A framework for analysing extraordinary events in the power system

Gerd Kjølle

Senior research scientist, SINTEF Energy Research
Adjunct professor, Norwegian University of Science and Technology

Risk and Vulnerability in Infrastructures in Lund 10 – 11 May 2010

Outline

- R&D project ”Vulnerability and security in a changing power system”- ongoing work
- Challenges, key drivers and scenarios
- A framework for analysis of extraordinary events in the power system
- Analysis of previous events
- Conclusions and further work

R&D-project: ”Vulnerability and security in a changing power system”

2009 – 2012

RENERGI program, Research Council of Norway

Knowledge-building project with user involvement

People: Gerd Kjølle, Oddbjørn Gjerde, Agnes Nybø, Emil Johansson, Thomas Trötscher, Matthias Hofmann

R&D project: Vulnerability and security
Main objective:

- Build competence and knowledge regarding vulnerabilities related to the changing electric power system and thereby contribute to ensure an appropriate level of security of supply
  - Establish a scientific basis for monitoring and management of vulnerabilities in a changing power system
  - Provide a methodical framework for analyses of vulnerability and security in the development and operation of the transmission and distribution systems

- Focus areas:
  - Failures and disturbances in electric power grids leading to wide-area interruptions with severe impact on society

Vulnerability and security in a changing power system

- Indicators and methods to monitor and classify vulnerabilities in electric power grids
- Methods and operational tools for power system risk and vulnerability analysis
- Duration 2009 – 2012
- Budget: 16,6 mill. NOK ≈ 1,8 mill. Euro

Vulnerability – a definition

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat

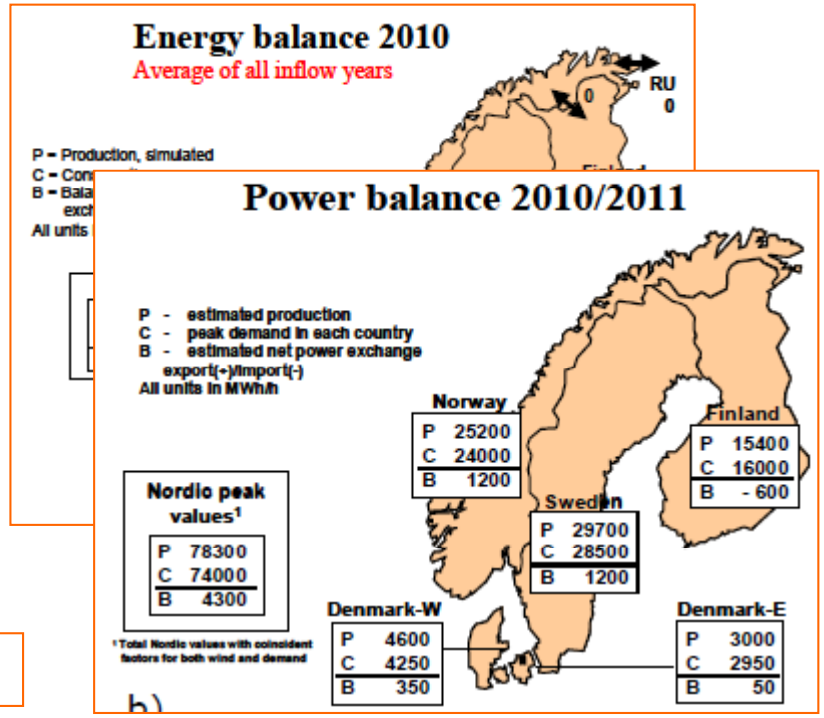
Vulnerability is closely related to security of supply

EPCIP Green Paper, COM(2005) 576 final

Security of electricity of supply - SoS

- ”***Security of electricity supply*** *means the ability of an electricity system to supply final customers with electricity*” (EU Directive)

