Research and Education in Risk and Safety

Dr. Eng. Wolfgang Kröger, Professor and Director
Laboratory for Safety Analysis, Institute of Energy Technology,
Dept. for Mechanical and process Engineering, ETH Zurich &
Founding Rector of the Int. Risk Governance Council, Geneva

Media Tour “Emergency Preparedness” (Zurich, 21 April 2009)

Basic Safety Approach: Putting preparedness in perspective

Avoid/eliminate hazardous substances and processes

⇩ If no (not sufficient)

Avoid failures and incidents by high quality of technical and organisational means

⇩

Stop incidents to develop into severe accident scenarios by highly reliable safety systems and barriers

⇩

Reduce risks, in particular mitigate consequences by prepared and trained accident management

⇩

Reduce offsite risks by planned emergency measures, i.e. evacuation

All must be based on deep understanding/sufficient knowledge, readiness to become aware and get prepared – often targets or acceptability criteria are needed

...if not done adequately: Eschede, 3. 6.1998

- Single failure („Radreifen“, 200 km/h) causing unexpected event chain
- 120 people killed; high financial losses, loss of reputation and market chances

Safety concept according to Swiss HSK-R-100

Safety level	Cate-gory	Frequency H per year	Verification	Goal	Dose limit environment
Normal operation				Prevention of incidents and accidents, minimisation of radiation to workers	
Incidents		H>10E-01	Covered by deterministic accident analysis		Q-DRW [1)]
Design base accidents	1	10E-02< H<10E-01	Deterministic accident analysis, safety systems are available as required	Prevention of damage to: - safety relevant components - fuel clading	Q-DRW
	2	10E-04< H<10E-02		Limitation of damage to: - safety relevant components - fuel clading	1 mSv
	3	10E-02< H<10E-04		Assuring the - coolability of the reactor core - integrity of the containment	100 mSv
Beyond design base accidents		H<10E-06	PRA	Limitation of the consequences by including the radioactivity or the controlled release of radioactivity into the environment (internal accident management)	-
			Emergency preparedness	Mitigation of radiological consequences in the environment (external accident management	-

[1)] specified guiding figures

Focus at ETH: Prevention and development of analytical tools for

- Reliable and robust system design and integration
- Risk and vulnerability analysis of single complicated (e.g. NPPs) and networked complex systems (e.g. electric power supply – interconnected critical infrastructures)
- Provision of scientific support for strategic decision making

Witnessed and future trends: Key drivers

- Technological developments, pervasive use of computer-based ICT
- Greater and tighter integration of systems
- Changing, more stressing operational environment, e.g., deliberalised markets
- Broadened set of hazards and threats, e.g., extreme weather conditions, malicious attacks

Risks / Threats to Energy and Transport Security: Multifacetted

- **Natural events** such as earthquakes, hurricanes, tornados, severe flooding, or other (increasing) extreme weather conditions
- **Accidents or (combination of) technical failures** leading to the depilation of plants, networks and operations
- **Market factors** such as cartel induced production limits, instability associated with major producer groups, or economic pressure trading-off security factors, lack of adequate investment
- **Policy factors** such as artificial supply limitations or negative pricing outcomes or misusing “energy” for political purposes
- **Human factors** including unintentional and malicious attacks carried out against physical energy infrastructures or cyber-attacks

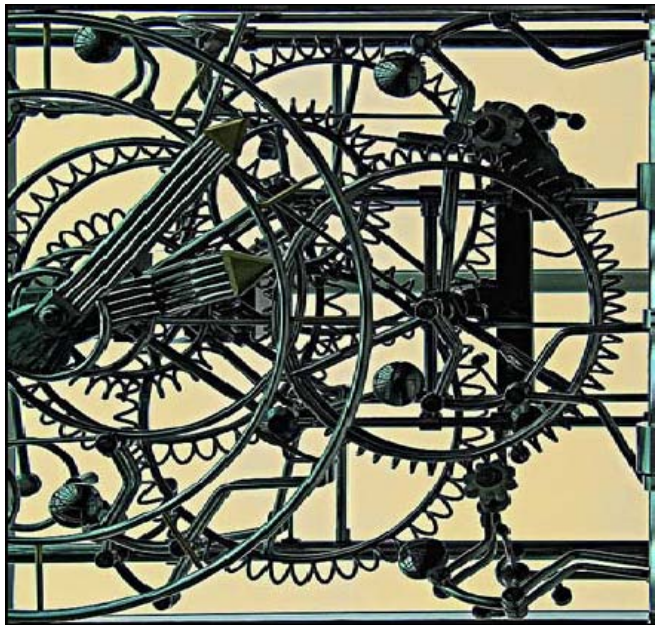
Major challenge : From reliability engineering of complicated systems ...

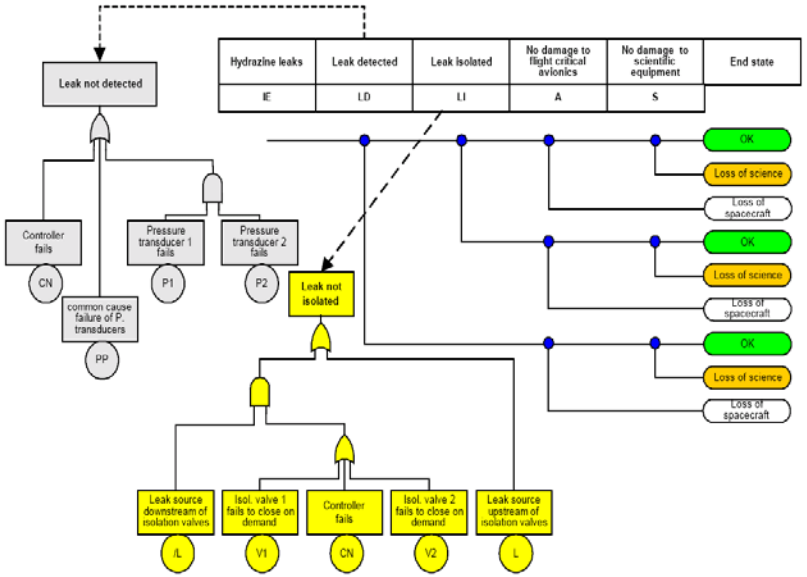
Problems:

