: Major Rome Telcom Node Failure, 2 Jan 2004 and Spread into Other Systems



Testing Theory and Reality: Nov 25, 2005 Münsterland Snow Chaos - Lack of Investment and Preparedness

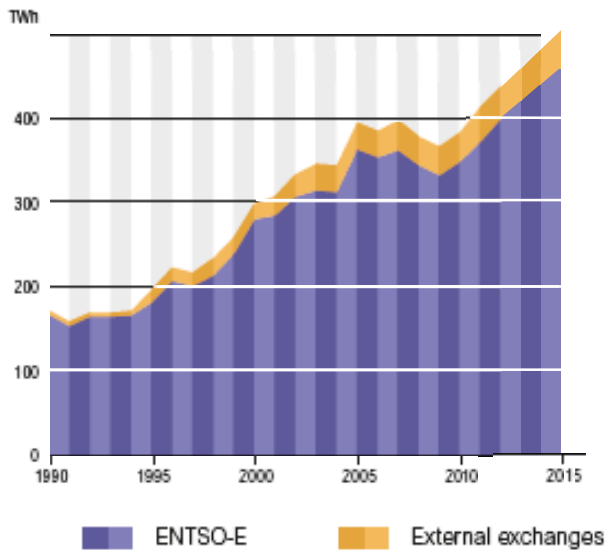
- Extreme rare weather situation with heavy snowfall and strong winds led to massive icing of power lines
- Buckling of aged pylons, broken or deep hanging lines due to heavy loads
- Loss of power supply affecting about 250‘000 people in 25 municipalities for about 3 days; long lasting repair works
- Strong public debate and incomprehension
- Lack of investment into new pylons made of less brittle steel

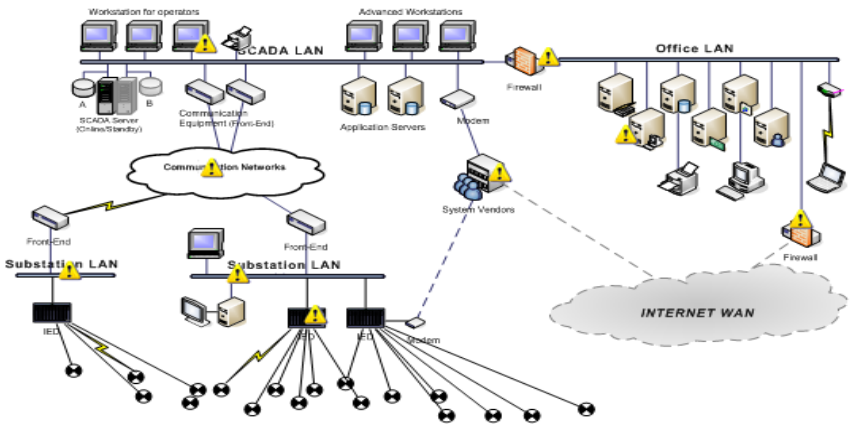
Framing Complexity: Limits of Predictability

- Limits of predictability due to a) lack of knowledge/data/tools and incomplete set of potential disruptions and b) difficulties to identify/ understand often surprising events.
- Some claim, there are no means to anticipate or predict them („Black Swans“), others believe in the opposite, if we have/use sufficient real time information („Dragon Kings“).
- Some argue, with complexity we loose control over resp. systems, should develop strategies to reduce/better balance complexity and re-organize decision making and regulation from top down to bottom up.

Electric Power Supply Systems: Major Changes and Trends

- Replacement of monopolies by intricate (unbundled) market structure and stressing operation modes; shift to growing user involvement and fragmentation of control
- Increasing share of intermittent, seasonal renewable energy sources (wind, solar), highly dispersed, requiring massive transfers
- Increasing volumes of cross-border exchange as well as short-term trading
- Cyber security issues and increasing “smartness” due to IC host technology