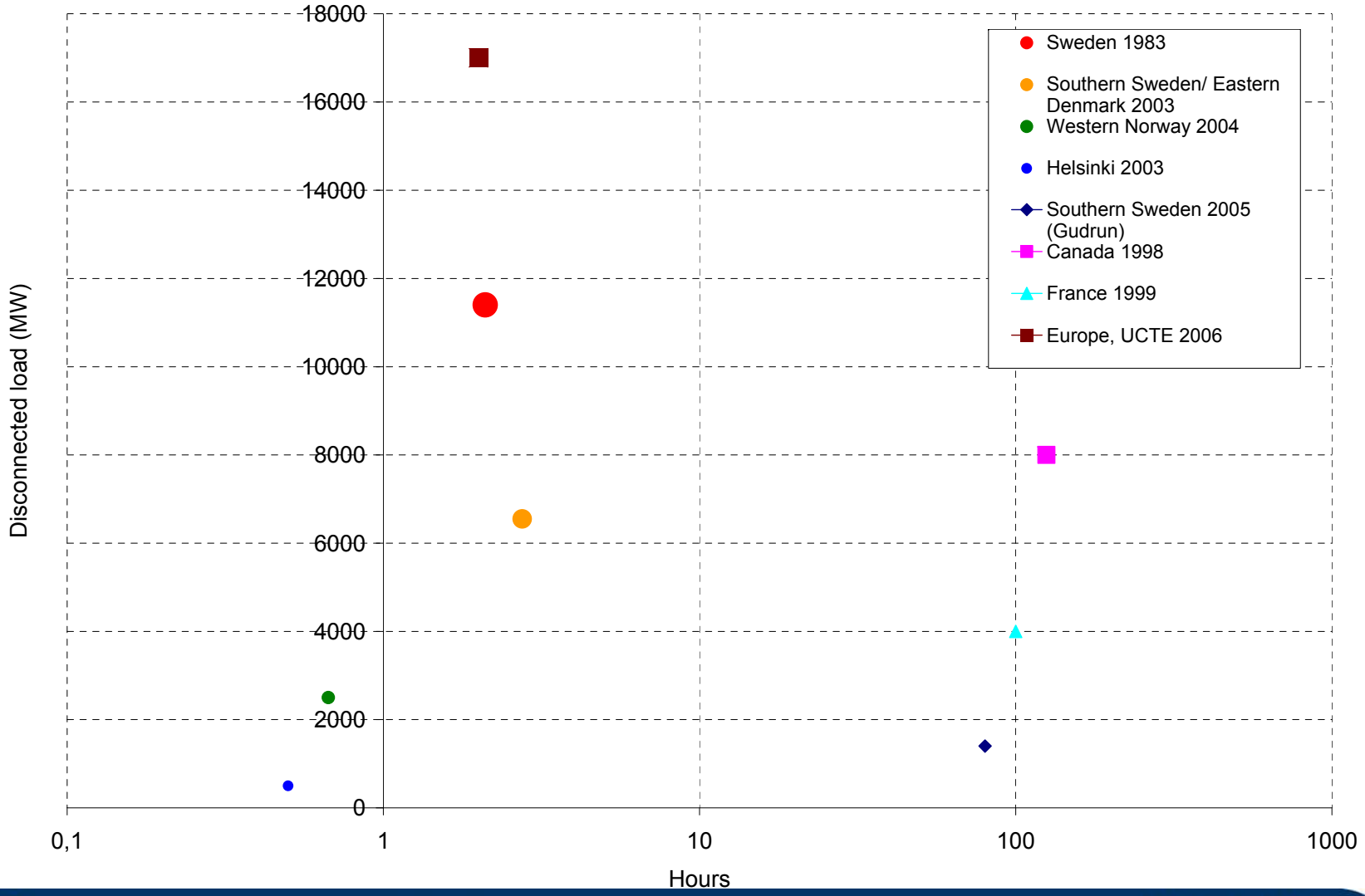
- Energy availability
- Power capacity
- Reliability



Power system failures

Challenges, key drivers and scenarios

Historical wide-area interruptions (blackouts – examples)



Challenges and some key drivers for a changing power system

- Climate changes
  - Increasing climatic stress (wind, ice loads, flooding etc)
- Power sector restructuring and technology changes
  - Ageing infrastructure
  - A strained power balance and higher utilization of the transmission grid
  - Integration of intermittent power generation (wind)
  - Transition to smart energy networks
  - Increasing dependency to other infrastructures, such as ICT
  - Workforce reductions and ageing workforce
- Society
  - Increasing electricity demand and society's dependency to electricity
  - Ageing population, recruitment to the power sector

Challenges

- Increasing strains
- Limited access to personnel and competence
- Increasing dependencies, complexity and uncertainties

