Universität Bremen

artec
Sustainability
Research Center

Resilience and vulnerability of energy systems

Mariela Tapia
Oldenburg 27.09.2023

RESILIENT ENERGY SYSTEMS

artec
Sustainability
Research Center

Agenda

- **Resilient Energy System department**
- **Introduction**
- **Theoretical framework**
- **Application project**

artec
Sustainability
Research Center

Agenda

- **Resilient Energy System department**
- Introduction
- Theoretical framework
- Application project

BEST Energy Solutions

artec Sustainability Research Center

RESILIENT ENERGY SYSTEMS

Resilient Energy System Department

- **Energy systems** as socio-technical systems
- **Resilience** as **guiding principle** for the transformation of complex socio-technical systems
- Investigation of **transformation pathways** towards **100% renewable energies** in all energy sectors
- Analyses from **socio-technical** and **socio-economic** perspectives
- Optimized utilization of variable renewable energies & sector coupling via process **flexibilization**, **storage** and conversion routes (**Power-to-X**)

Research Projects

hyBit

STROM ± RESILIENZ

nordwest2050
Perspektiven für klimaangepasste Innovationsprozesse in der Metropolregion Bremen-Oldenburg im Nordwesten

QUARREE 100

wärme wende nordwest

KOPERNIKUS PROJEKTE
ENavi
Die Zukunft unserer Energie

H_2B

RESYSTRA

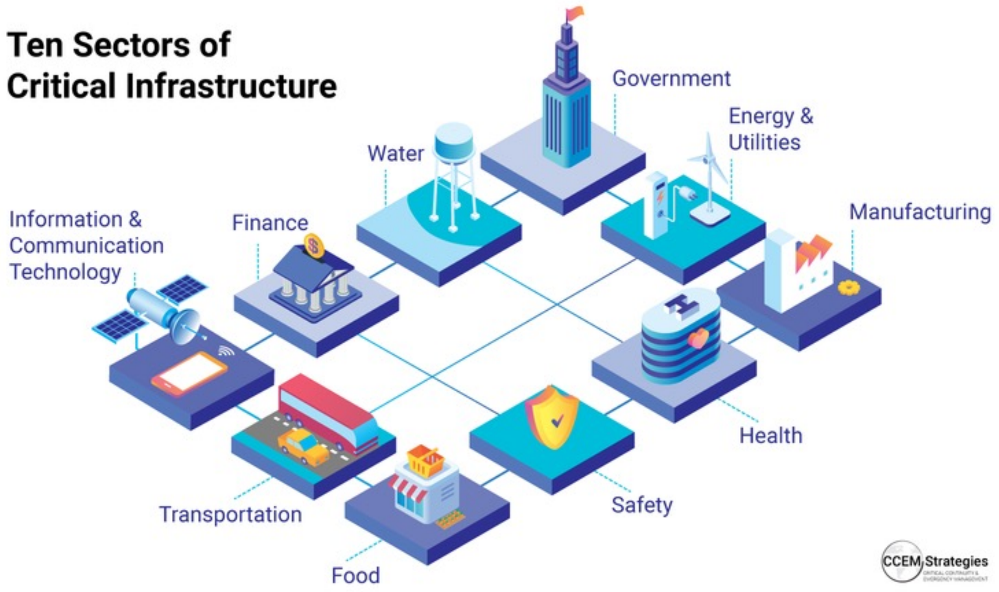
KEROSyN 100

Agenda

- Resilient Energy System department
- **Introduction**
- Theoretical framework
- Application project

Critical infrastructures

- Critical infrastructures are vital for the development of our society
- Protection of these infrastructures against known and unknown stressors is highly important



www.ccemstrategies.com

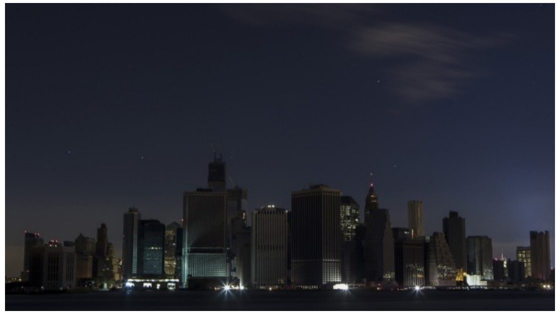
Stressors

- Natural disasters: hurricanes (e.g. Katrina, Sandy), earthquakes, tsunamis
- Nuclear disasters: e.g. Fukushima power plant
- Terrorist attacks: e.g. 9/11 attack
- Cyber-attacks: e.g. Ukrainian Blackouts in 2015, 2016

→ Produced catastrophic socio-economic impacts and showed the fragility of critical infrastructures