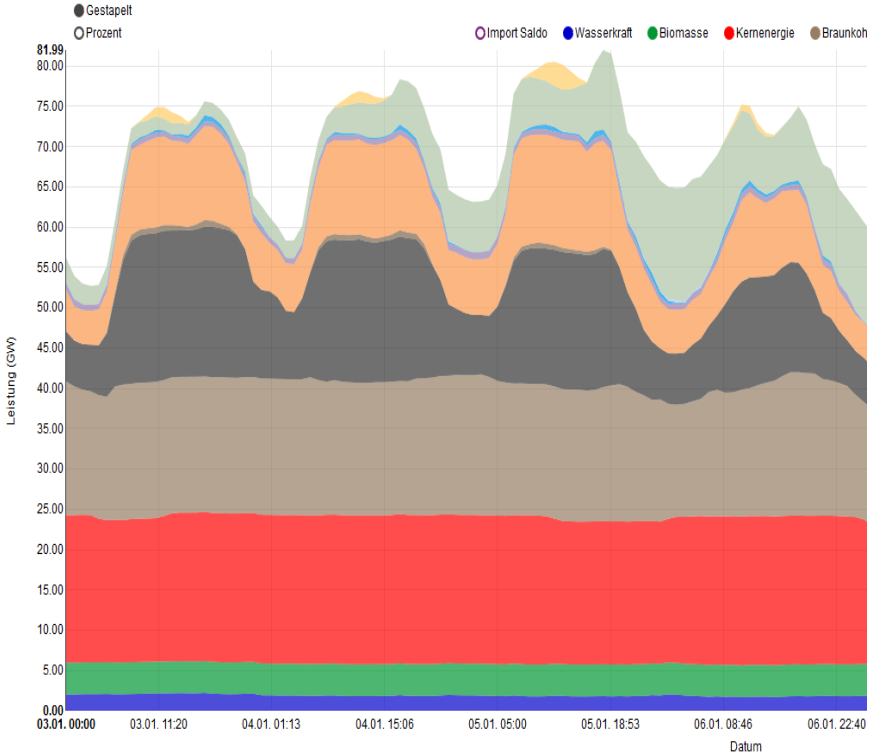




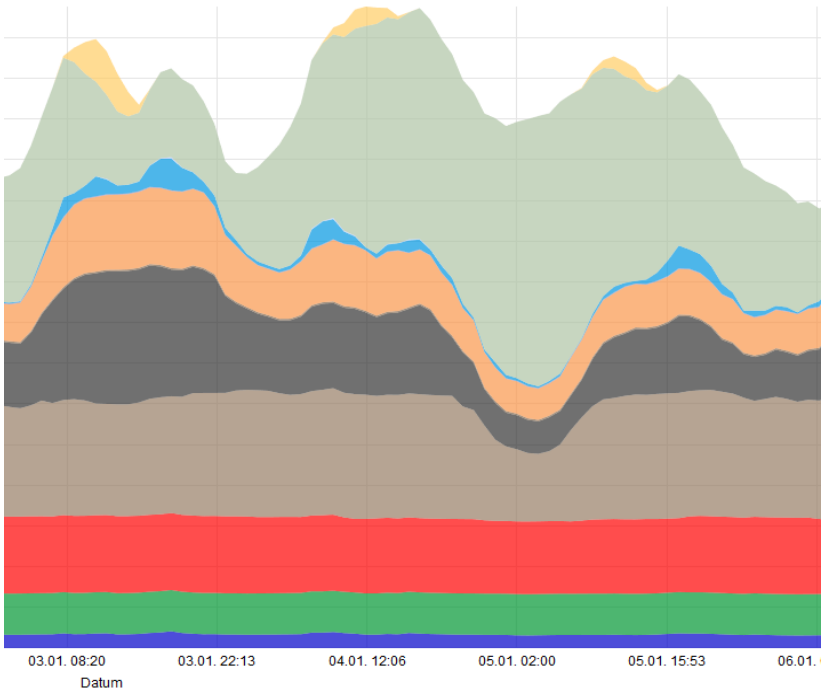
Source: VIKING Project, www.vikingproject.eu.

Veränderungen bei der Nettostromerzeugung in Deutschland

2011



2019



- Intermittierende (variable) Anteile: ~ 12% in 2011; ~ 30% in 2018, Anstieg um Faktor 2,5
- Starke tages- und jahreszeitlichen Schwankungen, einhergehend u.a. mit zunehmender Abhängigkeit von der Wettervorhersagequalität

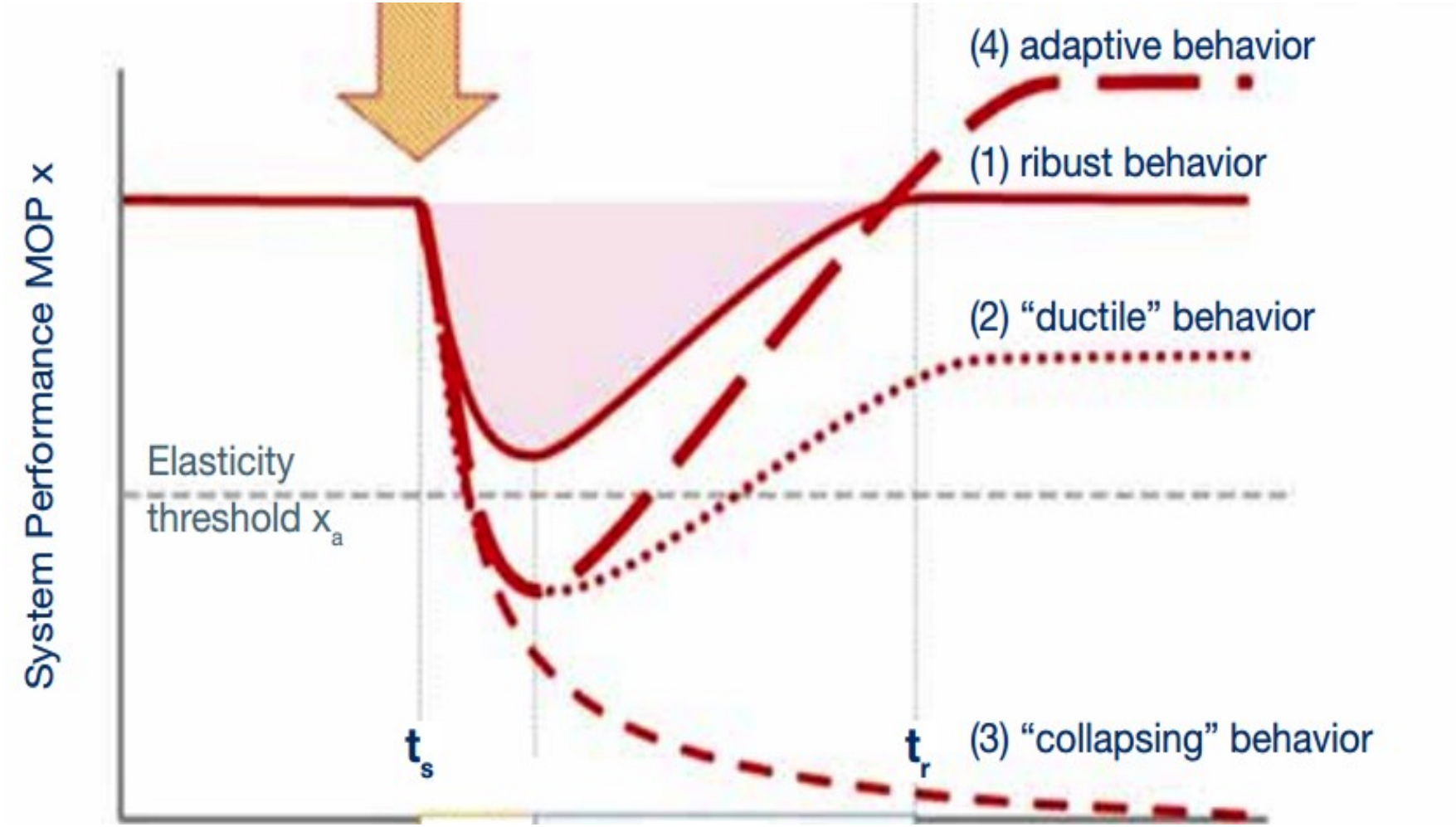
Definition of „Risk“

- Occurrence of some negative consequences, potentially arising from faulty operation of considered systems or activities and associated uncertainties; consequences of events are measured in terms of, e.g., damages to health of people and/or to the environment; uncertainty is expressed in terms of probabilities (frequencies) of undesired events, following the rules of probability calculus.
- For critical infrastructures the risk may include the probability of loss of goods and services with its resulting consequences for the people and other systems affected.
- The risk concept aims to prevent, reduce and control/manage risks.
- Risk analysis is a formalized subject for the purpose of revealing potential failures or hazard triggering events and induced event sequences as well as estimating specified consequences and associated frequencies.