- Numerous variables, highly integrated
- Structure stable over time, low dynamics
- Analytical thinking and diligence sufficient

Methods:

- Decomposition of systems, causal chains; PSA framework
- Further development required, e.g. human factors





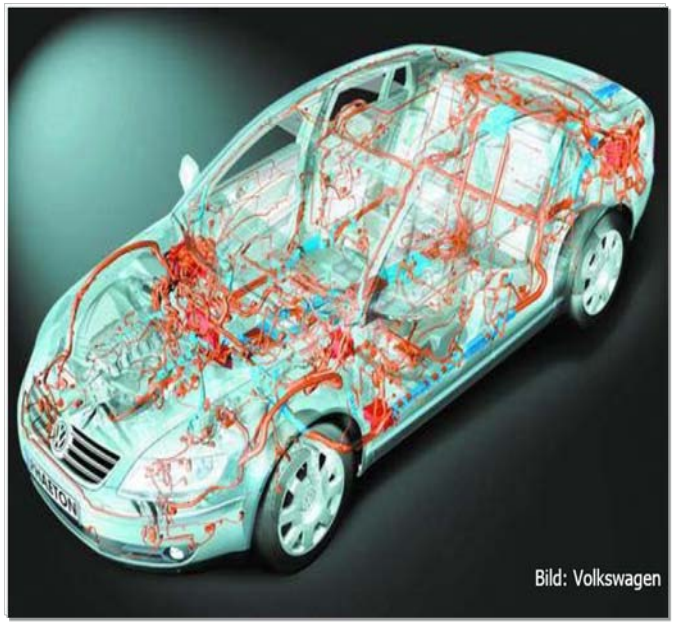
... to reliability engineering of complex systems

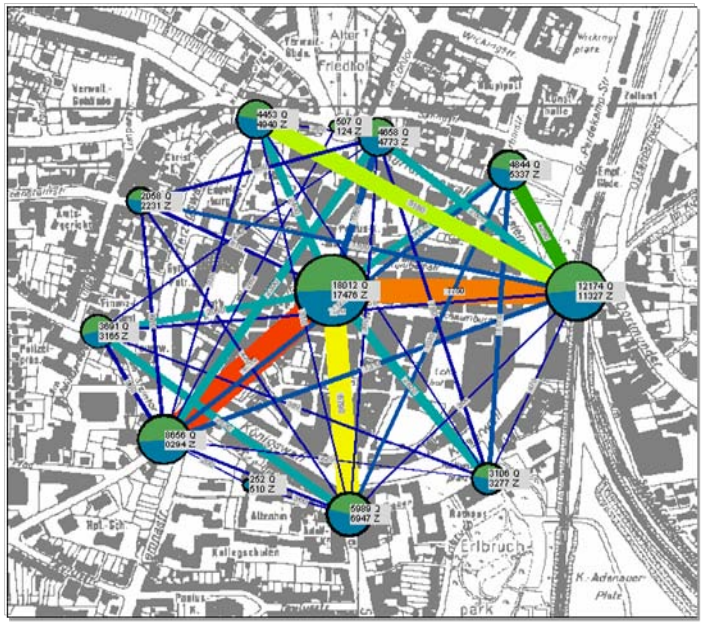
Complex systems:

- Inadequate information about elements, states and interactions
- Nonlinearities, adaptive emergent behavior
- Feedback loops
- Tend to create surprise

Problems:

- System behavior unequal sum of single elements' behavior
- Strong interdependencies
- Need to model and simulate „system-of-systems"





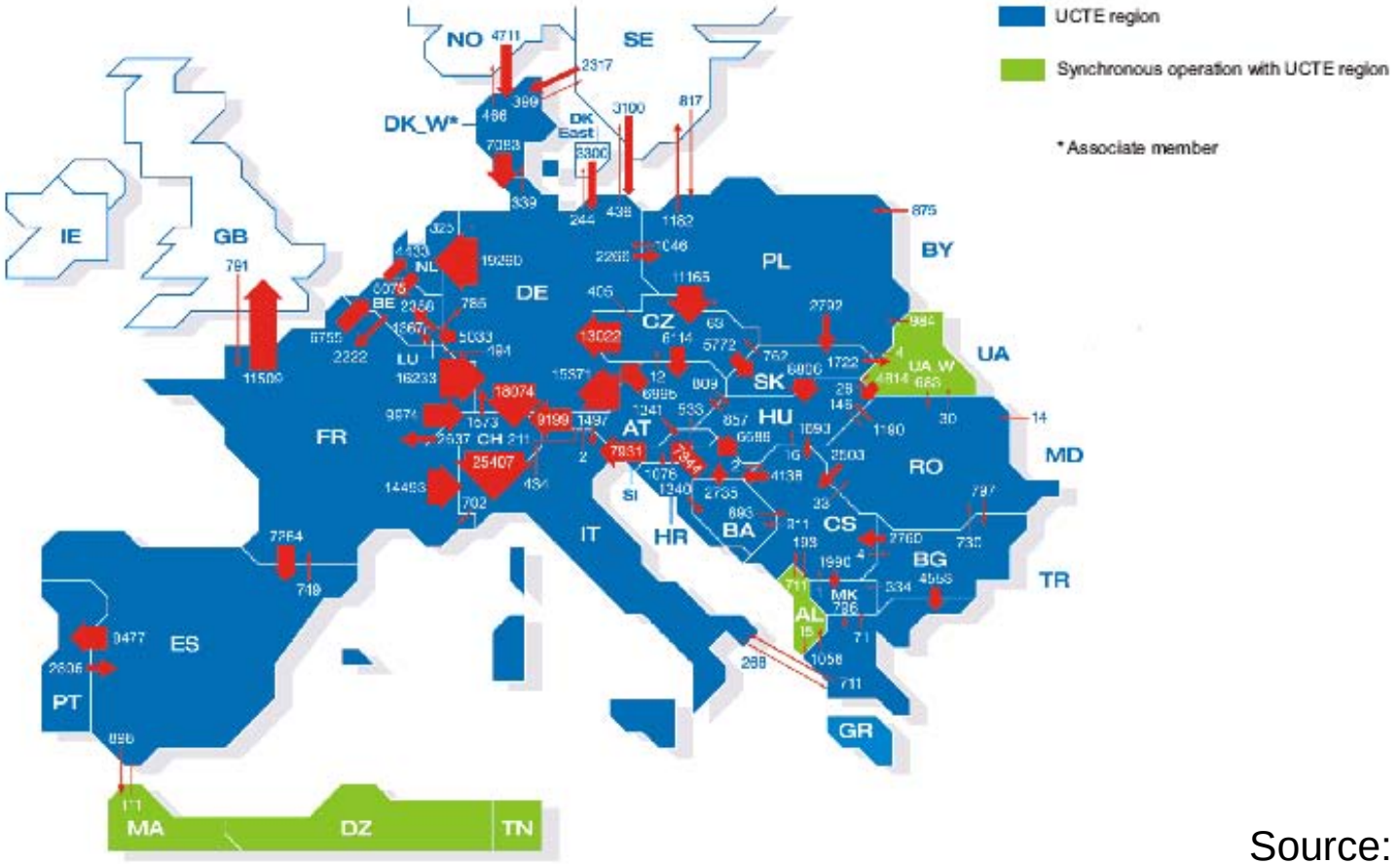
ETH–offer with reference to technical systems: Education

