ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Risk Analysis of Highly-integrated Systems

VA: Vulnerability and Resilience / Building Robust Systems

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Concept of vulnerability (Verletzbarkeit) – definition of terms (I)

- Disasters in the past revealed that “hazard-centric” perception / concepts are too limited as “a hazard of low intensity could have severe consequences, while a hazard of high intensity could have negligible consequences. The level of vulnerability was making the difference“ (White, 1974).
- Hazard = Gefahr (threat = Gefahr, Bedrohung): … a possible / potential source of danger….

Properties and characteristics of hazards

Hazard's characteristics	Description
Nature	Natural, socio-natural, technological, sociopolitical, man-made hazards
Magnitude	Only those occurrences that exceed some common level of magnitude are extreme
Location or geographical extent	Space covered by the hazardous event
Spatial dispersion	Pattern of distribution over the space in which its impact can occur
Speed of onset	Length of time between the first appearance of an event and its peak
Duration	Length of time over which a hazardous event persist, the onset to peak period
Frequency/Probability	The sequencing of events, ranging along a continuum from random to periodic. From the frequency the probability of return can be defined

Source: S. Bouchon, after Gravley, 2001

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

Concept of vulnerability – definition of terms (II)

No consensus definition of vulnerability to date

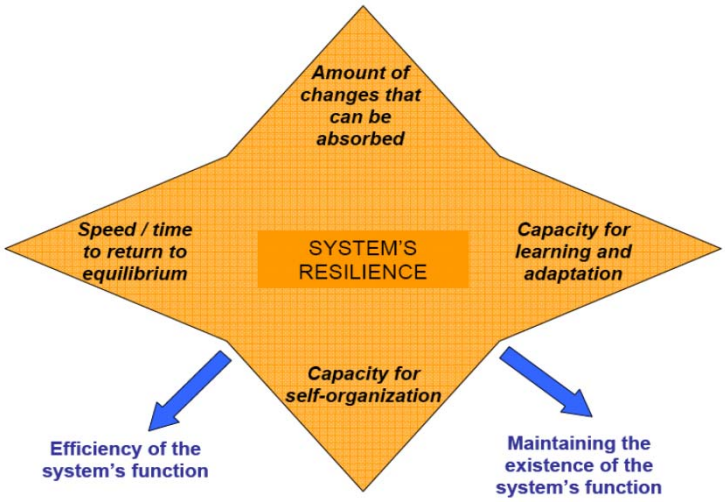
We define **vulnerability** as a flaw or weakness (inherent characteristics including resilience capacity) in the design, implementation, operation and/or management of an infrastructure system or ist element to a hazard or threat.

The concept of vulnerability develops in three main steps and finally focuses on three elements:

- Degree of loss and damages due to the impact of a hazard (technical dimensions),
- Degree of exposure to the hazard, i.e. likelihood of being exposed to hazards of a certain degree and the susceptibility of an element at risk to suffer loss and damages (element at risk could be a technical system),
- Degree of capacity of resilience, i.e. the ability of a system to anticipate, cope with/absorb, resist and recover the impact of a hazard (technical) or disaster (social)

Resilience: ability to recover from some shock or disturbance – the quality or state of being flexible.