Paradigm Shift from „Hardening“ *(risk reduction)* to Post-shock „Soft Landing Capabilities“ *(resilience)*

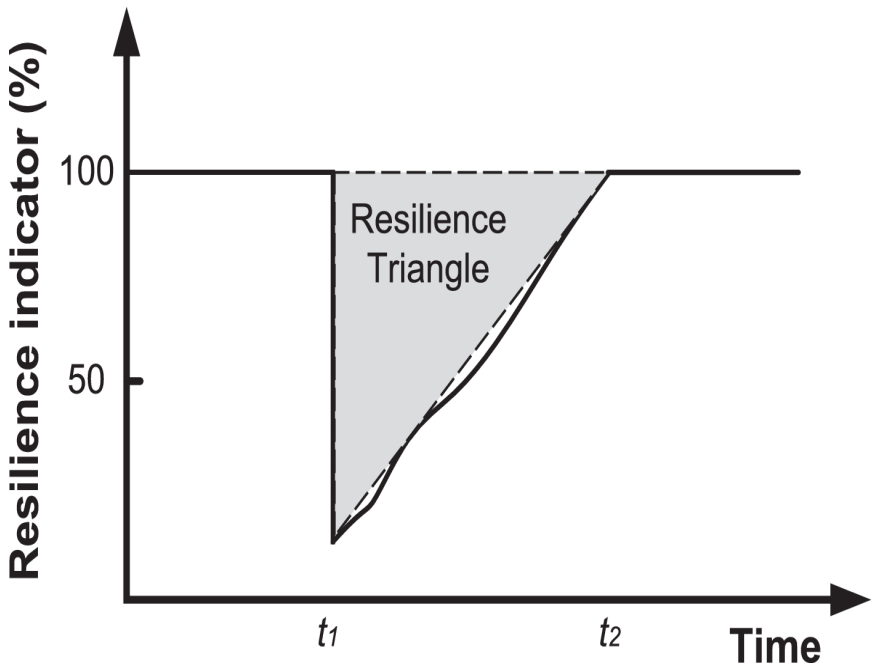
- There is no **commonly agreed definition** of resilience: In general, it is the ability of the system to sustain or restore its basic functionality following a risk source or event (even unknown) [SRA glossary 2015].
- More specifically, it is the system‘s ability to resist/absorb the adverse effects of a disruptive force (either sudden or creeping, including all hazards/threats) with decreasing performance but not collapsing, and the ability and speed to recover and return to functionality – by adapting through self-organization and learning and even-tually bouncing back or transforming into a different state [Kröger 2017].
- The US National Academy of Sciences defines disaster resilience „ as the ability to plan and prepare for, absorb and recover from, and adapt to adverse events“ [NAS 2012].