pbs.org

Reuters: Mainichi Shimbun



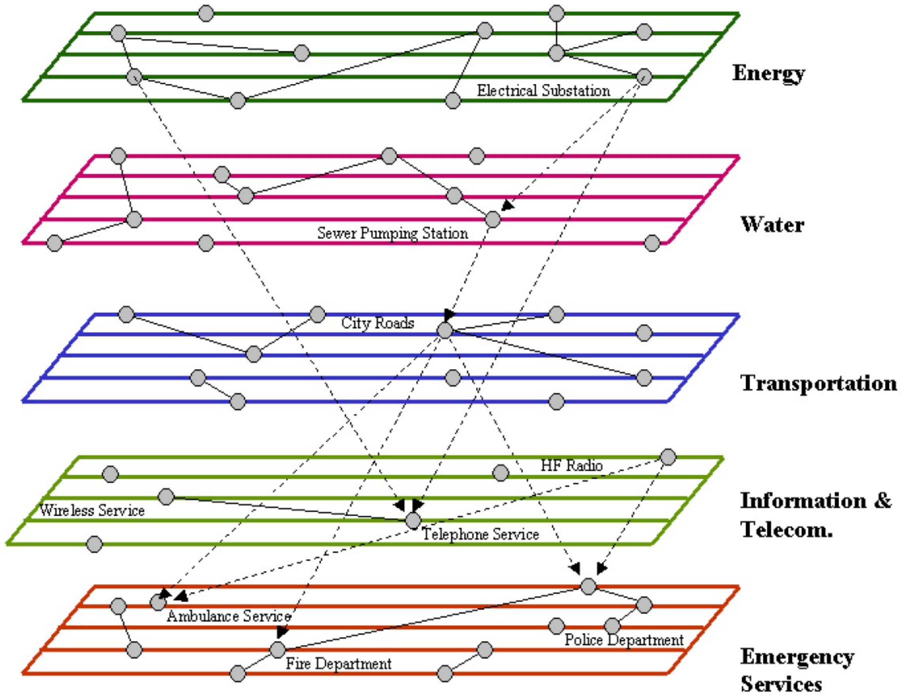
cfr.org

express.co.uk

Current development and uncertainties

- Growing complexity and interdependence of infrastructures
- Increasing digitalization
- Growing number of extreme weather events
- Human failures leading to large-scale disruption of service

→ Higher uncertainties of stressors that could impact critical infrastructures



Infrastructure interdependencies: Illustration based on the scenario of a flooding event and subsequent response.
Peterson et al. (2006) Critical infrastructure interdependency modeling: a survey of US and international research

Agenda

- Resilient Energy System department
- Introduction
- **Theoretical framework**
- Application project

Classical risk management approach

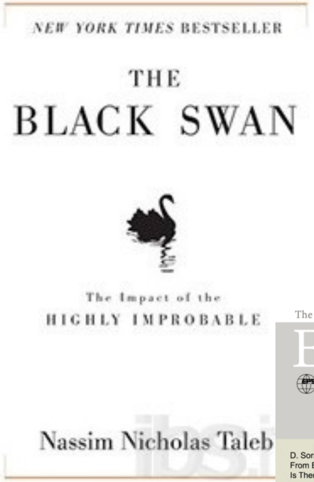
- Focused on stressors which can sufficiently be described in terms of:
  - frequency of occurrence
  - size and duration
  - impact
- Associated uncertainties are regarded as being numerically quantifiable

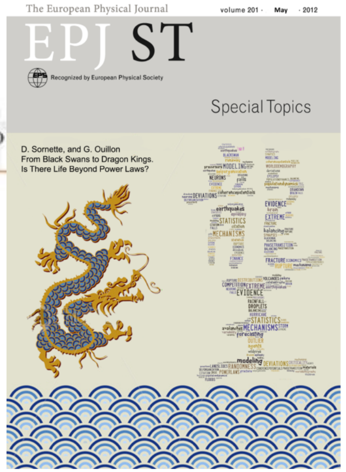
centranum.com

Analysis of uncertainties and stressors

- But it is also needed to deal with surprises, which are difficult to describe in terms of probabilities
- Difficulties in predicting a stressor or its impact occur in different forms:
  - Unknown (or changing) probability of occurrence
  - Unknown nature/type of the stress
  - Unknown probability of extent and duration
  - Unknown impact on the system
  - Unknown system state or interdependence with other systems

→ “unknown unknowns”, “black swans”, “dragon kings”, ...





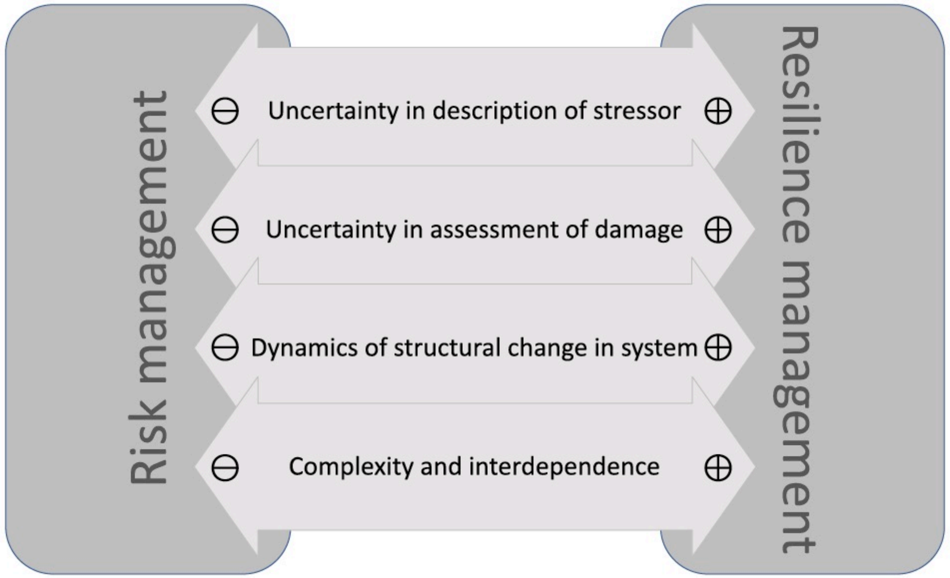
wikipedia.org

How to prepare the system for such events?