Features of system's resilience



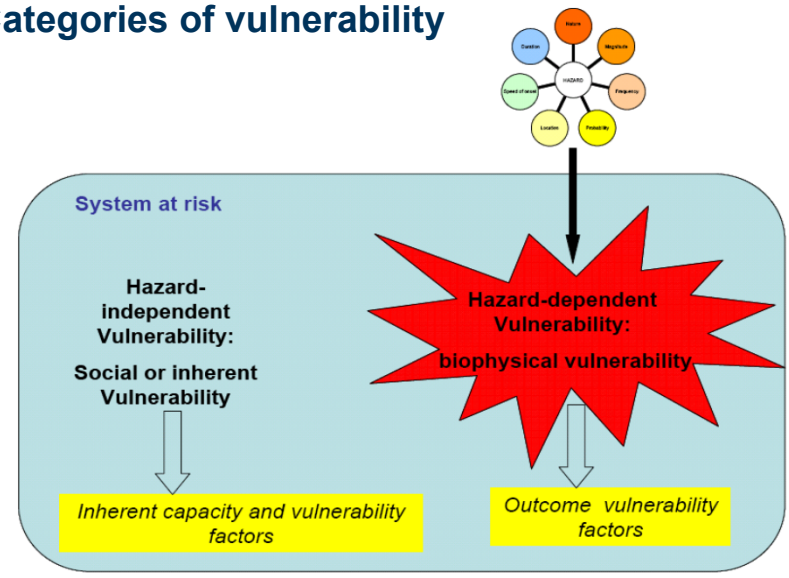
Source: S. Bouchon

Concept of vulnerability – definition of terms (III)

Distinction between two categories viewing vulnerability either

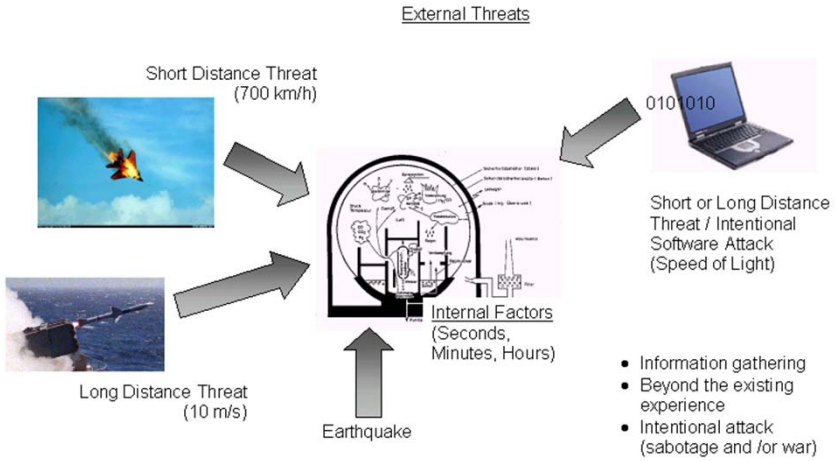
1. as the amount of (potential) damages caused to a system by a particular hazardous event (hazard dependent, biophysical vulnerability)
2. as a state that exists within a system before it encounters a particular hazardous event (hazard independent, inherent vulnerability)