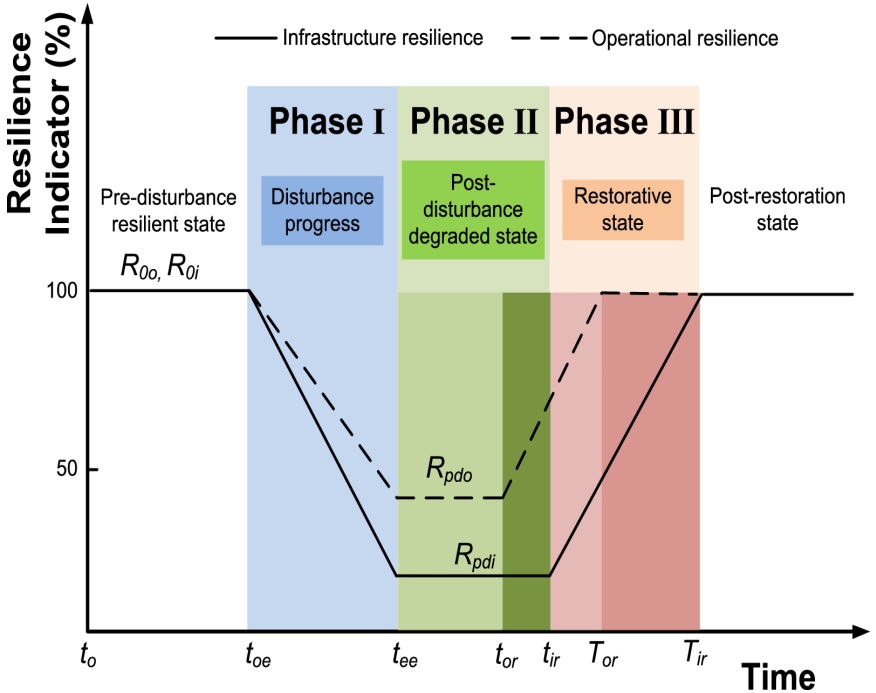
Illustration of Patterns of Resilience



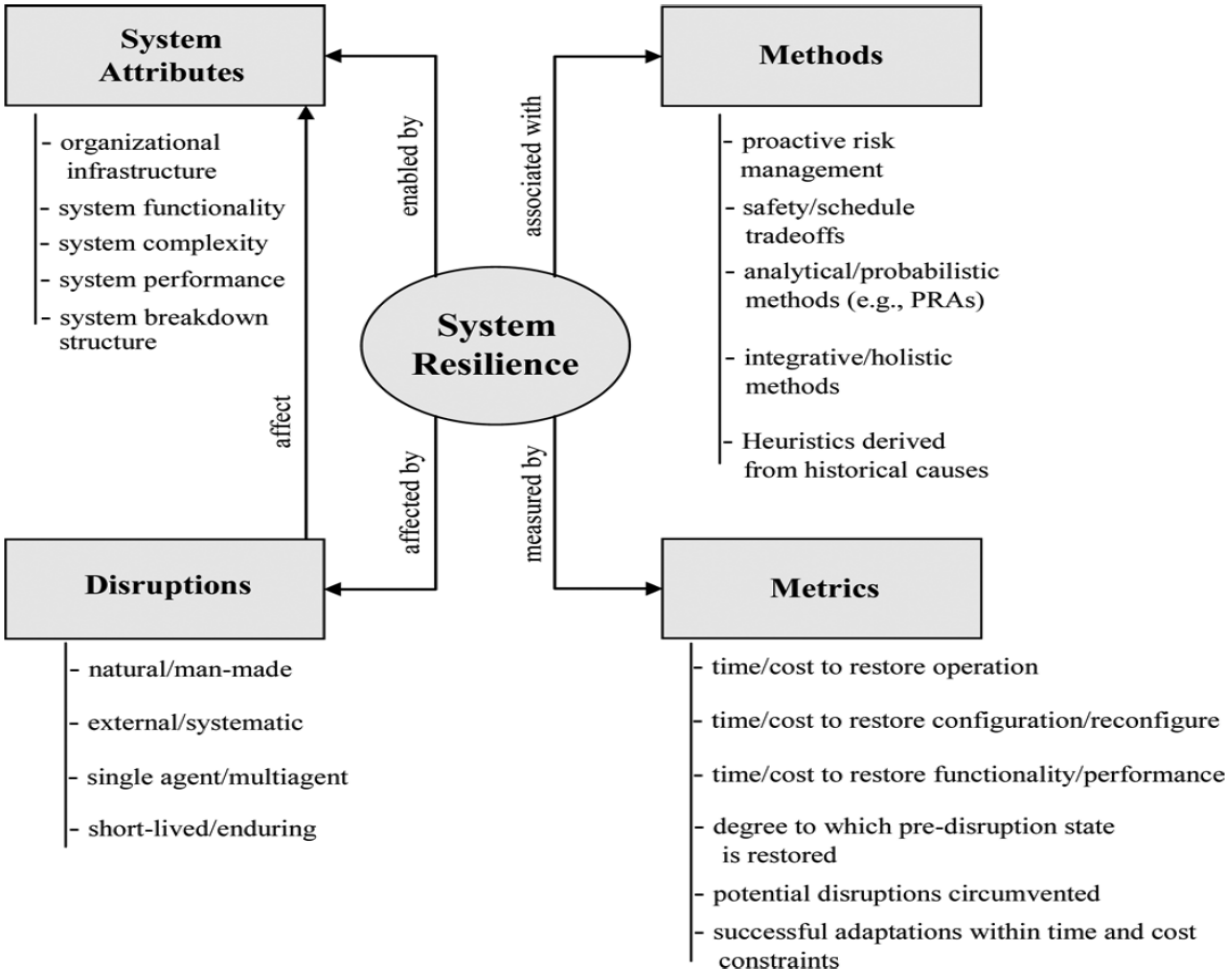
Übergang vom Resilienz „Triangle“ zum „Trapezoid“

[Panteli et al. 2017]





Conceptual Framework for Resilience Engineering



Understanding Complex Critical Infrastructures: Challenges to Methods (I)

- Need to capture multifacetted interactions with intervening variables of a plethora of different components, hierarchically organized, often resulting in „emergent“ behavior related with non-linear feedback mechanisms, self-organizing processes and adaptive learning.
- The collective behavior is more than the sum of individual behaviors, thus, instead of deductionism, a holistic theoretical approach is needed to analyse the system as a whole.
- Small changes of initial conditions can trigger cascades within the system and across boundaries, and have big global effect.
- Depending on their topological structure and initial stress level critical „tipping points“ may be reached, leading to bifurcations and abrupt system collapses.

.... Challenges to Methods (II)

- Most such systems are large-scale, multi-layered, evolving and strongly coupled, they are open and subject to a widening set of natural hazards and man-made threats; damages can be caused directly and indirectly.
- A set of social factors, either operational or organizational, intertwinned with purely technological factors, as well as the interplay of the system with its operational environment need to be taken into account.

- Traditional methods, based on „decomposition“ and „causality“ like logic trees as well as human reliability analysis, often reach their limits.
- No single modeling approach “that captures it all“, instead a framework is needed to integrate a number of methods, comprising different aspects, aiming to identify surprising scenarios.

Advanced Methods Mainly for Risk Analysis of Single Infrastructure Systems

- Empirical approach aims to evaluate statistical information to identify formation mechanisms and patterns of cascading failures.
- Predictive approach refers to modeling and simulating the major system characteristics through reasonable simplifications; methods are either structural/topological/state-related like Complex Network Theory (**CNT**), Petri- and Bayesian-Net, phenomenological/functional like Agent-Based Modeling (**ABM**), or flow-focused like Input-output Inoperability Modeling and System Dynamic.
- The human factor is included by predicting and quantifying the likelihood of human error of omission; considering the potential impact of modifying factors, e.g., time pressure/stress, and effects of the environment on the execution of the task by shaping factors (PSFs).

Advanced Methods...