Resilience management

- Focus of **risk analysis** and management lies on **stressors which can sufficiently be described** in terms of frequency of occurrence, size and duration and impact on the system

- Focus of **resilience** approach lies on the affected system, its capability to **preserve system services** and on complex, interacting or interdependent systems



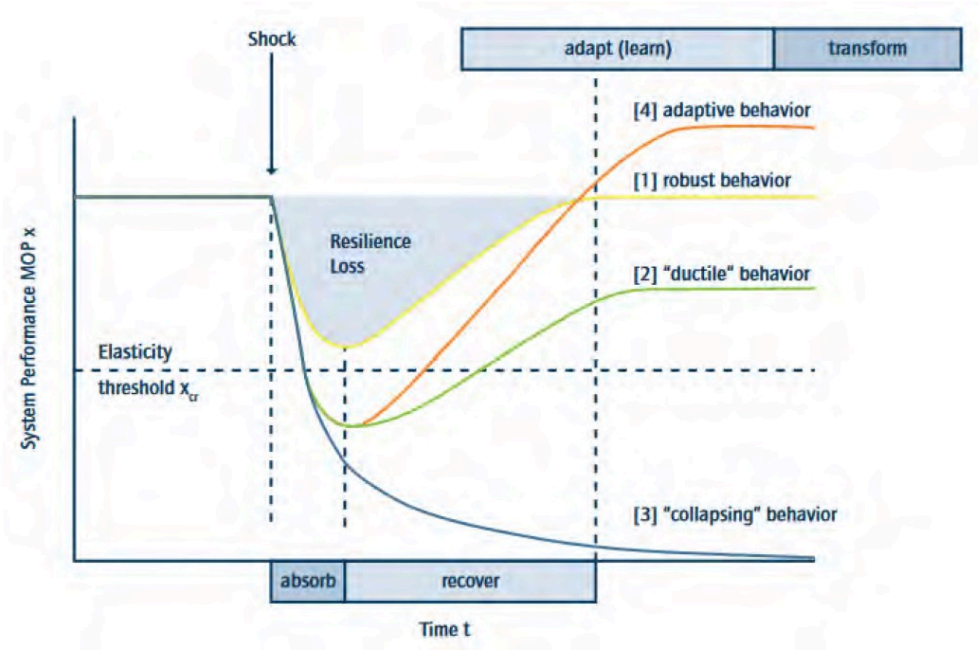
Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures.

Resilience

Many roots, many meanings:

- **Material science**: property of materials to withstand severe conditions (Tredgold 1818, Mallet 1856)
- **Psychology**: ability of people and organizations to cope with traumatic experiences (Werner et al. 1971)
- **System ecology**: ability of ecosystems to maintain their function under stress (Holling 1973)
- **Social-ecological systems**: ability of managed ecosystems to maintain their services (Walker et al. 2004)
- **Engineering**: ability of engineered systems to sustain required operations under expected and unexpected conditions (Hollnagel 2006)

Illustration of patterns of resilience



- Absorbing a shock with decreasing performance, without collapsing
- Recovering from a shock
- Adapting through self-organization and learning
- Bouncing back or transforming into a different state by altering structures or functions and feedback loops

Based on:

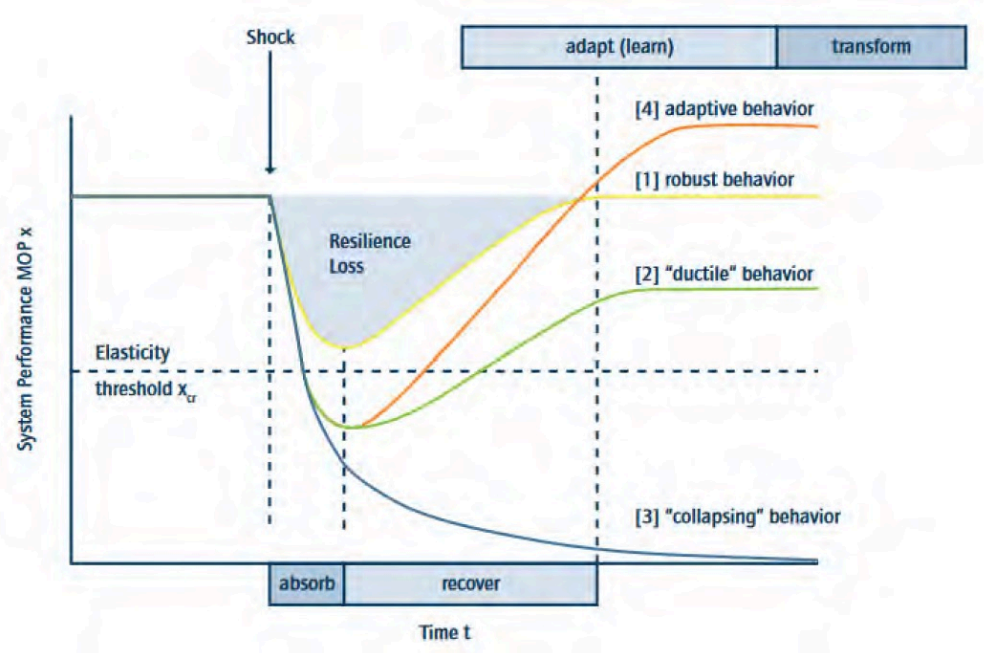
- Kröger, W. (2017). Securing the Operation of Socially Critical Systems from an Engineering Perspective: New Challenges, Enhanced Tools and Novel Concepts. *European Journal for Security Research*, *2*(1), 39–55.
- Nan, C., & Sansavini, G. (2017). A quantitative method for assessing resilience of interdependent infrastructures. Reliability Engineering and System Safety, 157, 35–53.