- Lectures within Master and PhD Programs on methods for
  - Reliability Analysis
  - Risk and Vulnerability Analysis of highly integrated systems (in a regional context)
  - Nuclear safety assessment (PRA)
- (Postgraduate) Certification Course of Applied Sciences on ‘Risk and Safety’
- PhD research projects on development and application of advanced methods

Transboundary Physical Energy Flows (GWh) in 2005

UCTE synchronized network serves 450 million people, provides 2400 TWh/a

(10% transborder exchange at present)



Source: UCTE 2006

Electric power supply systems: Recent major blackouts

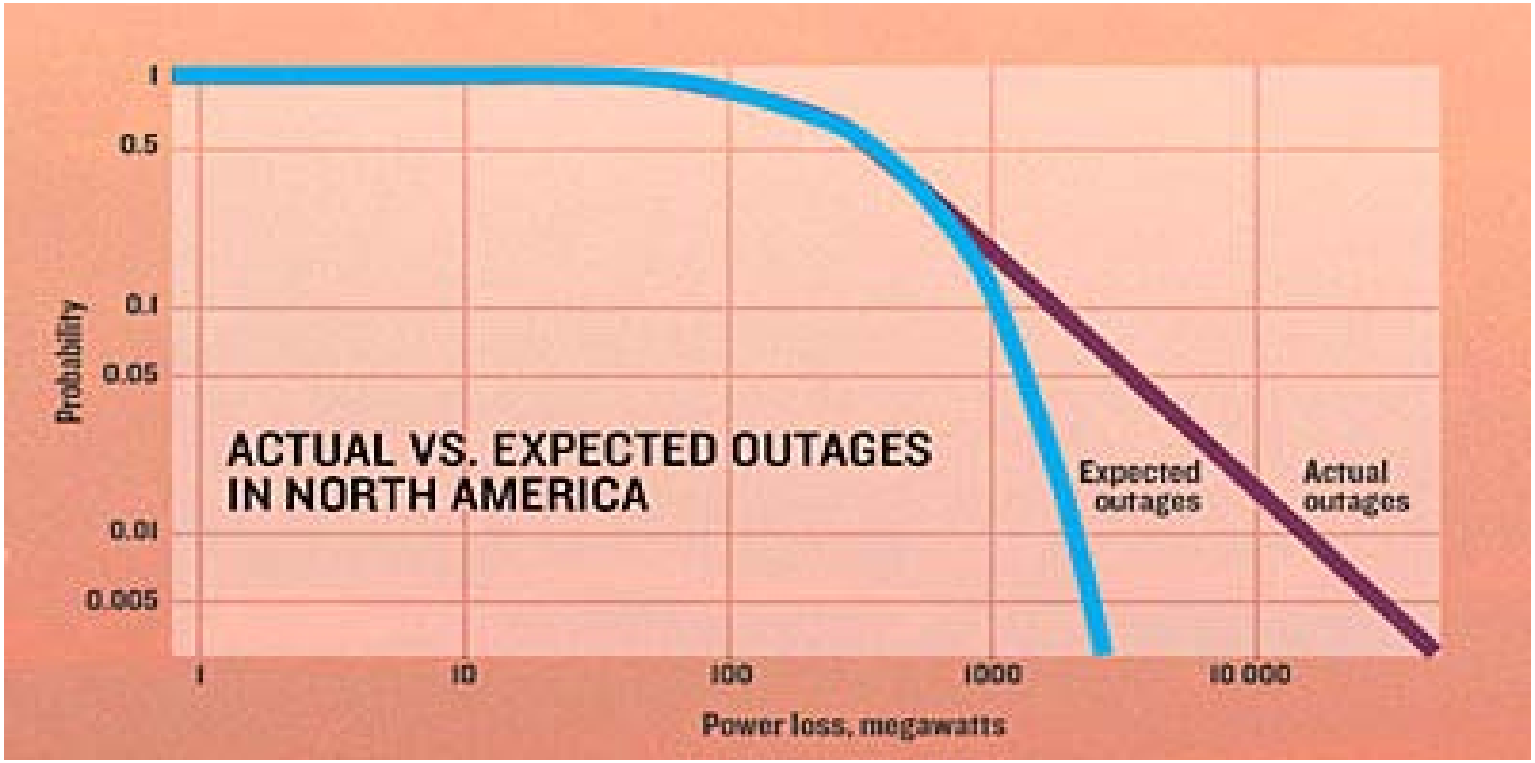
Blackout		Load loss [GW]	Duration [h]	People affected	Main causes
Aug. 14, 2003	Great Lakes, NYC	~ 60	~ 16	50 Mio	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighbouring TSOs
Aug. 28, 2003	London	0,72	1	500´000	Incorrect line protection device setting
Sept. 23, 2003	Denmark / Sweden	6,4	~ 7	4,2 Mio.	Two independent component failures (not covered by N-1 rule)
Sept. 28, 2003	Italy	~ 30	up to 18	56 Mio.	High load flow CH-I, line flashovers, poor coordination among neighbouring TSOs
July 12, 2004	Athens	~ 9	~ 3	5 Mio.	Voltage collapse
May 25, 2005	Moscow	2,5	~ 4	4 Mio	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0.2	~ 3	200´000 passengers	Non-fulfilment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug. 14, 2006	Tokyo	?	~ 5	0.8 Mio households	Damage of a main line due to construction work
Nov. 4, 2006	Western Europe (“controlled” line cut off)	~ 14	~ 2	15 Mio. households	High load flow D-NL, violation of the N-1 rule, poor inter TSO-coordination