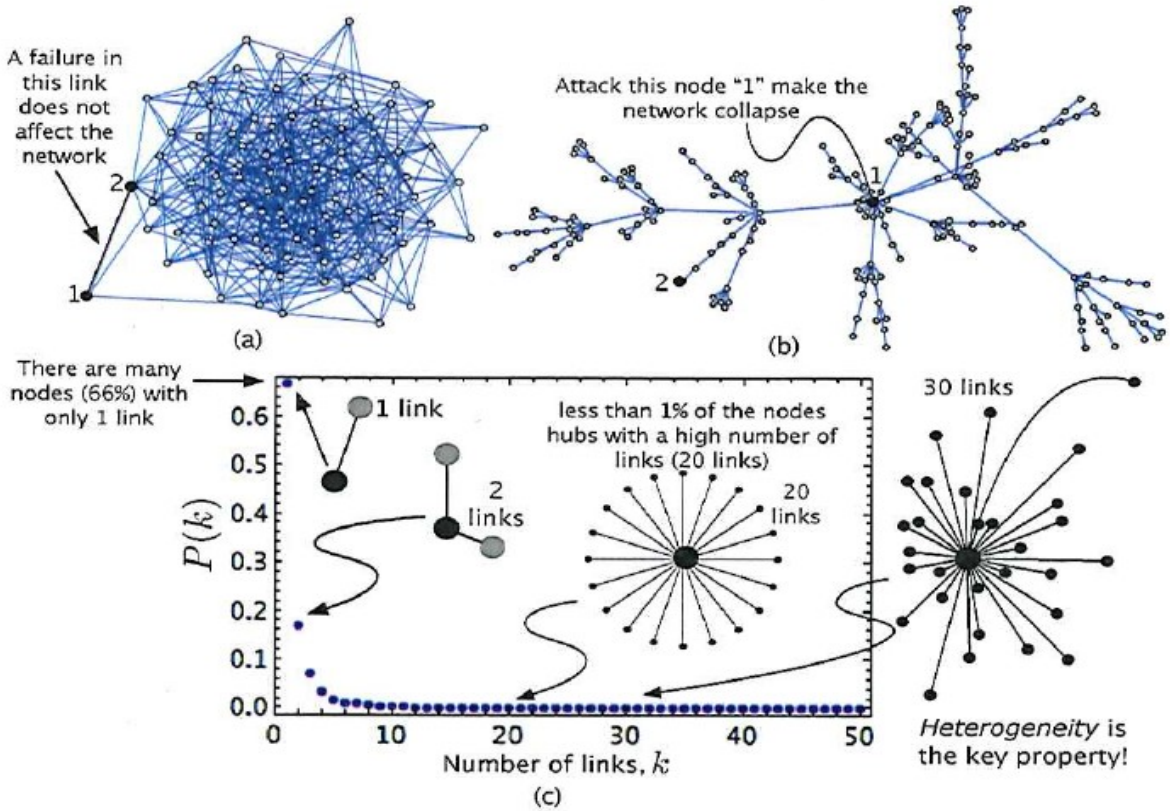
Physical power flow models, event-based **simulations:**

- Analysis of a slow cascade of line disconnections after a triggering event (line break) due to sustained overload, exceeding line temperature and followed knock-on effects
- Result: Demand-not-served vs. total load [Sansavini, 2014]

Structural/topological/state-related models: Complex Network Theory

- Aim to understand the structure of components‘ interactions, characterize the topology and check vulnerability by removal of elements
- Basically, transform real system (power grid) into a graph with nodes (stations, substations) and links (lines), build adjacency matrix
- Measure drop in performance by a group of topology-based metrics: path lengths, node degree distribution, clustering coefficient, etc.
- Typical insight: Most power grids have a highly homogenous structure (hubs) making them robust against random failures but vulnerable against targeted attacks

Standard Complex Network Theory: Illustration & Results



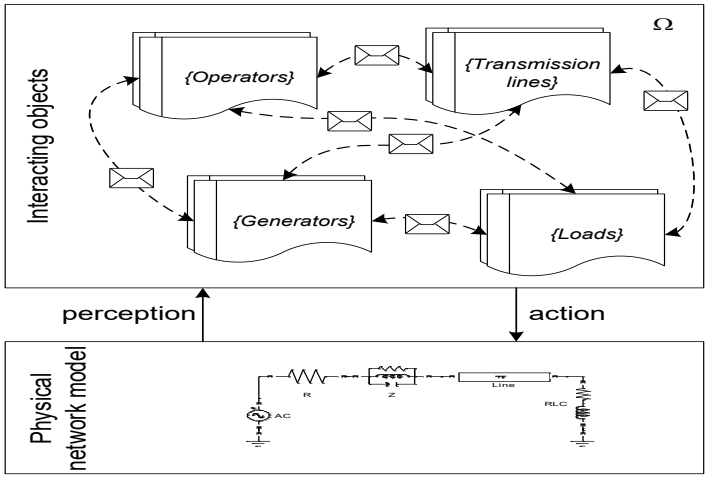
(a) Example of robust network; (b) example of a scale-free network, vulnerable to attacks on nodes with many links ; (c) node degree probability density function of a network similar to that represented in (b)

Complex Network Theory: Advanced Approaches

- Capturing power flow redistribution after node/link failure (removal) by flow-based performance and vulnerability metrics such as amount of power supply, average line load level, weighted shortest path.
- Considering holding load level and shedding load to neighbors when holding capacity is exceeded (“sandpile model”).
- Identifying “giant component” which remains functional while small clusters become non-functional (“percolation theory”).

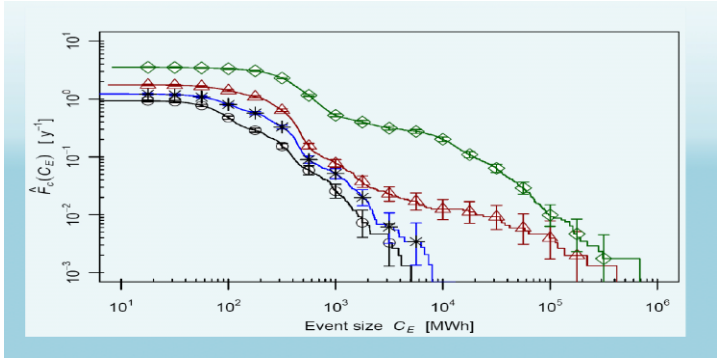
Phenomenological/Functional Approach

- A time-stepped model based on a two layer agent-based approach (**ABM**)
- Scenarios continuously simulated by means of power flow calculations
- 587 agents model technical components (generators, lines) and non-technical components (grid operator)