(MOP: Measure of performance)

Questions regarding this interpretation of resilience

What is the system performance? Quantitative vs qualitative

Is minimizing the „triangle“ the best approach?



What is the resilience of interdependent systems of systems?

How do we identify the main design elements of resilience?

Whose resilience anyway?

Can we understand the dynamics of resilience? (evolution of systems)

Can we assess a system‘s resilience *ex ante*?

Questions taken from: Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures.

Resilience for socio-technical systems

"Resilience describes a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions"

Gleich et al. (2010)

Turbulence: dynamic changes in system structure and environment, irregular conditions, limited predictability, and surprises acting on the system

Gleich et al. (2010). Resilienz als Leitkonzept – Vulnerabilität als analytische Kategorie

Socio-technical system services

- Defined by:
  - Quantitative component: “What?”
  - Qualitative component: “How?”
- Provision of electricity as example:

Quantitative Component

Delivery of power

Qualitative Component

Direct Technical Parameters	Indirect Parameters
Power quality:	Environmental impacts
Voltage level (e.g. 400 V +/-10%)	CO_2 Emissions
Frequency (e.g. 50 +/- 0.2 Hz)	Land / Resources use
	Waste production
Reliability indices:	Economic impacts
SAIDI (System Average Interruption Duration Index)	Costs/Market price effects
	Competitiveness
…	Public acceptance
	Customer privacy
	Technology acceptance

Based on: Gößling-Reisemann et al. (2013). Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany.

Resilience in preparation for the unexpected

- **Resilient systems** should be **prepared** for ‘**complete surprises**’
- It changes the focus to ‘**precaution-oriented design**’
- Three different sources of information to gain insights:
  - **Event-based vulnerability assessment**
  - **Structural vulnerability assessment**
  - ‘**Learning from nature**’: Design principles of resilient energy systems derived from nature

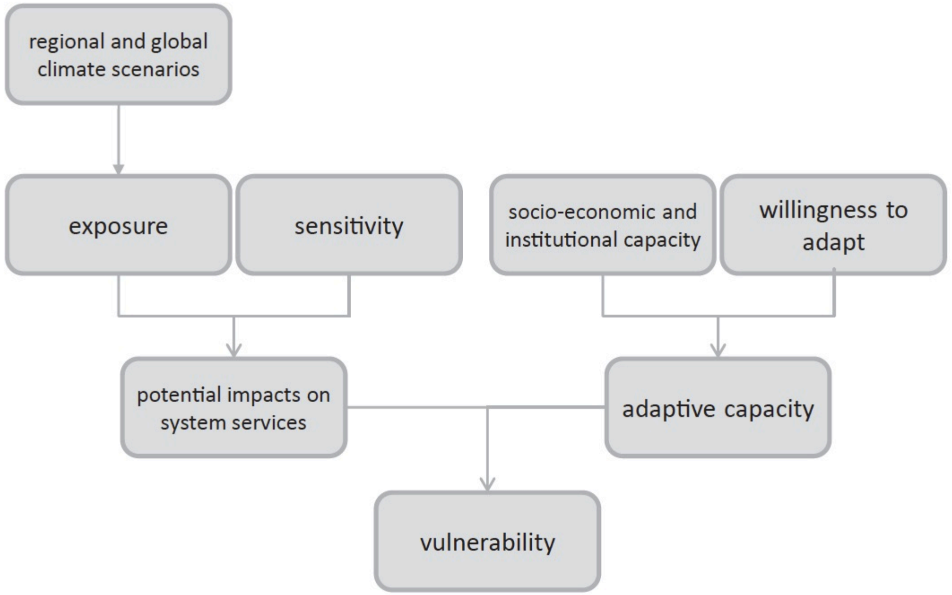
Vulnerability as Analytical Tool

"The degree to which a system is likely to experience harm due to exposure to a hazard, either an exogenous perturbation or an endogenous stress or stressor"

Turner et al. (2003)

Turner et al. (2003). A framework for vulnerability analysis in sustainability science.

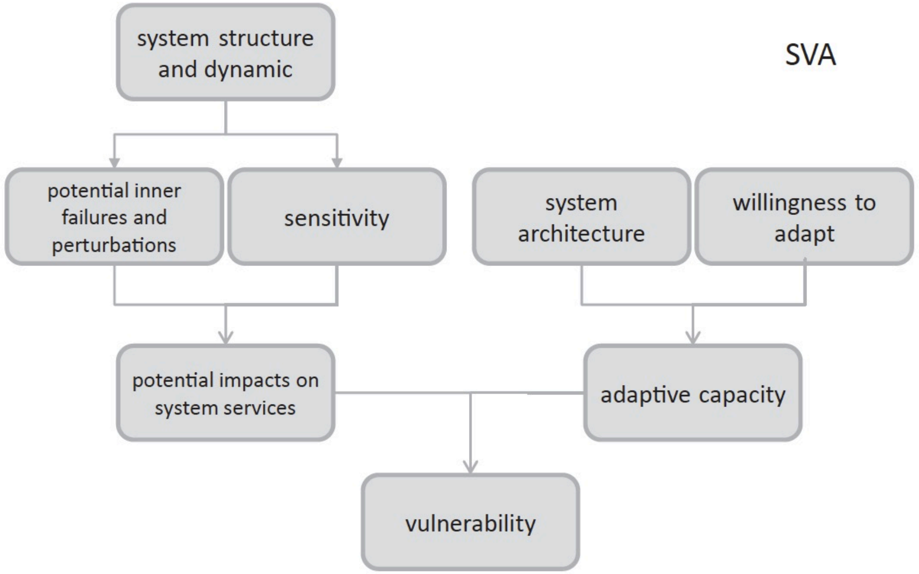
Event-based vulnerability assessment (EVA)



- Steps:
  - Identification of possible perturbations
  - Analysis of exposure and sensitivity
  - Identification of potential impacts on system services
  - Analysis of adaptive capacity
  - The result indicates the vulnerability
- Design options can be developed to reduce this identified vulnerability

Gößling-Reisemann et al. (2013). Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany.