Some Lessons Learned from Recent Major Blackouts

- Operation of the systems beyond the original design parameters (market liberalization, integration of wind power, etc.)
- Malfunction of critical equipment and adverse behavior of protective devices; insufficient system automation in some cases
- Lack of situational awareness and short-term emergency preparedness
- Limited real time system monitoring beyond the TSO's* control area and poor timely cross-border coordination
- Inadequacy of N-1 security criterion, of its implementation/evaluation

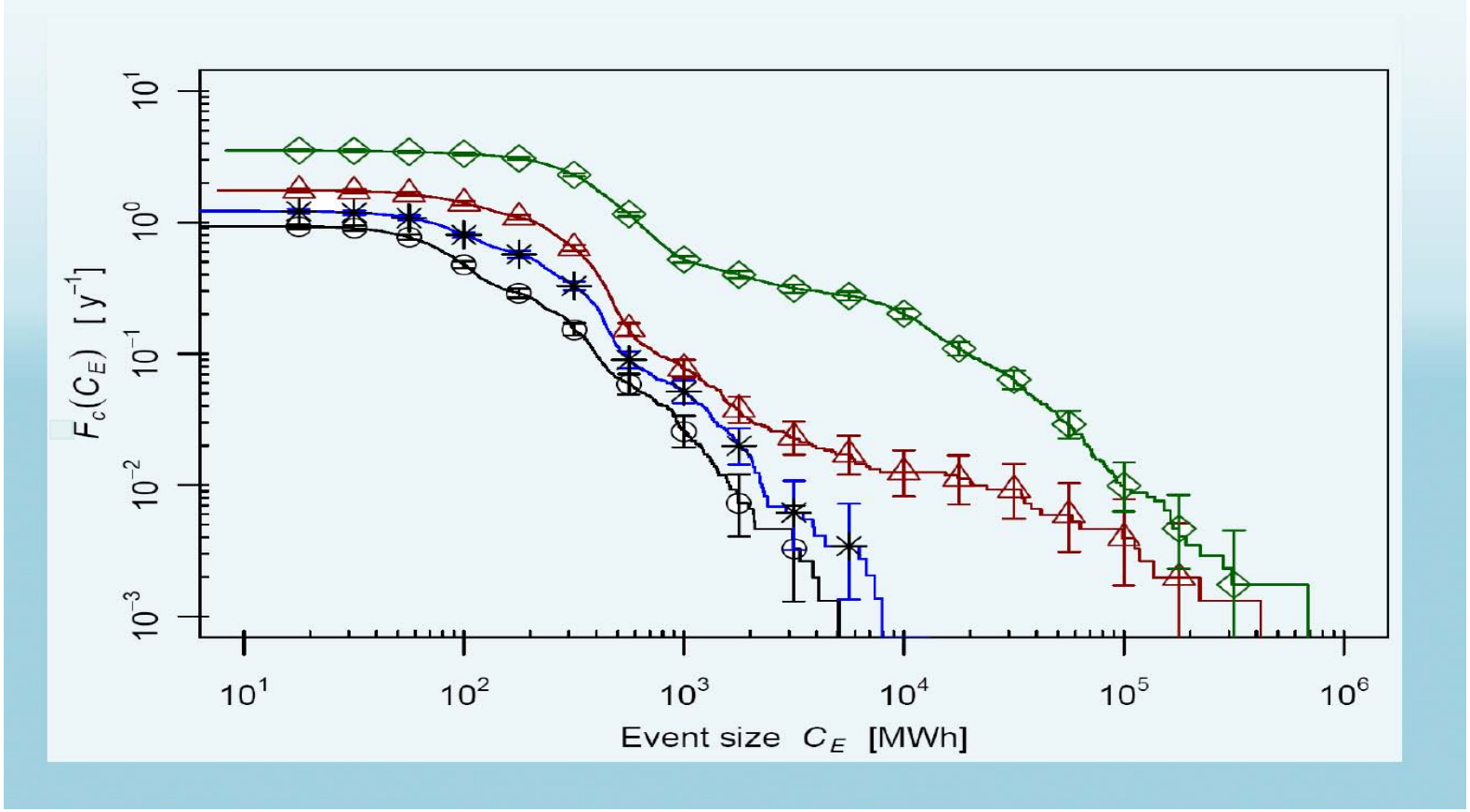
*Transmission System Operators

Analysis of Interruption Data



Cascading failures in the North American electricity grid have been more common than one might expect. Forty-six of the events between 1984 and 2000 , or nearly three per year, involved losses of >1,000MW. The probability of smaller power losses follows an exponential curve, for losses >500 MW a law typical for self-organized systems [compiled by J. Apt, 2004]

Sensitivity of blackout frequencies to increased grid loads



Complementary cumulative blackout frequencies for four different grid load levels L=100% (circles), 110% (stars), 120% (triangles) and 137% (diamonds)

Source: M. Schläpfer, 2008

Results: Influence of operator response time on 'Expected Energy Not Supplied' - factor 3