Results:

- Blackout frequency with (unfavorable) power law distribution for high initial loads
- Significant influence of operator response within first 20 min



*Cumulative blackout frequencies for different grid load levels (100% (circles), 110% (stars), 120% (triangles) and 137% (diamonds)) [**Schläpfer et al., 2008**]*

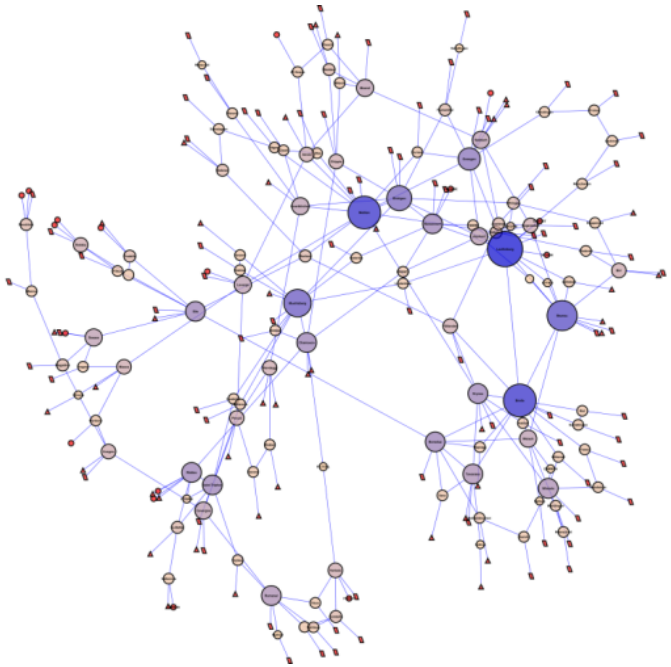
Complex Network Theory and Load Flow Model Combined to Investigate Impact of Malicious Attacks

Important elements of the Swiss grid are identified by centrality analysis using

- deterministic attacks, targeted on substations
- stochastic attacks on lines (randomly disconnected)

Results based on response analysis:

- No highly unstable conditions emerged from the attack on the most critical substations (hubs)
- Although the load flow model is quasi-dynamic, the effect of cascading failures was very small
- Overloading of transmission lines in only a few scenarios shows good safety margins for the grid



Swiss transmission grid: 242 nodes for substations, loads, generators and 310 links for lines, node size analog to degree centrality

Bilis, E. I., et al.. (2013). IEEE Systems Journal, 7(4), 854-865

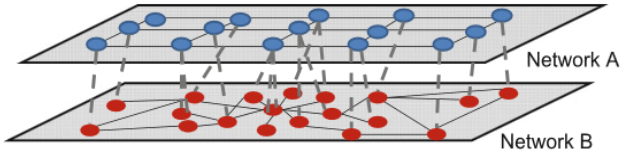
From Single to Interdependent Systems

- Real-world interdependent networks pose even harder challenges to methods than single networks ... [Havlin et al., 2012].
- Interdependent networks are more [Buldyrev et al., 2010] or less [Brummit et al., 2012] vulnerable to cascades.
- Most of the advanced methods still address interdependencies in a simplified idealized way but „oversimplifications“ may not account for characteristics of real systems like power grids [Kenett et al.; D‘Souza, 2014], often integrated into a system-of-systems.
- A „all by one“ modeling approach would be necessarry but turned out to be extremely difficult and moreover inefficient.

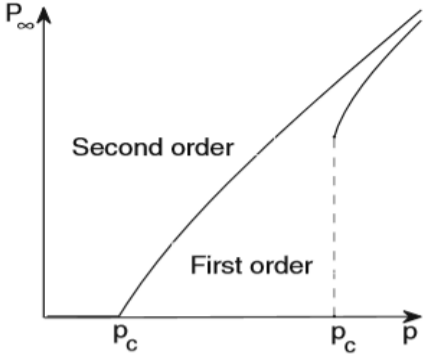
Approaches to Scope with Interdependencies: Enhancement of Complex Network Theory

Enhancement of CNT

[Kenett et al., 2014]



- Introducing additional layer(s) and couplings (analogous interactions between particles in statistical physics)
- Extending „percolation theory“: Removal of A-nodes causes removal of coupled B-nodes and of A-nodes connected; spreading of failures will fragment the system into small clusters beyond a threshold (fraction p_c) and a giant mutually connected cluster (with a fraction of nodes P_∞) which ensures functionality