Structural vulnerability assessment (SVA)



- It goes beyond learning from experience with stressors to learning on the basis of structural analysis of affected systems
- Uses methods of engineering science:
  - Failure mode and effective analysis (FMEA), fault tree analysis, stress tests, among others
- It focusses on the system to discover where its weak points lie
  - At which points will the system surrender?
  - Which components or relations could fail if the system is under stress?
- From results, further precaution-orientated design options can be developed, which could minimize or compensate for these weak points

Gößling-Reisemann et al. (2013). Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany.

Resilience as a guiding principle

- We use resilience as a guiding concept for system design
  - i.e. for deriving system structure, components, couplings, etc.
  - In system analysis the focus lies on ‘progress towards the target’

- Benefit of using design guideline: reduce demand on knowledge and certainty
  - Resilient system should be (if designed adequately) less susceptible to unknown stressors / surprises
  - Then you need to know less about external stressors and disturbances to build a reliable system

Desired capabilities of resilient systems

- Resilience means:
  - Being prepared for expected and unexpected stressors
  - Being prepared for slowly and fast developing stressors
- Stressors are characterized by the state of knowledge about their nature and dynamics

Stressor	Known / expected	Unknown / unexpected
Gradual / creeping	Adaptive Capacity	Innovation capacity
Abrupt / sudden	Robustness	Improvisation capacity

Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures.

Design elements for resilient systems:

‘Learning from nature’

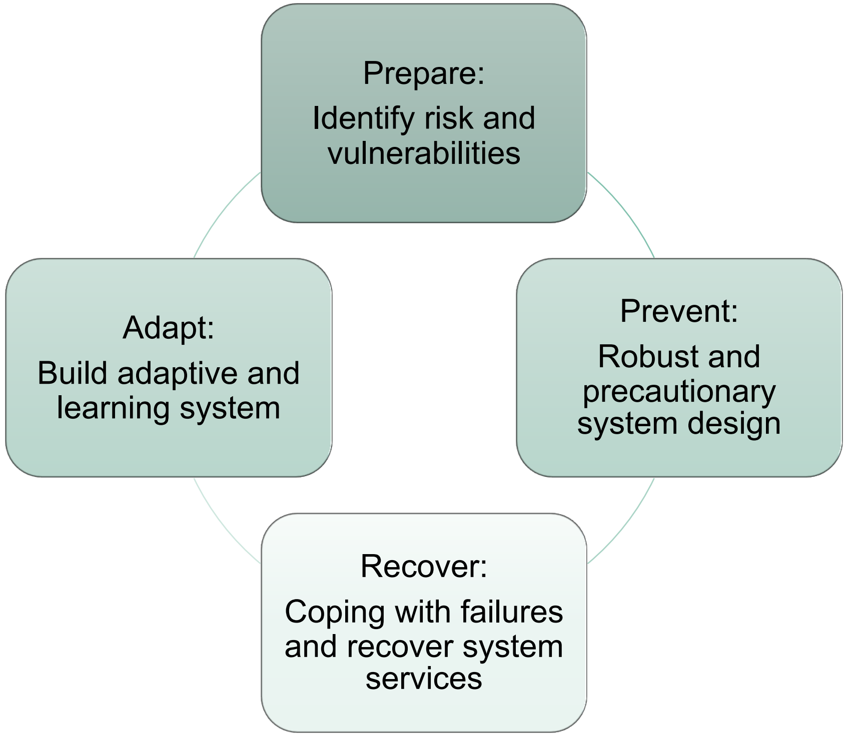
- Diversity (functional/structural)
- Geographical Dispersion
- Redundancy (numerical/functional)
- Balance of feedback mechanisms
- Flexibility / optional coupling
- Buffer and storage
- Subsidiarity
- Modularity / Cellularity
- (unallocated) Resources / Slack
- Flexibility of system service requirements (quant/qual)

Based on:
Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures.
Brand et al. (2017), Auf Dem Weg Zu Resilienten Energiesystemen! - Schlussbericht Des Vom BMBF Geförderten Projektes RESYSTRA.

Critical issues in design for resilience

- Necessary amount + combination of components is unclear
- Additional costs have to be justified (scientifically + economically)
  - How to justify costs to protect against the ‘unprecedent’?
- Trade-offs must be managed, e.g.:
  - Redundancy reduces economic + energetic efficiency
  - Diversity reduces economies-of-scale effects
  - ...

Process of implementing resilience



Based on: Acatech, Leopoldina, & Akademienunion. (2017). Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung.