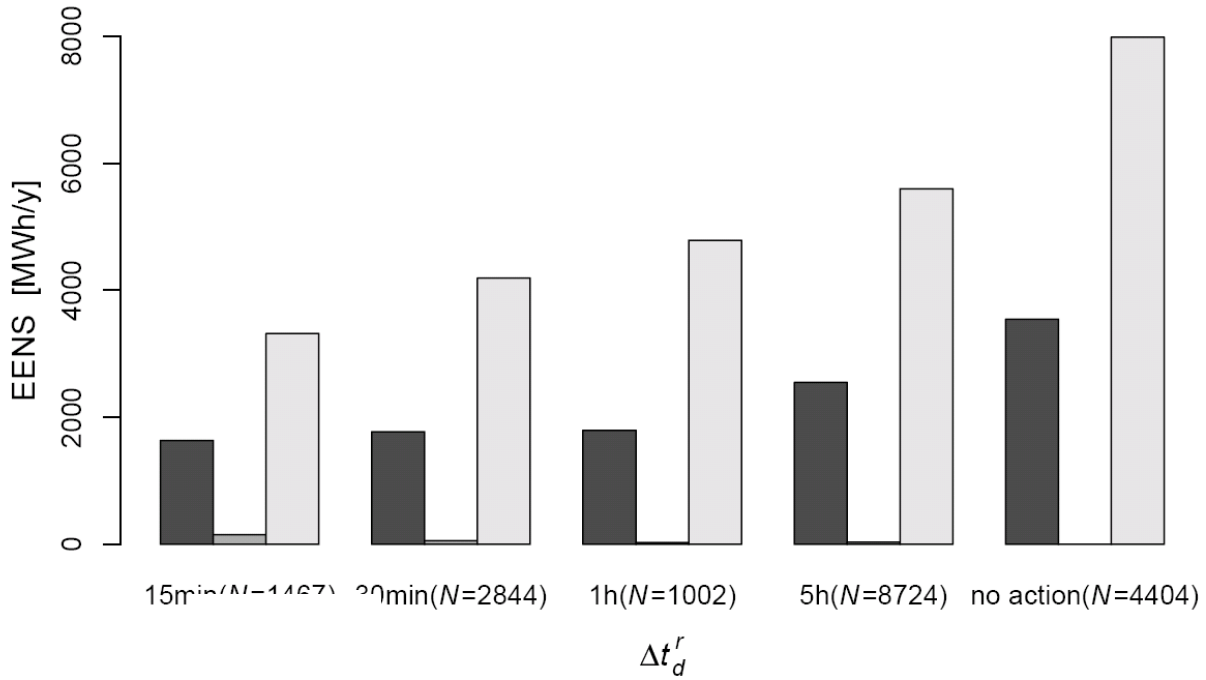


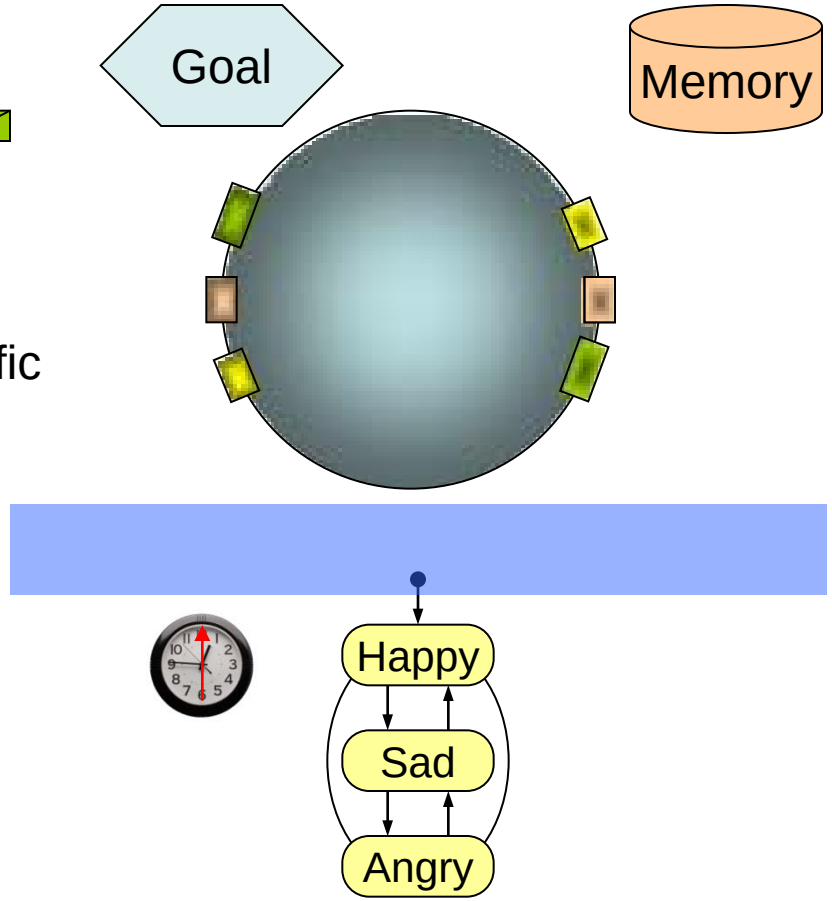
Figure 7: Influence of the operator response time on the EENS due to generation inadequacy (left, black bar), operator action (middle, dark-grey bar) and system splitting (right, light-grey bar) for L=1.37.