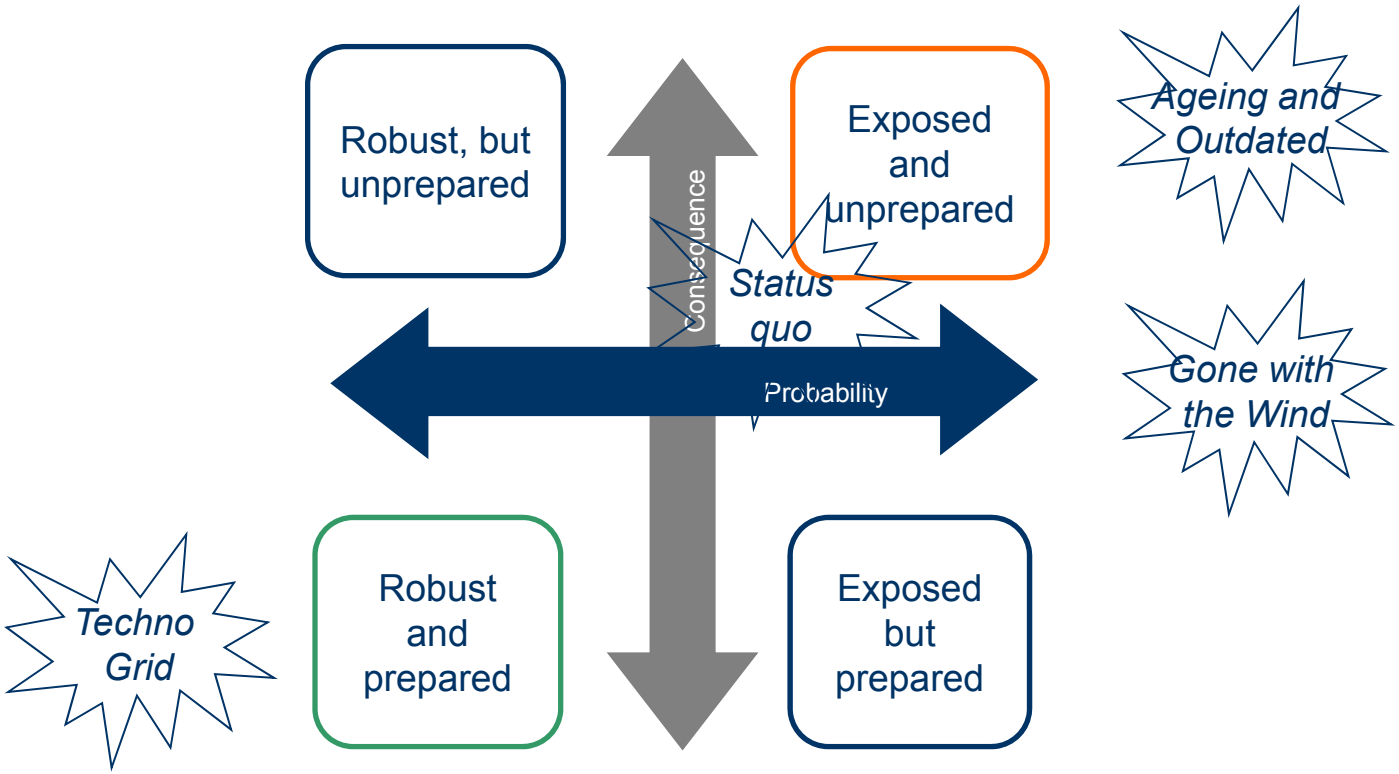
→ What will be the effect on vulnerability and security of supply?

- Probability of power system failures (unwanted events)
- Ability to handle power system failures (limit consequences)

Scenarios for a changing power system

- *"Describe **scenarios** for a changing power system, enabling the identification of threats, vulnerabilities and risks and the need for analytical tools."*
- *Status quo* – Casual adaptation
- *Ageing and Outdated* - Ageing of assets and competence
- *Techno Grid* - Integration of DG, active network and users
- *Gone with the Wind* - Climate change and extreme weather