Agenda

- Resilient Energy System department
- Introduction
- Theoretical framework
- **Application project**

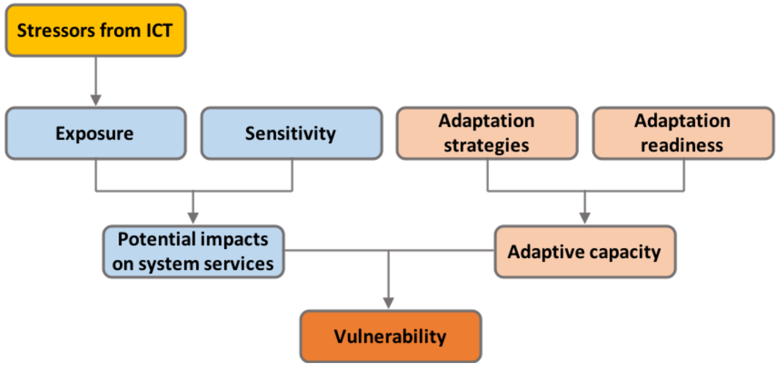
Project Objectives

- General:
  - Investigating opportunities and risks of an increasing interconnection of ICT and power systems
- Specifics:
  - Identify the properties, structures and elements critical to their vulnerability and resilience
  - Develop innovative resilience design criteria to ensure the system services are maintained, even under stress

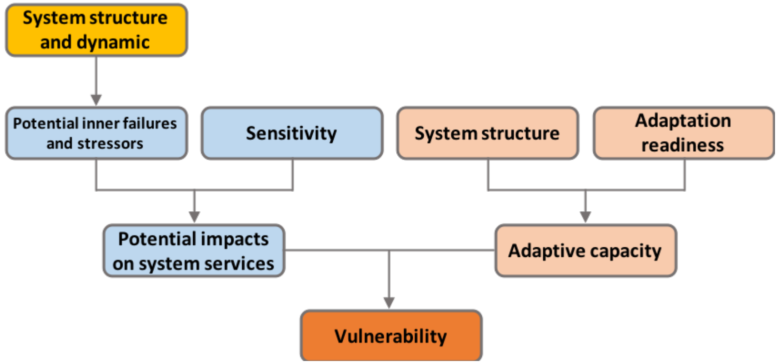
STROM ± RESILIENZ

Vulnerability Assessment Methodology

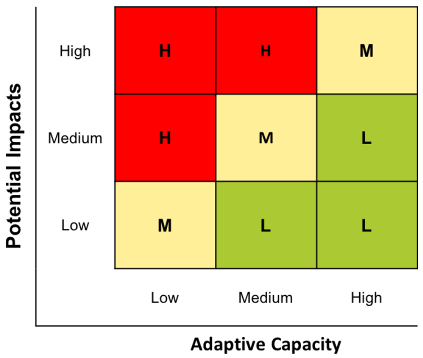
Event-based vulnerability assessment



Structural vulnerability assessment



Vulnerability Assessment Matrix



Tapia et al. (2020). Building resilient cyber-physical power systems.

Quantitative Criteria

Delivery of power

Qualitative Criteria

Direct Technical Parameters

- Power quality
- Reliability indices

Indirect Parameters

- Environmental impacts
- Economic impacts
- Public acceptance

Information assets

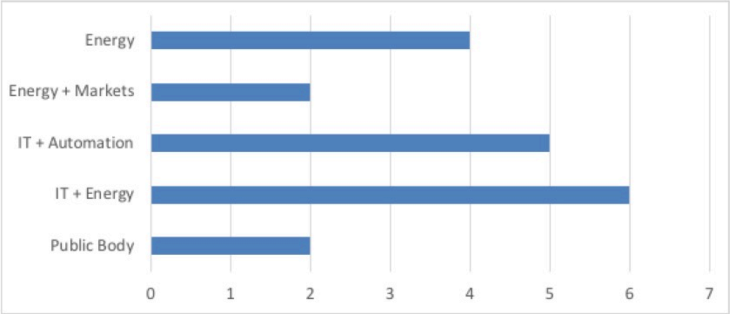
Data in transit or at rest (e.g. network state estimation, control commands, customer ID and location data, configuration data, firmware, software and drivers, time settings, etc..)