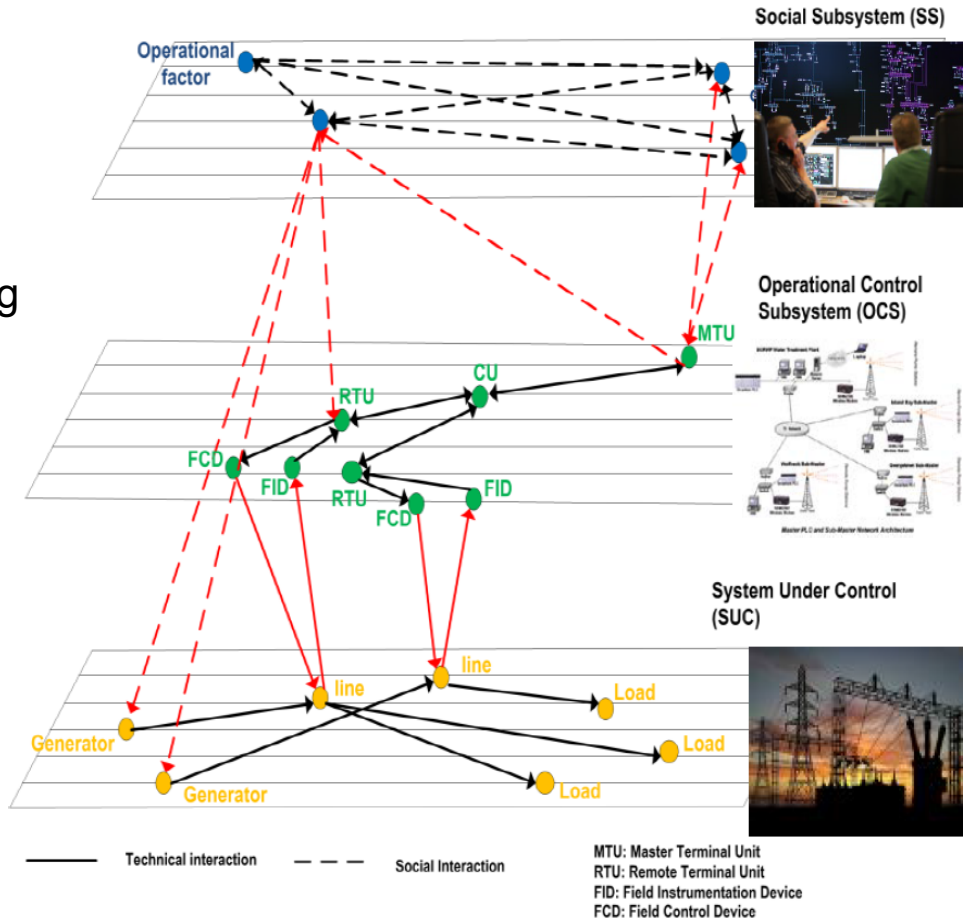
<u>Typical result</u>: When coupling is reduced the percolation transition becomes 2nd order (no discontinity) [Parshini et al., 2010; Gao et al., 2011]

Approaches to Cope with Interdependencies: Multi-layer, Hybrid Modeling Framework (I)

1. **System under control (SUC)**
   - Transmission lines, generators, busbars and protection relays

2. **Operational control system (OCS)**
   - Responsible for controlling and monitoring the couple SUC
   - Supervisory Control and Data Acquisition (SCADA) system
   - Field instrumentation and control devices (FIDs and FCDs), remote terminal units (RTUs), communication units (CUs), and master terminal unit (MTU)

3. **Social System (SS)**
   - Human and organizational factors
   - Monitoring/processing generated alarms, switching off components and sending commands to remote substations



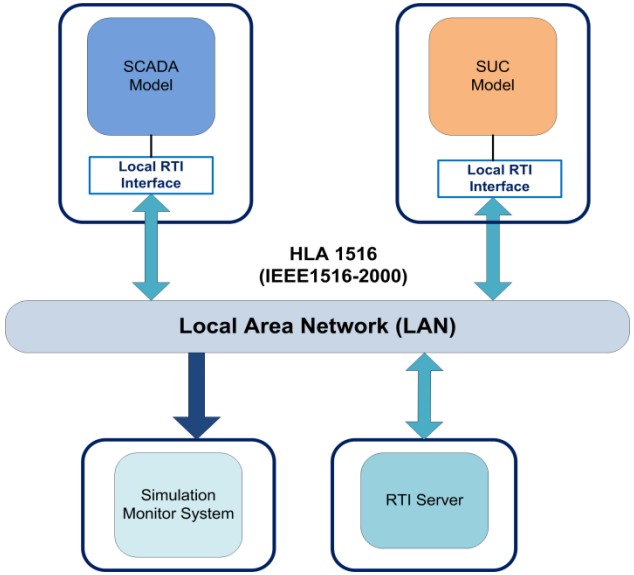
[Nan & Sansavini, 2015]

Approaches to Cope with Interdependencies: Multi-layer, Hybrid Modeling Framework (II)

- Second step: Development of individual models, capable to capture the characteristics of the related subsystem (layer)
- Third step: Representation of model interactions, e.g., by using the High Level Architecture (HLA) simulation standard

Exemplary application (Swiss power system)

- Investigation of interdepency-related vulnerabilities between SCADA and „system under control“ (SuC)
- Result: Propagation of failures crossing interlinked systems takes a certain period of time (!)



Experimental simulation platform [Kröger & Nan, 2014]

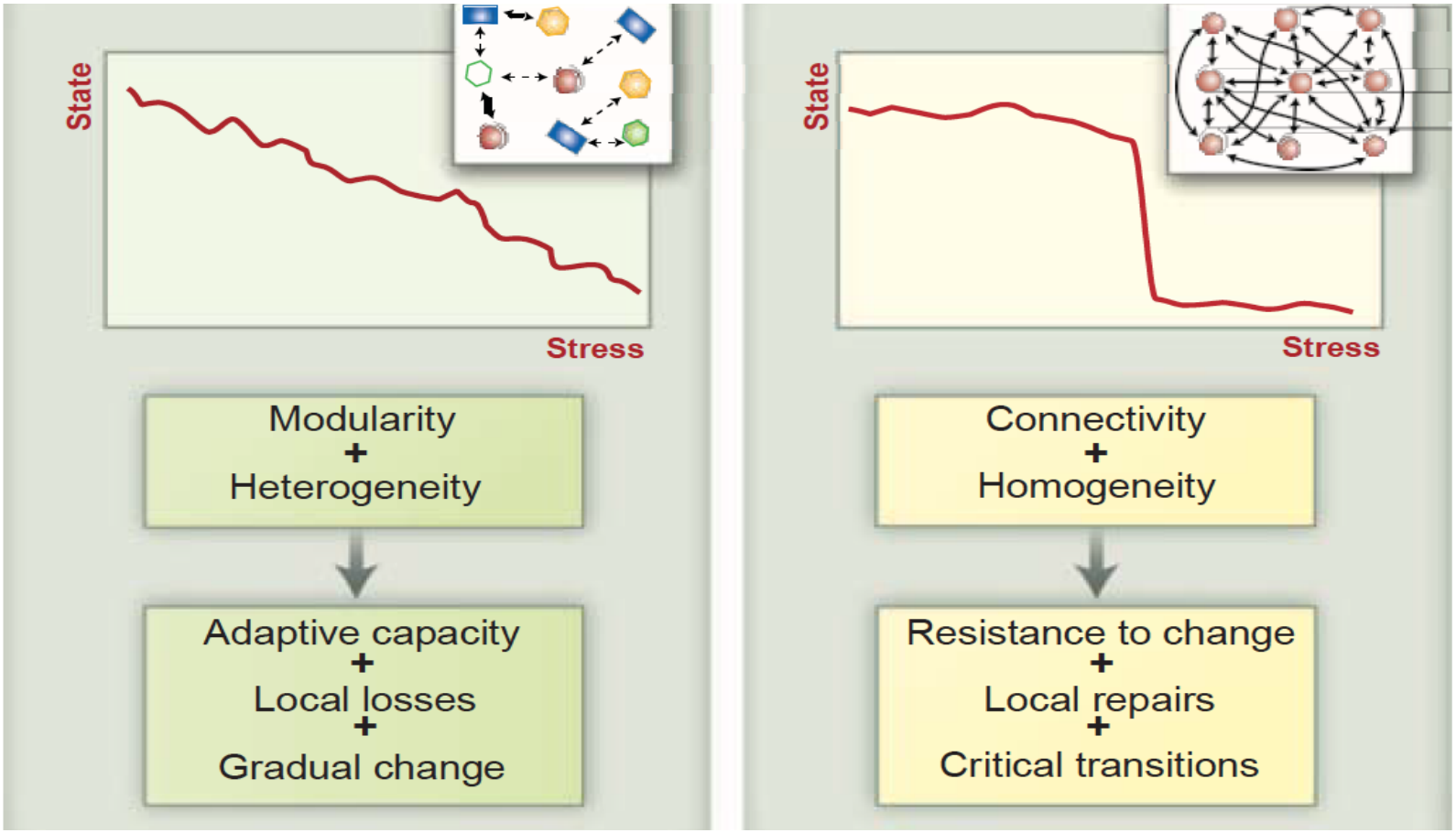
From Traditional Risk to Resilience Assessment