Scenarios described according to the dimensions probability and consequence



A framework for analysis of extraordinary events

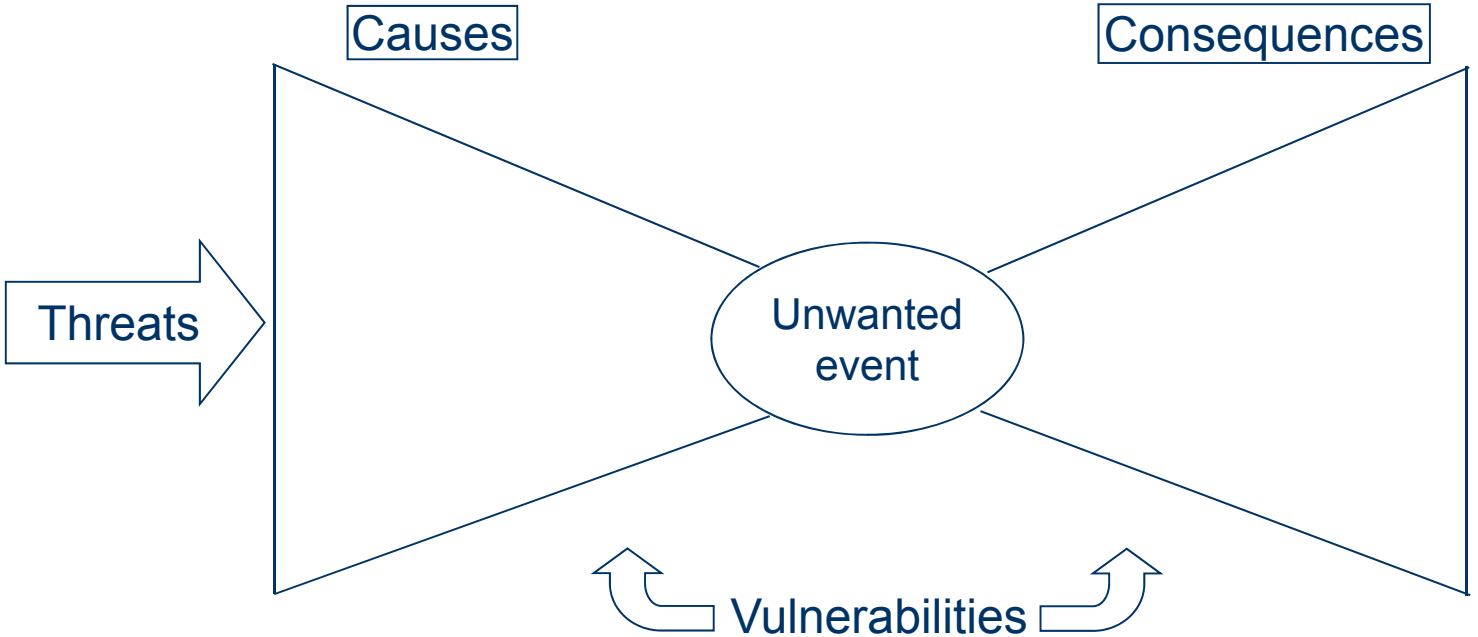
Based on two Nordic projects in 2004 and 2007 – 2009 respectively