Categories of vulnerability

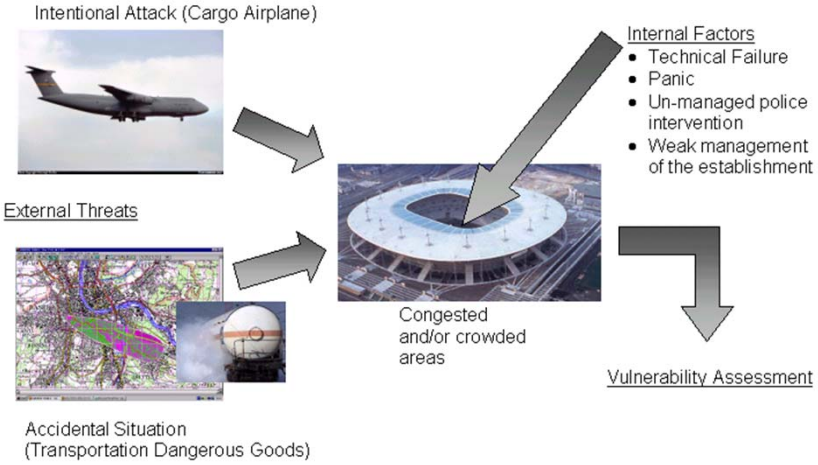


Source: S. Bouchon

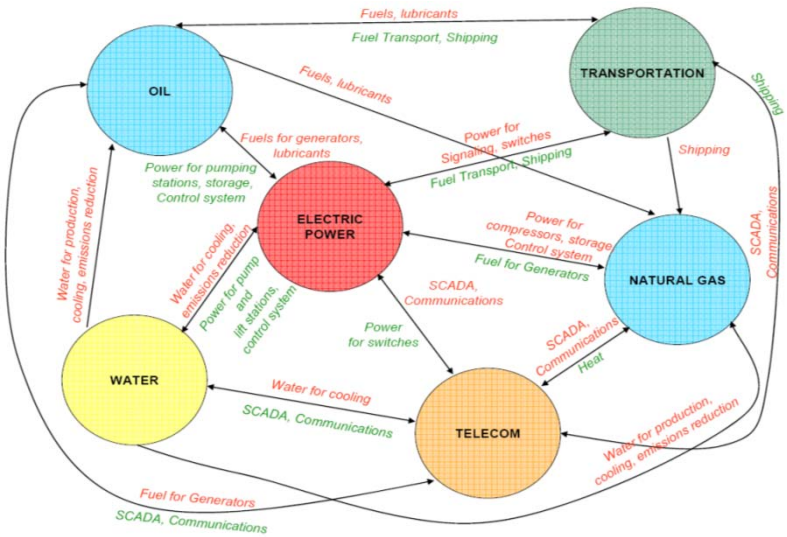
Vulnerability-Technical Example



Vulnerability-Societal Example

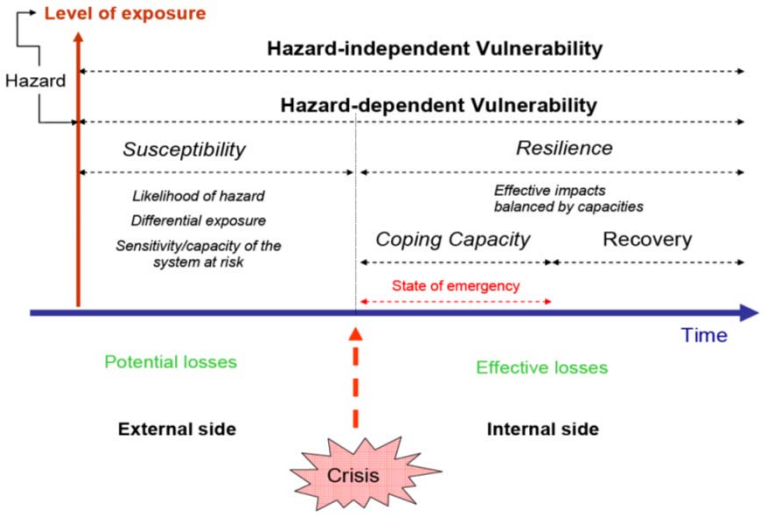


Critical infrastructures and their interdependencies



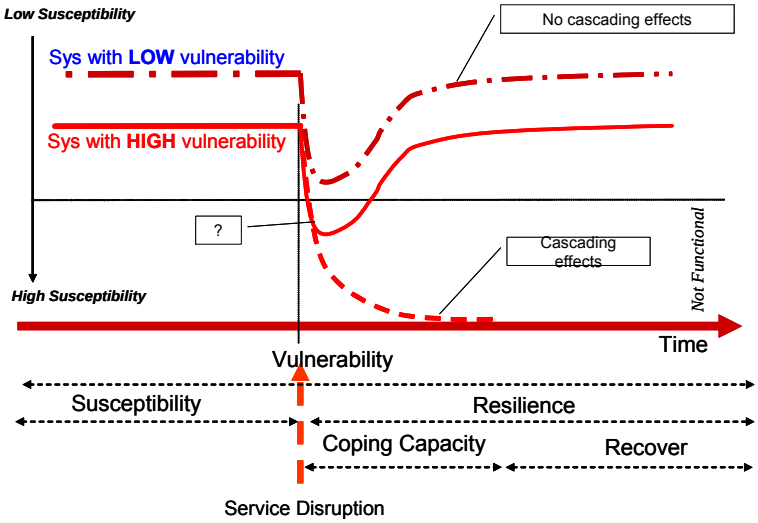
Source: Rinaldi, Peerenboom, Kelly, 2001