Object-oriented modeling approach: Framework

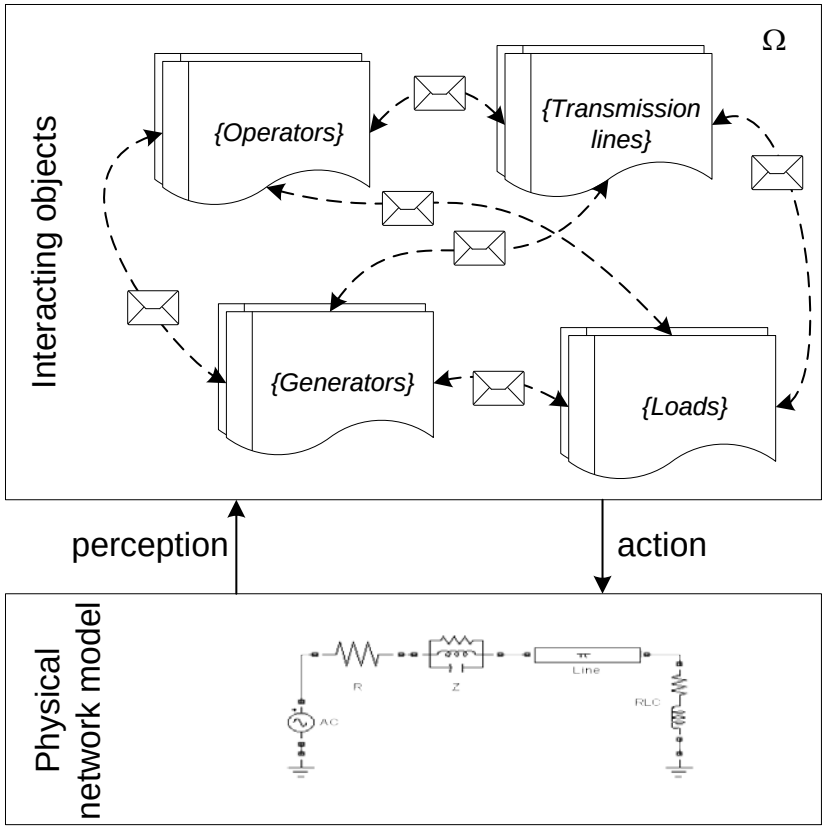
- Modeling the behaviour of the **components** (objects) and their interactions
- Stochastic simulation (Monte Carlo) of all components to investigate the **macro-behaviour** of the whole system
- Observed scenarios and system states are not predefined but emerge during the simulation (**emergence**)
- Frequency and consequence of events are determined "**experimentally**"

Introducing the term “object”

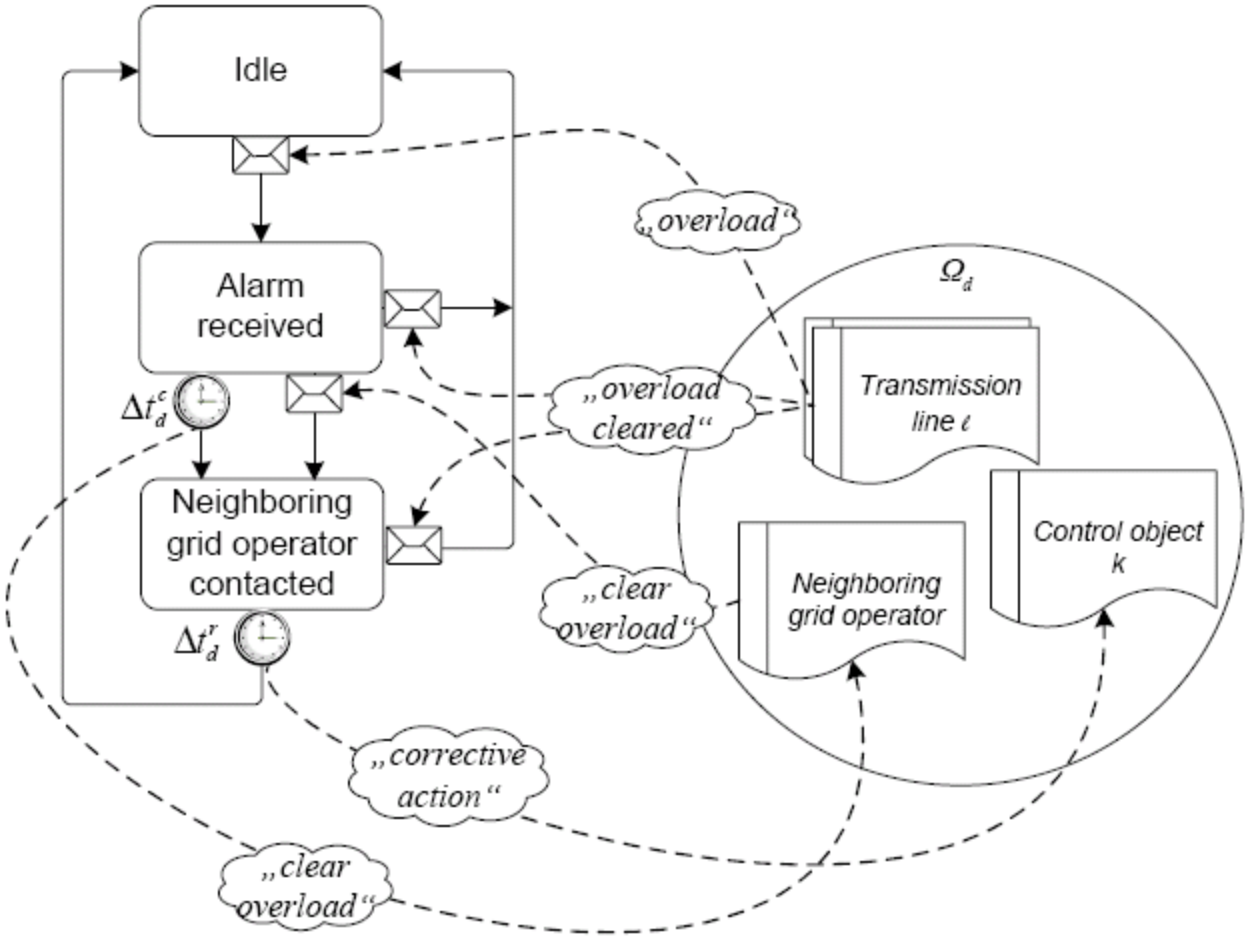
- **Has different states (Finite State Machine, FSM)**
- Is capable of interaction with its environment (e.g. other objects)
- has „receptors“ and „effectors“ for specific („messages“) and non-specific (environmental variables) signals
- Can act randomly
- May have a memory (learning)
- Can strive for a goal