Further developed in ”Vulnerability and security...” 2009 – 2012

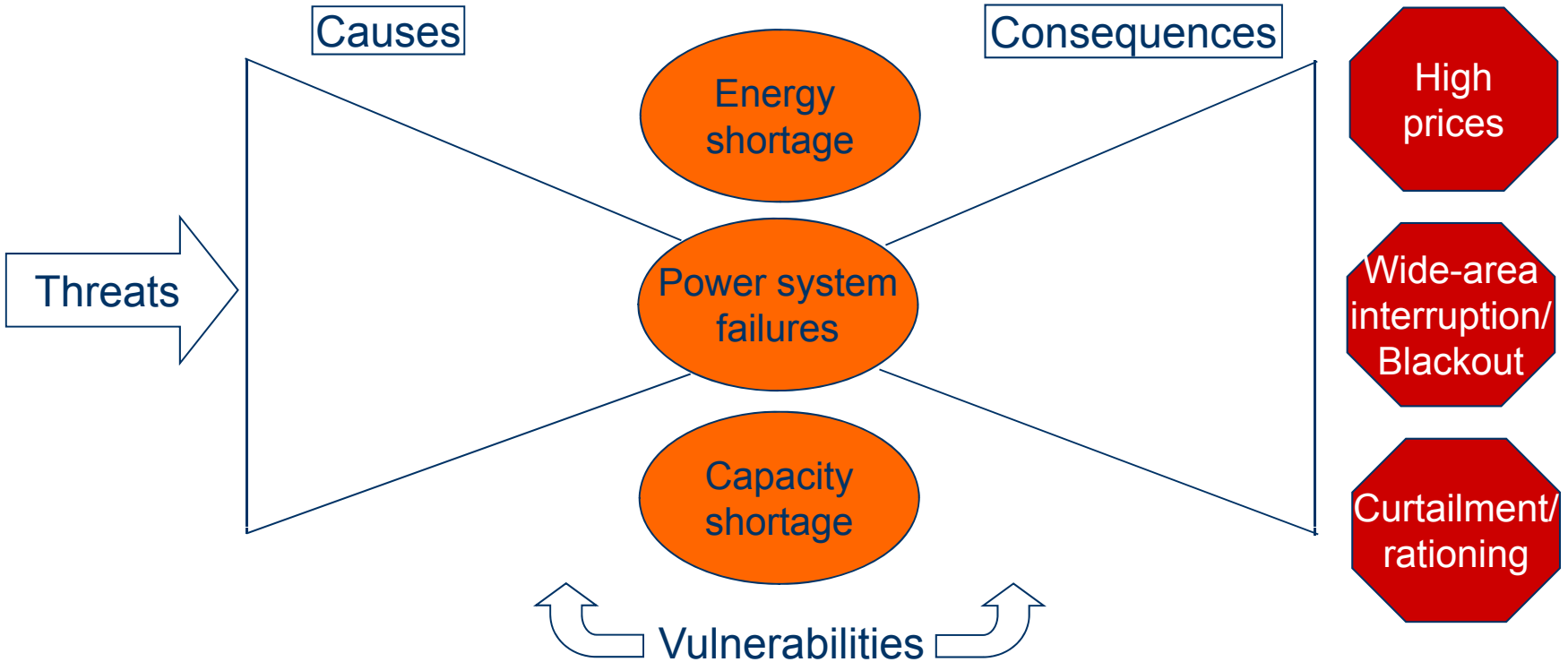
Two Nordic projects

- Vulnerability of the Nordic Power System, 2004, Nordic Council of Ministers
  - SINTEF Energy Research, Technical report A5962
- NordSecurEl – Risk and vulnerability assessments for contingency planning and training in the Nordic electricity system, 2009, EPCIP
  - Nordic energy authorities, Nordic TSOs, 4C Strategies, SINTEF Energy Research

Bow tie-model



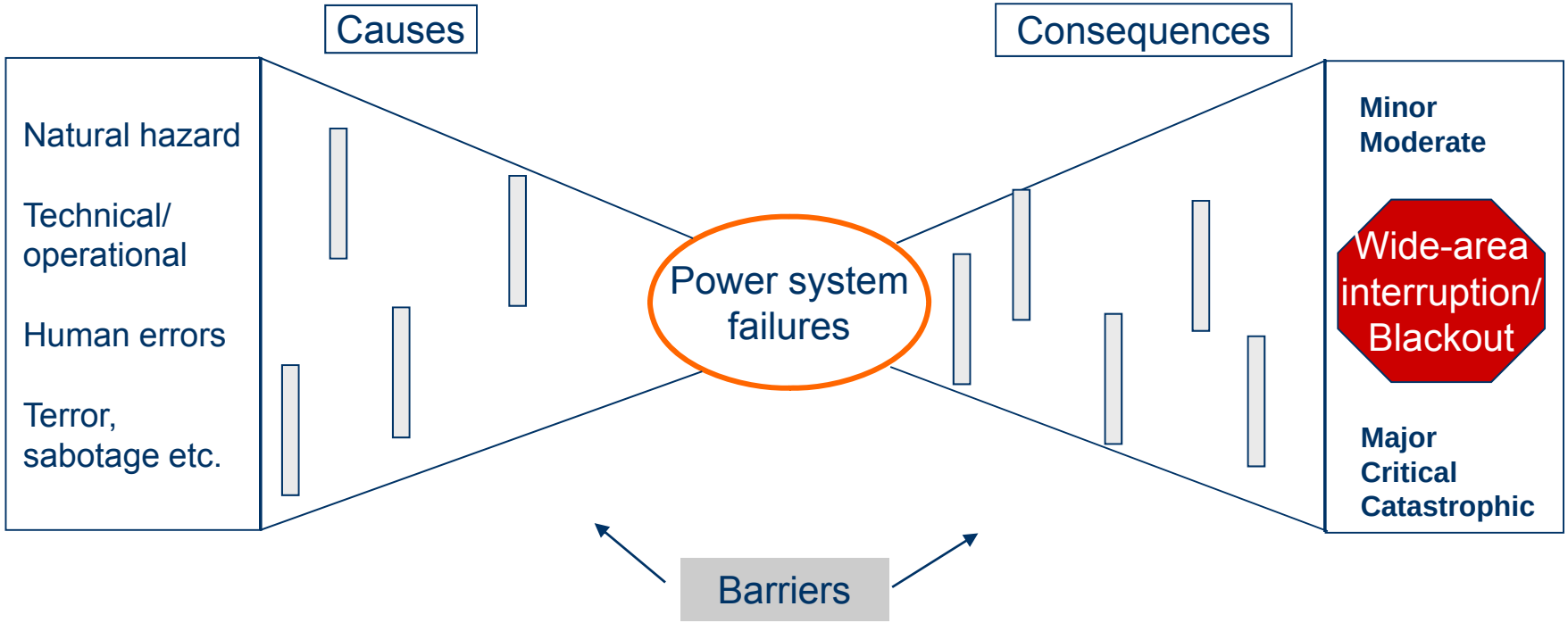
Security of supply, unwanted events and consequences



Three types of unwanted events and three types of consequences

Doorman, G., Kjølle, G.H., Uhlen, K., Huse, E.S., Flatabø, N.: Vulnerability of the Nordic Power System, SINTEF Energy Research 2004, Technical report A5962