Vulnerability model



Source: S. Bouchon

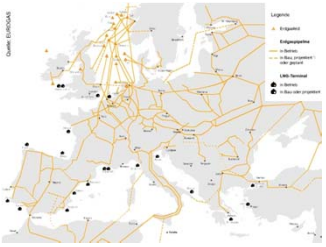
Vulnerability scenarios



Vulnerability Assessment of Networks
Examples of technical networks

Swiss Power System

Natural Gas Pipelines



- Internet
- World Wide Web
- Railway
- Motorway
- …

Multicomponents System's Vulnerability – Representation by U, V, t, modeling approach

System

- consists of large number, M, of elemental constituents, or members

System members

- interact with each other with a varying intensity; interaction described by a coupling constant, or intrinsic parameter U, and an exterior factor, or extrinsic parameter V.
- may assume two distinct states, 1 and 2, normal vs. abnormal, up vs. down, etc., at given time, t

Overall state of the system

- described via a pair of numbers (M_1, M_2), system dynamics, or motion in its space will follow from variations in M_1 and M_2.

Multicomponents System's Vulnerability (I)

Smallest transitions in the system's state involve alterations by one unit in the numbers of members:

$$(M_1 - 1, M_2 + 1) \underset{w_{21} \rightarrow}{\overset{\leftarrow w_{12}}{\rightleftarrows}} (M_1, M_2) \underset{\leftarrow w_{12}}{\overset{w_{21} \rightarrow}{\rightleftarrows}} (M_1 + 1, M_2 - 1) \quad (1)$$

while w_{12} and w_{21} are governing probabilities.

Admission of the process leads also to the recognition of a function of distribution of the system's states:

$$\partial f(M_1, M_2, t)/\partial t = w_{21}(M_1 - 1, M_2 + 1) \cdot f(M_1 - 1, M_2 + 1) + \\ + w_{12}(M_1 + 1, M_2 - 1) \cdot f(M_1 + 1, M_2 - 1) - \\ - (w_{21}(M_1, M_2) + w_{12}(M_1, M_2)) \cdot f(M_1, M_2) \quad (2)$$

Multicomponents System's Vulnerability (II)

The state (M1, M2) of the system can alternatively be described by the membership fraction

$$\zeta = (M_1 - M_2) / (2M), \quad (3)$$

if all system members are in state 1, then $\zeta = ½$, whereas if all members are in state 2, then $\zeta = -½$.

Equation (2) may be re-written as:

$$\partial f(\zeta)/\partial t = w_{21}(\zeta - 1/M) f(\zeta - 1/M) + w_{21}(\zeta + 1/M) f(\zeta + 1/M) - \\ - (w_{21}(\zeta) + w_{12}(\zeta)) f(\zeta) \quad (4)$$

Multicomponents System's Vulnerability (III)

Transition probabilities w_{12} and w_{21} need to assumed, e.g. if transitions are a co-operative phenomenon