Two-layers ABM-concept applied to the electric power system



Operator Action Model



Evidenced importance: Telco mini blackout (1/2)

Major telecommunication service node affected in Rome, 2 January 2004 :

- At 5.30 a.m. breakage of a pipe caused flooding of the first floor (cables of nodes located beneath)
- Telco devices for voice services were flooded (such devices connect different operators for fixed and mobile services)
- Fire Brigade arrived at 7:30; worked until 7:46 a.m. - pumping out water
- Technicians had to shut down the air conditioning plant
- Several boards/devices failed for short circuit, main power supply went out of service

Source IRRIIS

Telco mini blackout (2/2)

- Diesels failed to start due to flooding; only batteries provided power to supply still working boards/devices, finally one battery also dropped
- For five minutes last working boards/devices were not powered at all
- Other twenty minutes were needed to restore own services

Affected Infrastructures:

- Satellite system interruption caused ANSA print agency transmission problems
- Delays and troubles at Fiumicino airport (failure of check-in system, 70% of carriers affected)
- Delays and service perturbations at post offices and banks
- Blackout impacted ACEA services (power grid), operator lost monitoring and control of all remote unmanned substations

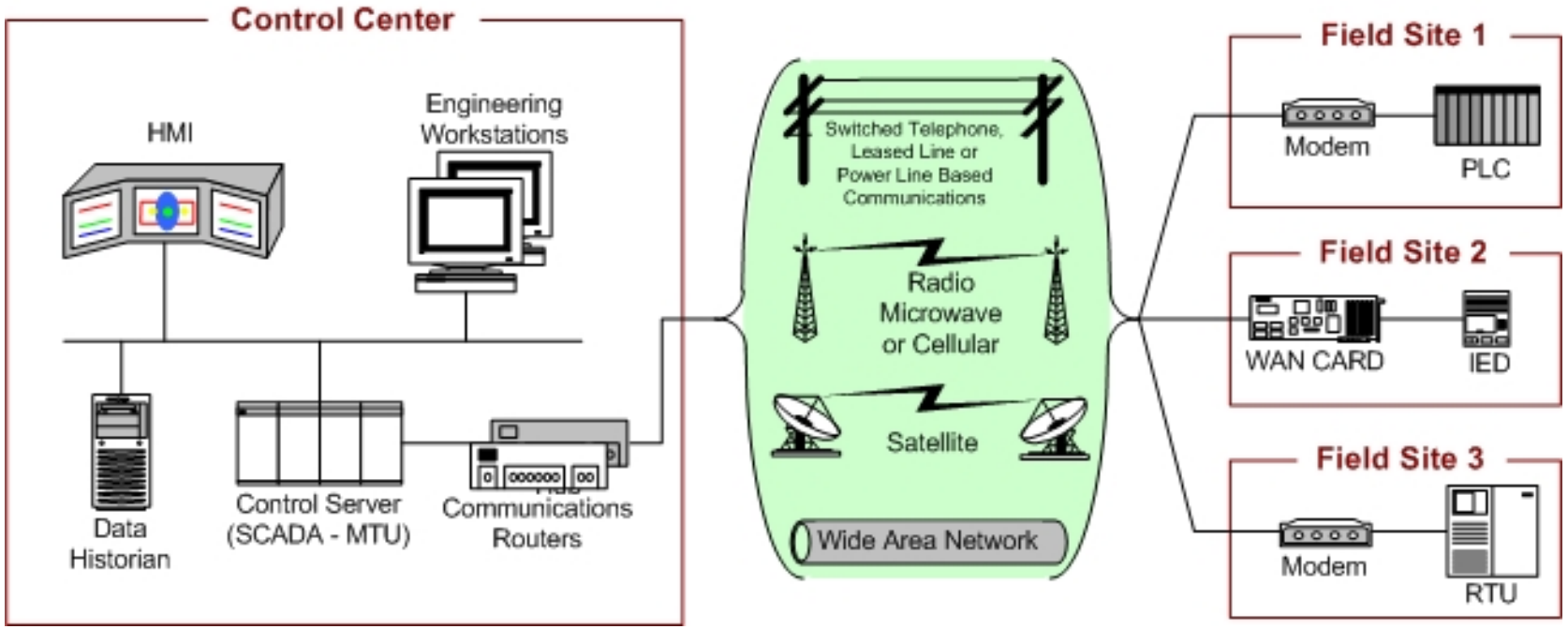
Importance of geopolitical hazards / cyber attacks

In 1982, the CIA exploited software transferred to the Soviet Union that operated pumps, turbines & valves of the pipeline. It caused the software to malfunction and to reset the pump speeds and valve settings.

The result was the largest non-nuclear explosion and fire ever seen from space. TNT equivalent 3 – Hiroshima 14-20 kilotons

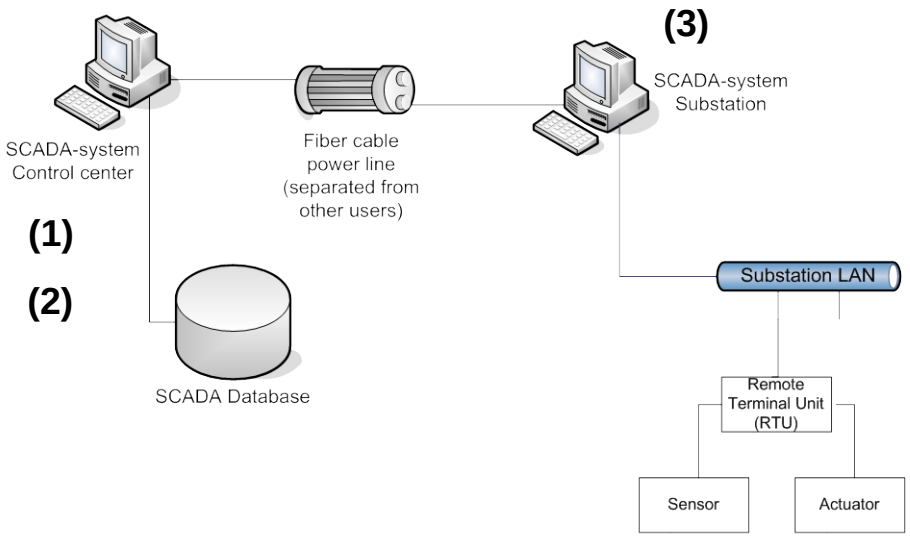
Source: J. Westby

SCADA System General Layout



Quelle: NIST SP800-82

SCADA System (real Swiss case)