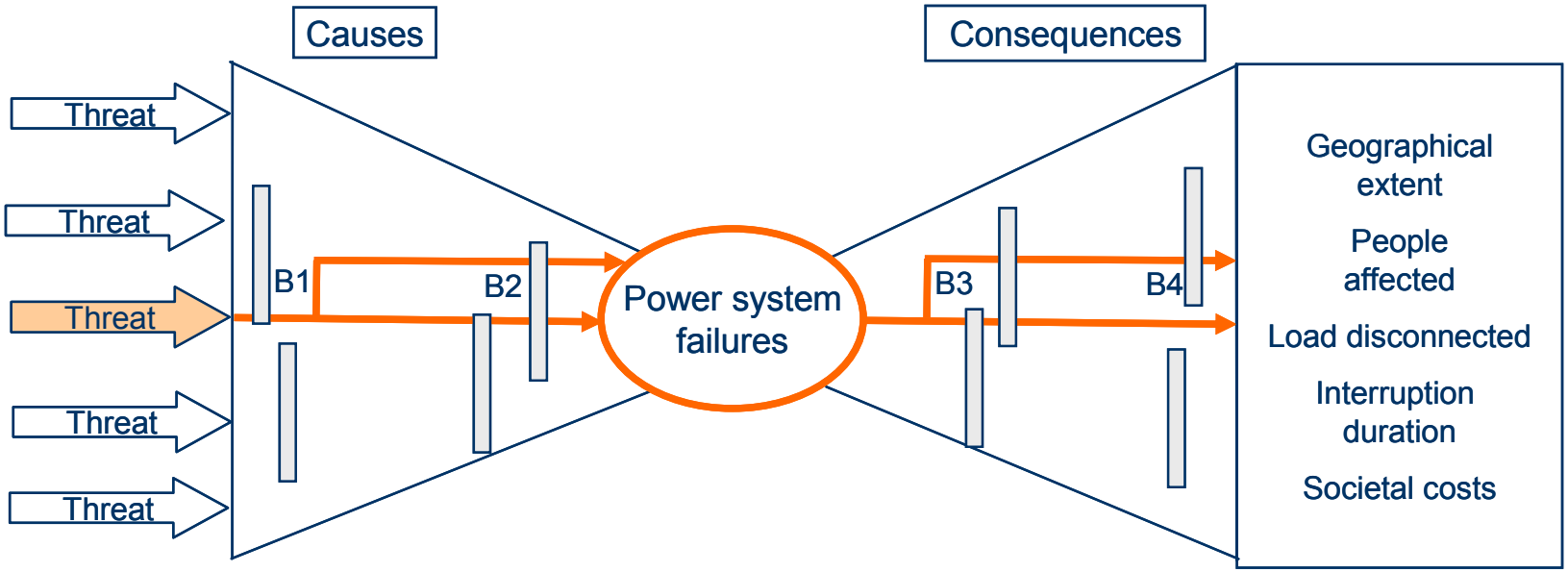
Threats, unwanted event, consequences and barriers – example for blackouts



A **barrier** is "something that can either prevent an event from taking place or protect against its consequence"

Hollnagel

Chain of events, different paths and types of barriers



B1: Prevent component failure

B2: Prevent power system failure

B3: Facilitate restoration

B4: Reduce end-users consequences

Vulnerability and types of barriers

- A system is **vulnerable** towards a **threat** if the **barriers** are weak or malfunctioning