Security requirements

- Confidentiality
- Integrity
- Availability
- Non-repudiation

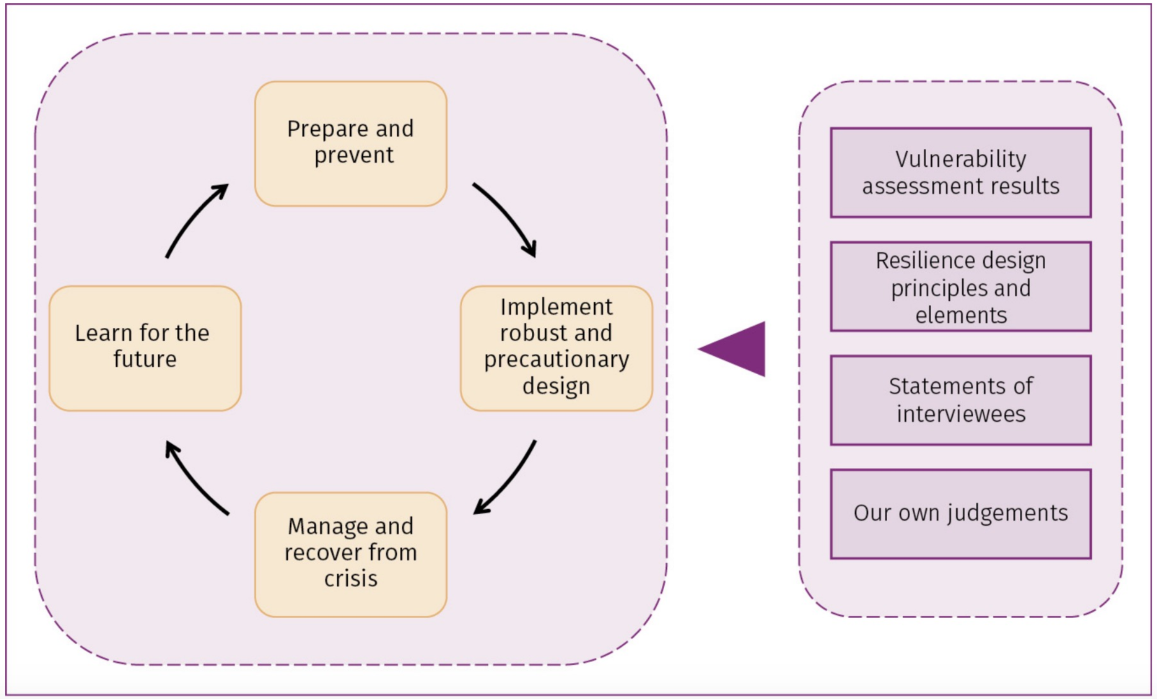
Expert interviews

- List of questions:
  - Exploring the cyber-vulnerabilities of current and envisioned future power systems
  - Investigating about potential impacts on the system service
  - Identifying adaptive capacities to prevent and cope with them
- 19 Interviews (Oct 2016 - Mar 2017)
- Statements were evaluated by means of a comprehensive qualitative content analysis



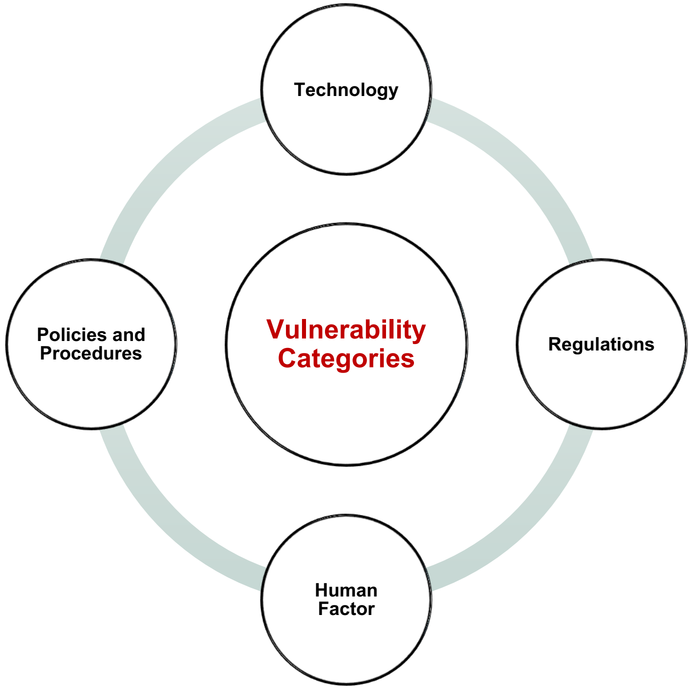
Number of interviewees

Resilience management approach



Tapia et al. (2020). Building resilient cyber-physical power systems.