(1) Dedicated data exchange between power stations and network operator via PIA

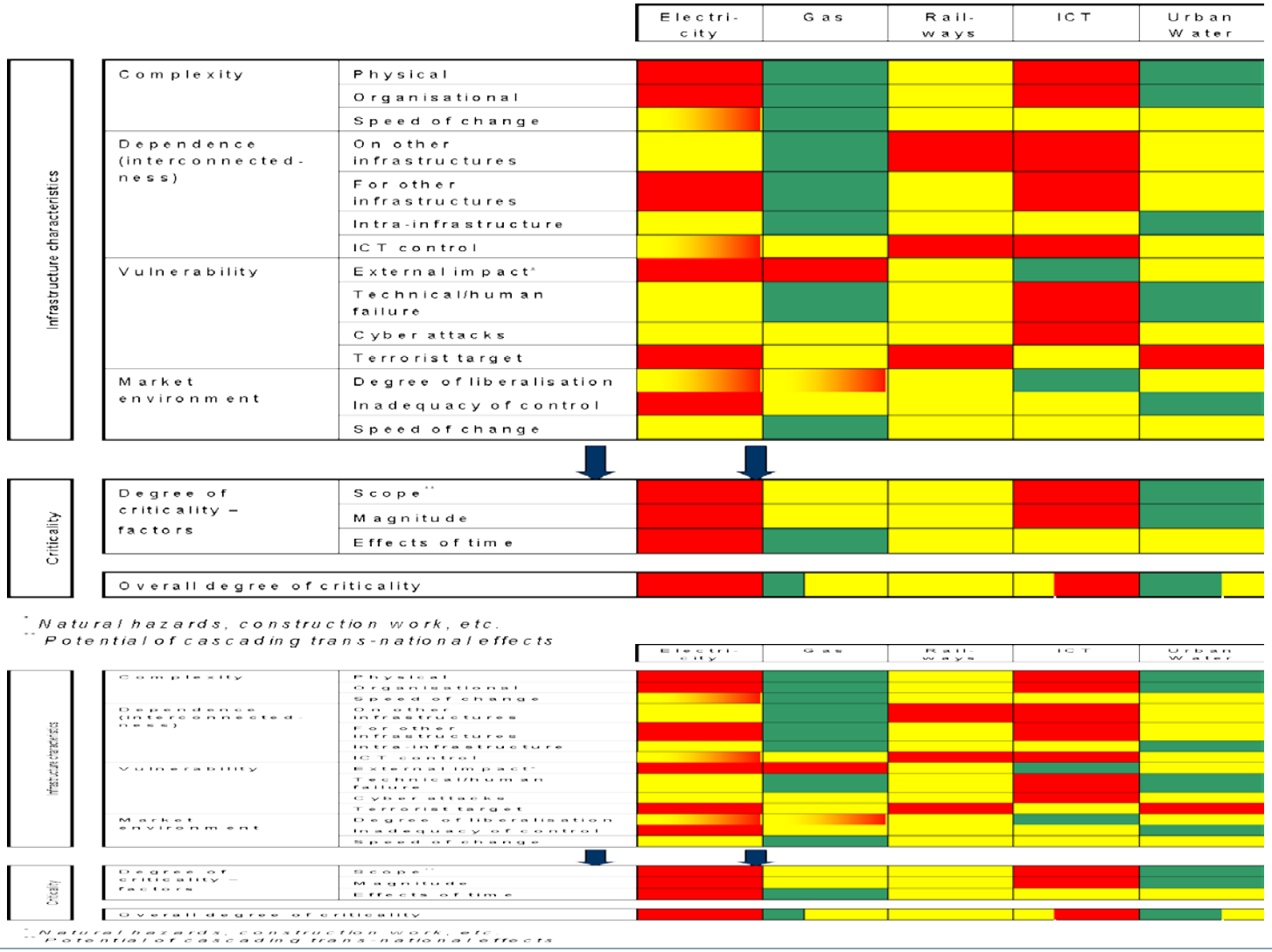
(2) Trading / Office Systeme of SCADA separated

(3) Substations have their own guidance systems and can, if needed, be operated by telephone lines; protection systems work independent of the SCADA

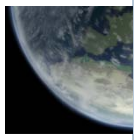
The applied systems are mostly redundant and also diversified.

Assessment Matrix for the Five Infrastructures Selected for this Study

Colours are used for our initial judgement: Red corresponds to high, green to low, yellow to in-between; transitions from one colour to another indicate changes/trends.



Some More Specific Policy Recommendations (I/II)

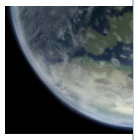


The Electric Power Supply System

In the EU internal market Directives and Regulations, national legal and regulatory authorities as well as provisions are still all market-focused. Reliability criteria are often traded-off against other factors in liberalised markets. Therefore:

- Security of continuous supply should be addressed more explicitly and become a new overarching principle. Strategies to ensure an appropriate level of protection and resilience need to be promoted
- ...

Some More Specific Policy Recommendations (II/II)



Communication and Information (Internet)

- Until research efforts, under way to develop much more secure Internets in the future, are successful, the public Internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure…

'Messages to take home'

- Preparedness is an essential part of a broader safety concept of preventive management strategy
- 'Deep understanding' and analytical tools as well as learning from the past form a basis for adequate preparedness
- ETH performs front-line research and educates people to do better
- Even in the best of circumstances, preventive and preparatory measures may fail and 'severe problems' may occur; this should also be communicated