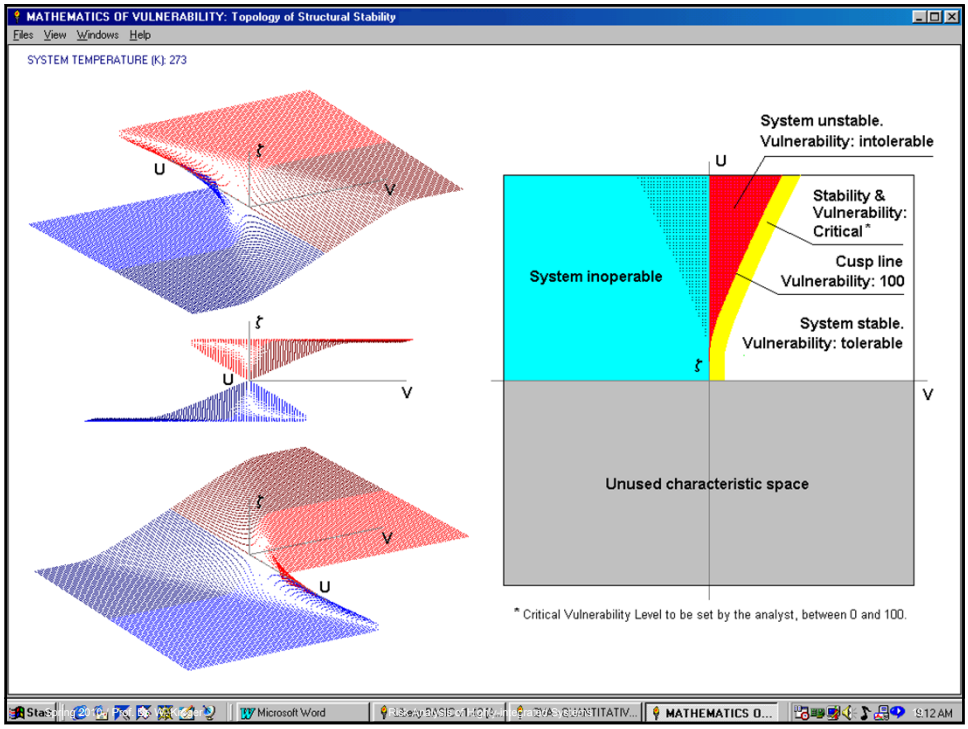
$$w_{12}(\zeta) = w\, M_1\, exp(-U\cdot\zeta + V) / \theta)$$
$$w_{21}(\zeta) = w\cdot M_2 \cdot exp(U\cdot\zeta + V) / \theta) \quad (5)$$

θ generalised 'temperature' of the system

Real solutions ζ

Depending on the degree of interaction between system constituents (members), reflected in the coupling constant U, and on the external influence on all system members - reflected in the field V, and also taking into consideration the temperature θ of the system, the equation may display the following number of real solutions ζ that may relate to the overall system condition:

Number of Real Solutions	System Condition
1	Stable. Smooth transitions in population membership, between state 1 and state. **Low and/or acceptable vulnerability.**
3, of which 2 identical	Critical. Sharp transitions in membership between states 1 and 2 are possible. Either state 1 or state 2 may suddenly become improbable. **System is critically vulnerable.**
3, all different from each other	Unstable. Sharp transitions in membership between states 1 and 2 are possible. Frequency of occurrence of states 1 and 2 are comparable. **System is dangerously/ un-acceptably vulnerable.**



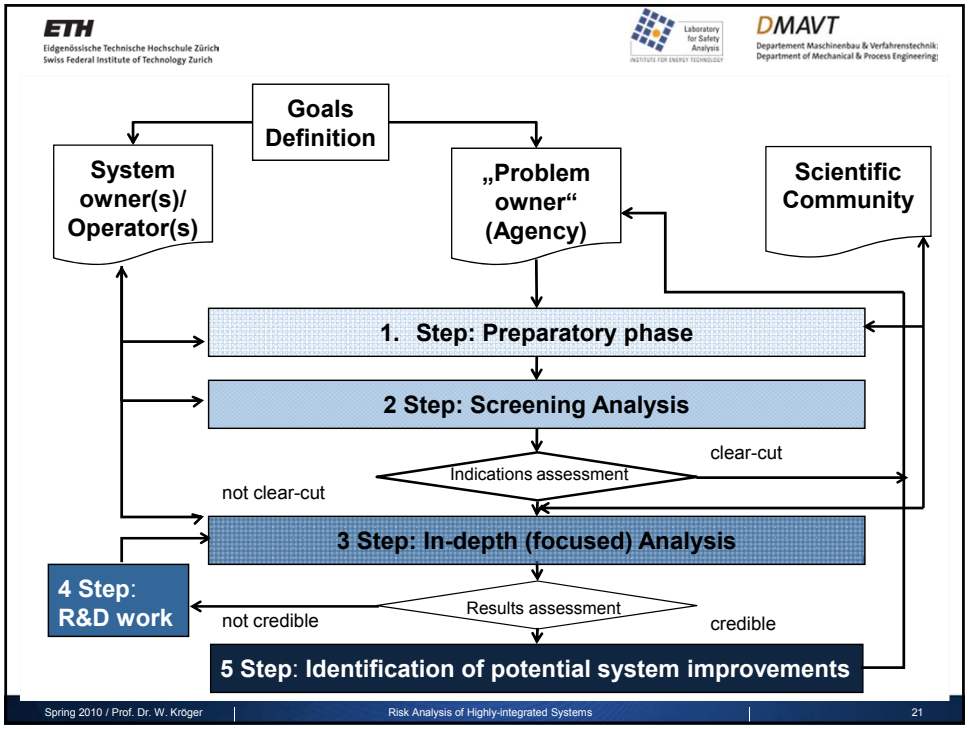
ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