B1: Prevent component failure,
- example: Vegetation management

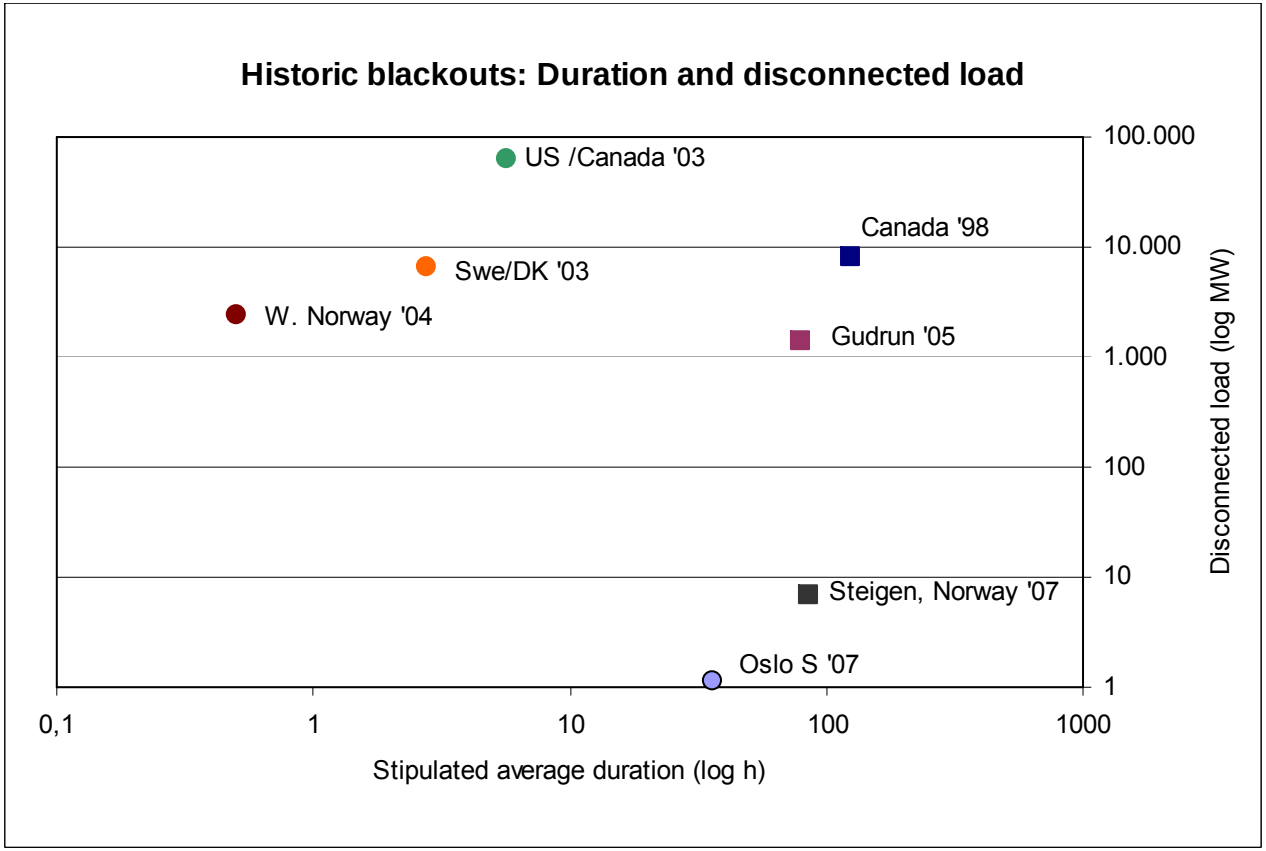
B2: Prevent power system failure
- example: Testing protection settings

B3: Facilitate restoration
- example: Standardisation of spare parts

B4: Reduce end-users consequences
- example: Reserve supply units

Analysis of previous events

What can we learn from previous blackouts?



Analysis of previous events

- Threats
- Unwanted events
- Final consequences for end-users
- Emergency preparedness, restoration of supply

- Vulnerabilities and barriers

Analysis of previous events provides useful information about need for indicators and methods to monitor and ”control” vulnerability

Events analysed and structured

- Canada 1998 – Ice storm
- US / Canada 2003 – Cascade
- Sweden/Denmark 2003 – Voltage collapse
- Western Norway 2004 – Delayed protection response

- Sweden 2005
  - Storm Gudrun
- Norway 2007
  - Storm and icing (Steigen)
- Norway 2007
  - Cable fire Oslo central station

Event	Threats	Unwanted events
Gudrun '05	Strong winds. Falling trees.	Severe damage to lines (distribution). Telecommunication, rail and road outage.
Steigen '07	Strong winds. Icing. Ageing.	Line breakages (regional and distribution).
Oslo S '07	Construction work.	Cable damage (distribution). Fire in cable culvert incl. ICT.

Inadequate barriers as contributing factors

Barriers	Sweden '05	Steigen '07	Oslo '07
Prevent component failure			
Strength and design of construction	●	O	O
Vegetation management and adequate choice of right-of-ways	●	O	
Condition monitoring		●	
Prevent power system failure			
Redundancy; reserve capacity		●	●
System operation response			O
Facilitate restoration			
Good and known restoration plan	O	O	O
Access to personnel and material	●		
Communication	●		
Coordination and clarification of responsibility	●	●	●
Reduce end-users consequences			
Alternative energy supply	●	●	●
Back-up in connected infrastructure			●
Information to the public	●	●	
● *Improvement potential.* ***O****: Some improvement potential*			

Conclusions and further work

- The framework, scenarios and previous events will help to classify events, identify barriers and vulnerability indicators, and need for analytical tools
- Complement the analysis of previous events, including nearly events
- Describe indicators, data and models needed to monitor vulnerability
- Work in progress...