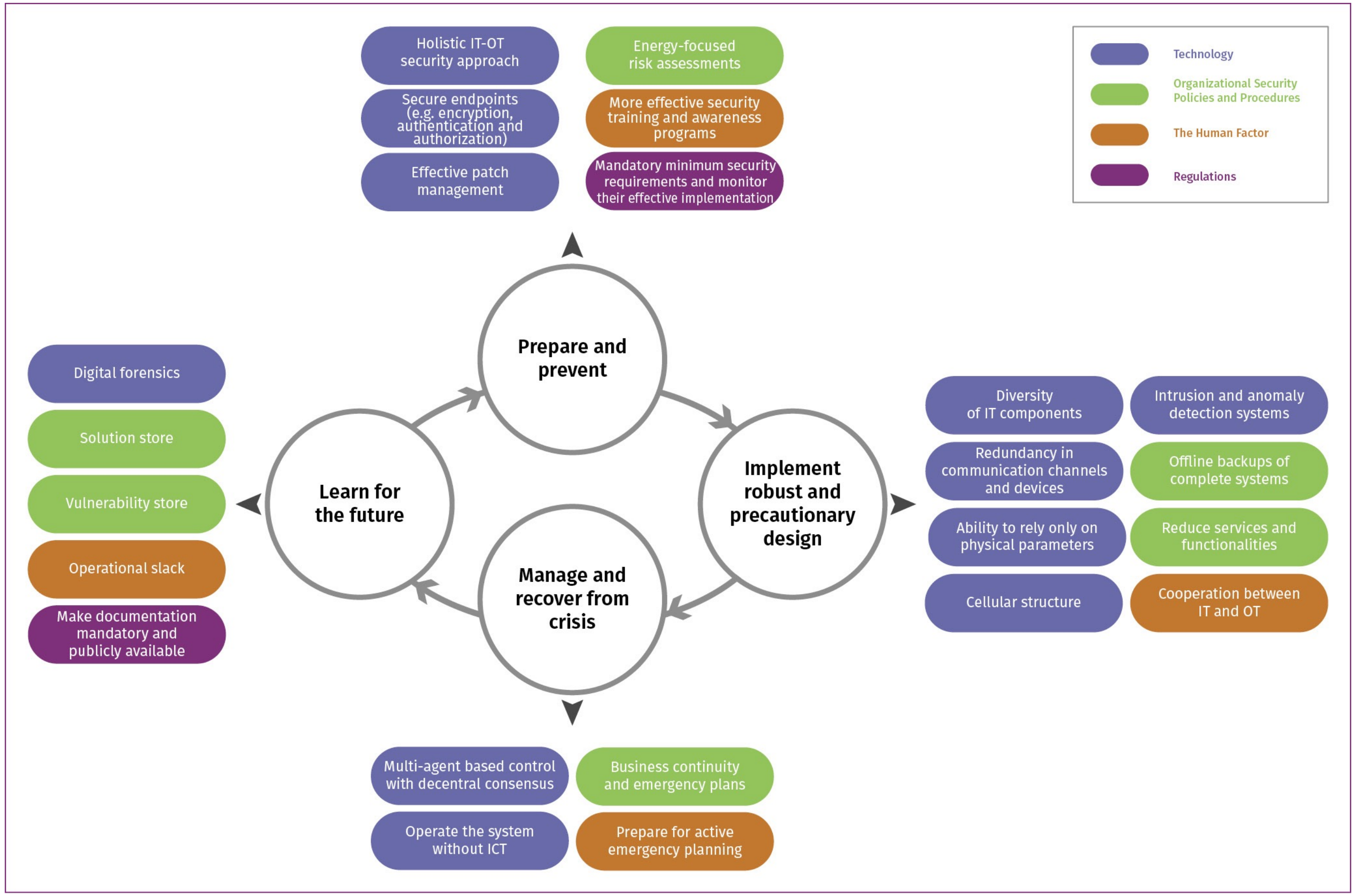
Vulnerability Assessment Results



Category	Subcategory	Potential Impacts	Adaptive Capacity	Vulnerability
Technology	Insecure endpoints	M-H	M	H
	Insecure communications	M-H	M	H
Policies & Procedures	Improper patch management	M-H	M	H
	Lack of interdisciplinary IT-OT knowledge	M-H	M	H
Human Factor	Lack of security awareness in organizations	M-H	M	H
	Lack of security awareness among consumers	M-H	L	H
Regulations	Lack of effective implementation of standards and regulations	M-H	M	H
	Lack of coordinated effort to improve security	M-H	M	H

Tapia et al. (2020b). Vulnerability and resilience of cyber-physical power systems.

Resilience management strategy



Tapia et al. (2020). Building resilient cyber-physical power systems.

Thank you for your attention!

RESILIENT
ENERGY SYSTEMS

mariela.tapia@uni-bremen.de

www.uni-bremen.de/res

References

- Gleich, A. v.; Gössling-Reisemann, S.; Stührmann, S.; Woizescke, P. (2010): Resilienz als Leitkonzept - Vulnerabilität als analytische Kategorie. In: K. Fichter; A. v. Gleich, R. Pfriem, B. Siebenhüner (Hg.): Theoretische Grundlagen für Klimaanpassungsstrategien. Bremen, Oldenburg (nordwest2050-Bericht, 1/2010), S. 13–45.
- Gößling-Reisemann, S., Wachsmuth, J., Stührmann, S., & von Gleich, A. (2013). Climate change and structural vulnerability of a metropolitan energy system: The case of Bremen-Oldenburg in Northwest Germany. Journal of Industrial Ecology, 17(6), 846–858.
- Goessling-Reisemann, S., & Thier, P. (2019). On the difference between risk management and resilience management for critical infrastructures. In M. Ruth & S. Goessling-Reisemann (Eds.), *Handbook on Resilience of Socio-technical Systems*. Edward Elgar
- Brand, U., B. Giese, A. von Gleich, K. Heinbach, U. Petschow, C. Schnülle, S. Stührmann, T. Stührmann, P. Thier, J. Wachsmuth and H. Wigger (2017), Auf Dem Weg Zu Resilienten Energiesystemen! - Schlussbericht Des Vom BMBF Geförderten Projektes RESYSTRA, Research report, Bremen: Universität Bremen & Institut für ökologische Wirtschaftsforschung (IÖW), p. 842.
- Peterson P., Dudenhoeffer D., Hartly S., Permann M. (2006) Critical infrastructure interdependency modeling: a survey of US and international research. Idaho National Laboratory
- Tredgold, T. (1818). On the transverse strength and resilience of timber, Taylor & Francis. Cited on: Cepin, M. (Ed.), Bris, R. (Ed.). (2017). Safety and Reliability. Theory and Applications. London: CRC Press
- Mallet, R. (1856). On the physical conditions involved in the construction of artillery: with an investigation of the relative and absolute values of the materials principally employed, and of some hitherto unexplained causes of the destruction of cannon in service. Longmans, Brown, Green, Longmans, and Roberts. Cited on: Cepin, M. (Ed.), Bris, R. (Ed.). (2017). Safety and Reliability. Theory and Applications. London: CRC Press
- Holling, C. S. (1973). Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics 4: 1-23.
- Walker, B., Holling, C. S., Carpenter, S.R, Kinyig, A. (2004). Resilience, Adaptability and Transformability in Social-ecological Systems. Ecology and Society 9 (2): art5.
- Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.) (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.
- Turner, B. L., II, R. E. Kasperson, P. A. Matson, J. J. McCarthy, R. W. Corell, L. Christensen, N. Eckley, J. X. Kasperson, A. Luers, M. L. Martello, C. Polsky, A. Pulsipher, and A. Schiller. (2003). A framework for vulnerability analysis in sustainability science. Proceedings of the National Academy of Sciences of the United States of America 100(14): 8074–8079
- Tapia, M., Thier, P., & Gößling-Reisemann, S. (2020). Building resilient cyber-physical power systems. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie Und Praxis*, *29*(1), 23-29.
- Tapia, M., Thier, P., & Gößling-Reisemann, S. (2020b). Vulnerability and resilience of cyber-physical power systems. Universität Bremen - Forschungszentrum Nachhaltigkeit, artec-paper Nr. 222, 124.