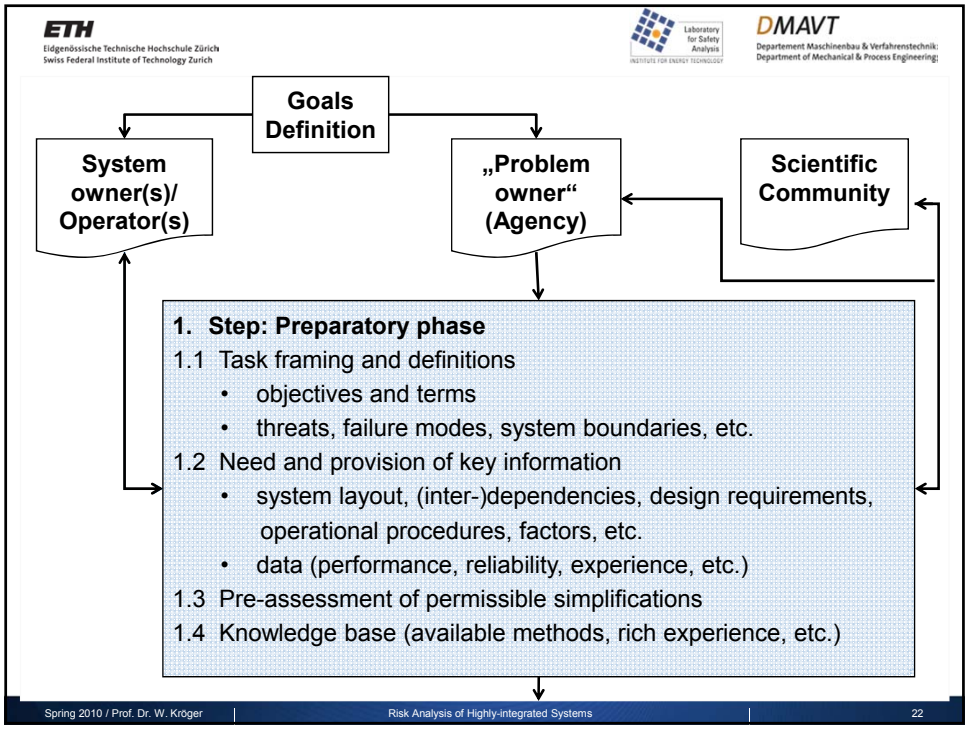
Laboratory for Safety Analysis

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

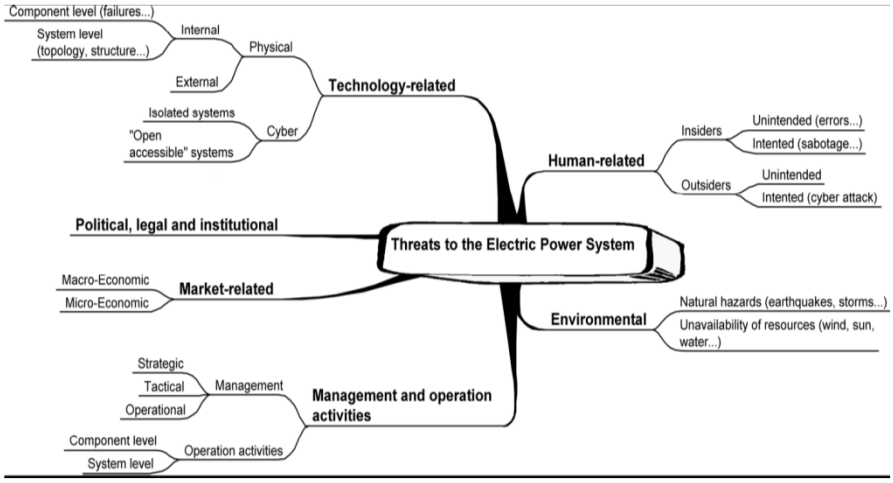
Motivation

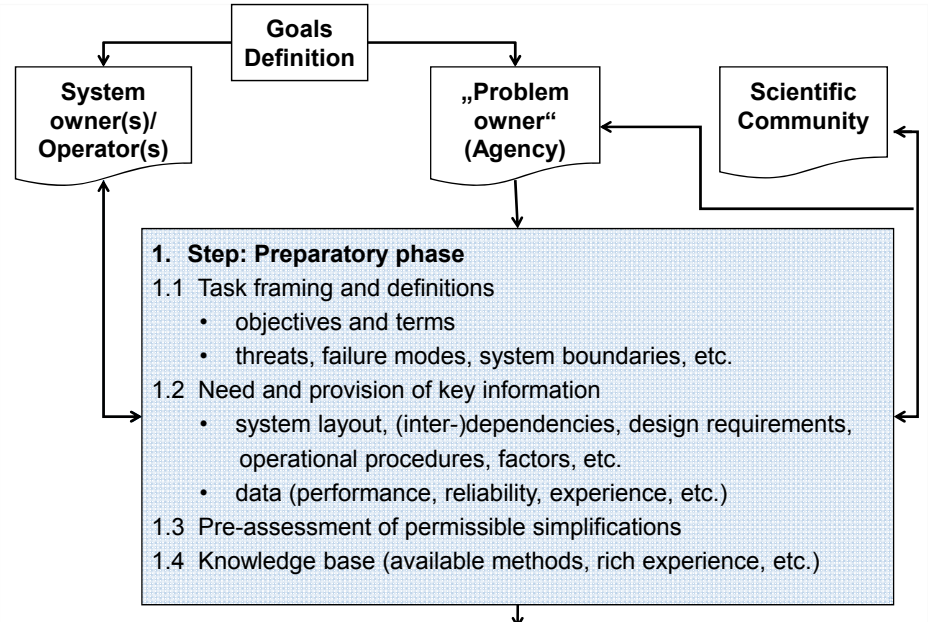
- Requirements: Vulnerability analysis of interconnected infrastructures calls for 'system-of-systems thinking', suitable techniques and problem-oriented approach.
- Available: Many models for analyzing individual critical infrastructures
- Missing: Comprehensive framework for modeling and simulation of interdependencies