- Risk assessment is regarded the preliminary triggering phase of resilience analysis which adds the ability to understand the capacity of an organization/system to rebound from massive external shocks.
- Resilience analysis/quantification is less mature than its peer methodology in risk assessment, also because resilience is particularly relevant for dealing with uncertain threats and unexpected system response under extreme conditions [Linkov & Palma-Oliveira 2017].
- Quantitave, semi-quantitative and qualitative approaches and associated metrics have been proposed/deployed to complex technical systems at local, national and international level for various events.
- Resilience management framework (adapted from ISO standard 3100) worked out including context establishing, disruptions identification, resilience analysis, evaluation and building [Heinimann & Hatfield 2017].

How to Increase Resilience of the Energy System: Some Recommendations from the Author‘s Perspective (I)

- Allocate resource buffers, implement physical and functional redundancy/diversity *(counter trend to reduce them because of economics).*
- Increase heterogeneity and modularity *(all in line with favored future decentralized/cellular structures*).
- Develop switching installlation, decoupling (islanding) and reconnecting strategies *(smart operational measures to avoid large-scale collapses).*
- Strive for robust topology, i.e. balance interconnectedness,prevent critical nodes from spreading failures, optimize structure *(use topological metrics)* against random failures and targeted attacks.
- Balance complexity *(avoid too little – too high)* as well as automation and human control (keep humans in the loop for the unforeseen); implement online monitoring/provide real-time information but secure devices/processes.

Offers from Science to Increase Resilience of the Energy Infrastructure: Connectivity - Homogeneity as Srews ?



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

How to Increase Resilience of the Energy System: Some Recommendations from the Author‘s Perspective (II)

- Design for operation within safety margins *(counter trends…),* notice early warning signals, reorganize decision making and system control *(top-down where appropriate)* in response to external changes.
- Distinguish between operational and physical infrastructure resilience as the first, based on smart solutions *(like de-/reconnecting)*, might be faster restored; plan recovery actions *(with adequate means/repair crews)*.

- Develop a sufficiently detailed model to studycomplex system behavior and the effect of measures; span hazards/threats and triggered scenarios to all imaginable, include malicious (cyber) attacks.
- Strive for predictability by applying new knowledge and advanced tools.
- Note that the public often lacks awareness of potential vulnerabilities and willingness to act (pay) before severe events (blackouts) happen.

Take-home Messages

- The energy/electric power supply system continues to be an (the) essential element within a network of coupled critical infrastructures, facing major changes („Energiewende“) and expanding its domain of application (transport sector).
- Resilience maintains much of the same philosophical background and mindset as the traditional risk concepts; resilience additionally delves into the unknow, uncertain and unexpected at the scale of the system as a whole and seeks to offer „soft landing“ after a significant shock.
- The concept should be further developed and operationalized, calls for a holistic, inter-disciplinary view, integrating various actors/forces.
- Research is still needed to help us better understand, (re-) design/ structure and operate the systems in an innovative cost-effective way.

Danke – Fragen?

Testing Theory with Experience: High Performance of the European Transmission System

- In Europe, the ENTSO-E Operation Handbook provides principles, technical standards and recommendations to help operators to manage their own network and ensure interoperability among them.
- The N-1 principle requires that after a failure of a single network element the remainning elements must be capable of accomodating the change of flows and avoiding cascading effects.

➢ The determistic framework has been successful in ensuring high performance of transmission grids, if properly implemented, but deems insufficient to cope with multiple failures and tripping cascades as demonstrated by a considerable number of major blackouts.

Conflicts and Trade-offs

- Measures to improve resilience like increased heterogeneity and decreased connectivity as well as decoupling strategies may lower the probablity of large-area blackouts but increase the probability of local performance losses.
- Some measures like „increased redundancy“ and „staying away from overloads“ are in contrast to recent developments driven by economics and to the sustainability (efficiency) imperative.
- Modern digital industrial control systems (ICS/SCADA) offer great benefits but may induce new risks (cyber attacks including manipulation), hard and costly to avoid and manage.
- The public often lacks awareness of potential system vulnerabilities and willingness to act and pay before severe events (blackouts) happen.