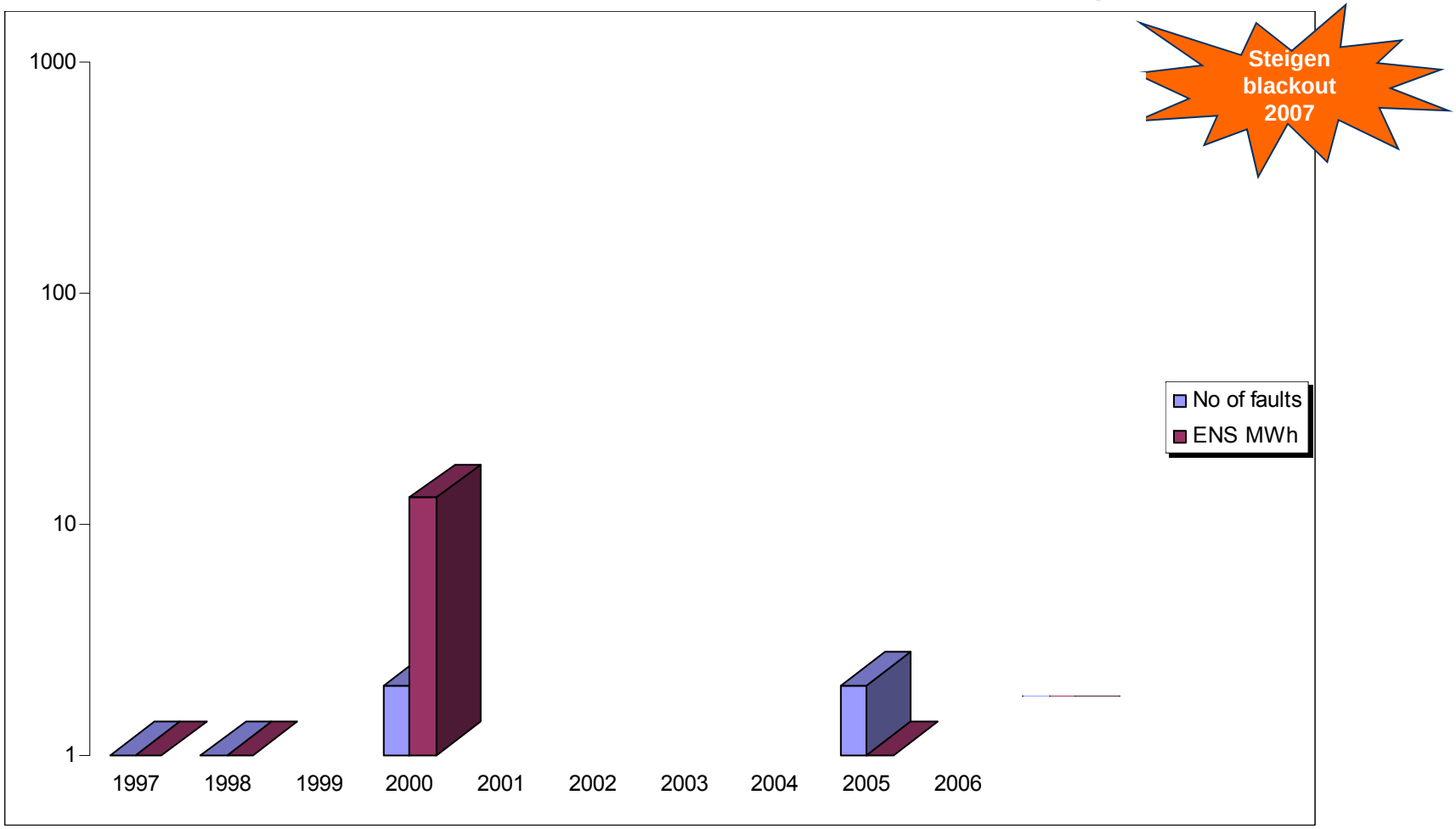
Monitoring security of supply – state of the art (in Norway)

- Energy and power balance
- Fault and interruption statistics
- Learning from blackouts/ major events
- Risk and vulnerability assessment
- Age development of assets
- Investment costs
- Maintenance and reinvestment costs

Examples of SoS-indicators in use

- Number of interruptions
- Interruption duration
- Energy not supplied
- Interruption costs
- Cost of very long interruptions (> 12 hrs)
- Fault rate
- Number of line repairmen
- Number of reserve units
- Vegetation management (frequency etc.)

Example from fault statistics, 66 kV overhead lines in North of Norway



Fault statistics give historical information about failed components only