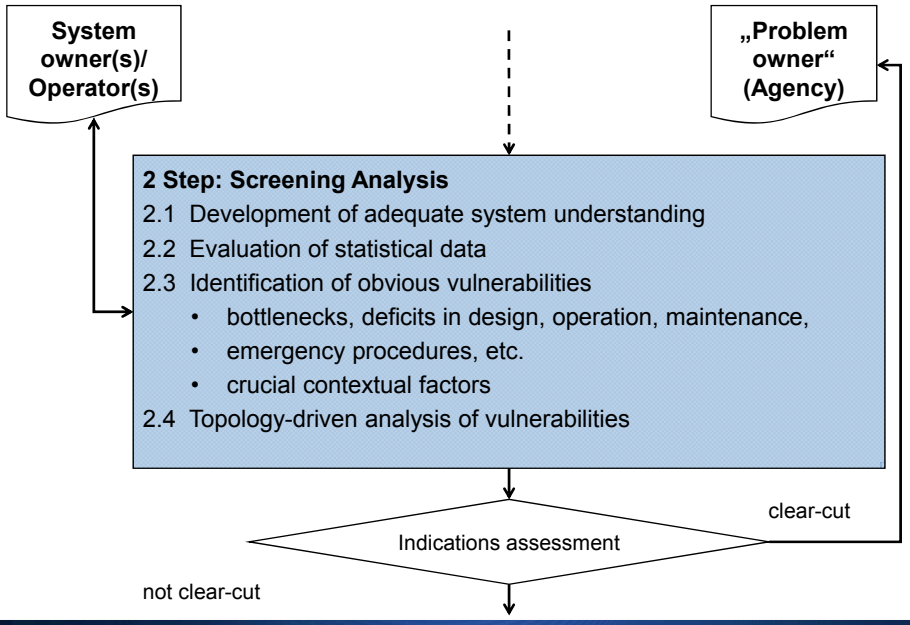

Goals Definition
System owner(s)/ Operator(s)
„Problem owner“ (Agency)
Scientific Community
1. Step: Preparatory phase
2 Step: Screening Analysis
Indications assessment
clear-cut
not clear-cut
3 Step: In-depth (focused) Analysis
4 Step: R&D work
Results assessment
not credible
credible
5 Step: Identification of potential system improvements
Spring 2010 / Prof. Dr. W. Kröger
Risk Analysis of Highly-integrated Systems
21


Goals Definition
System owner(s)/ Operator(s)
„Problem owner“ (Agency)
Scientific Community
1. Step: Preparatory phase
1.1 Task framing and definitions
• objectives and terms
• threats, failure modes, system boundaries, etc.
1.2 Need and provision of key information
• system layout, (inter-)dependencies, design requirements, operational procedures, factors, etc.
• data (performance, reliability, experience, etc.)
1.3 Pre-assessment of permissible simplifications
1.4 Knowledge base (available methods, rich experience, etc.)
Spring 2010 / Prof. Dr. W. Kröger
Risk Analysis of Highly-integrated Systems
22

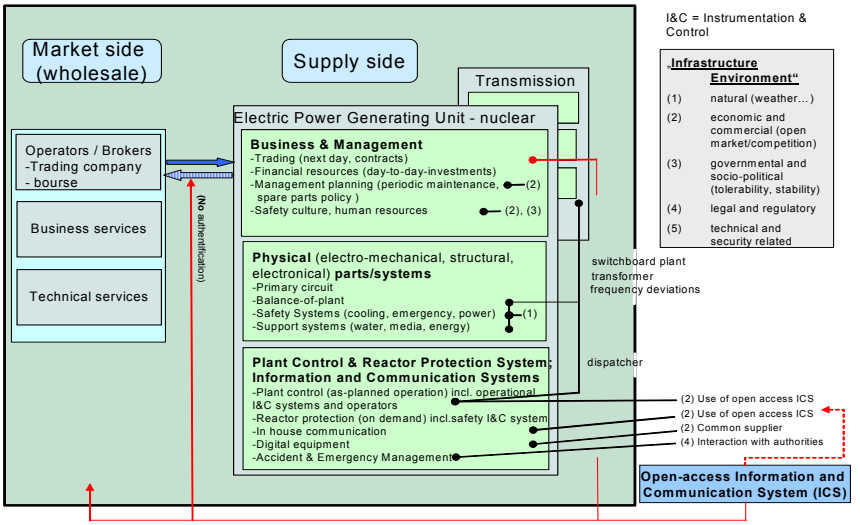
Threats to Electric Power Supply Infrastructure

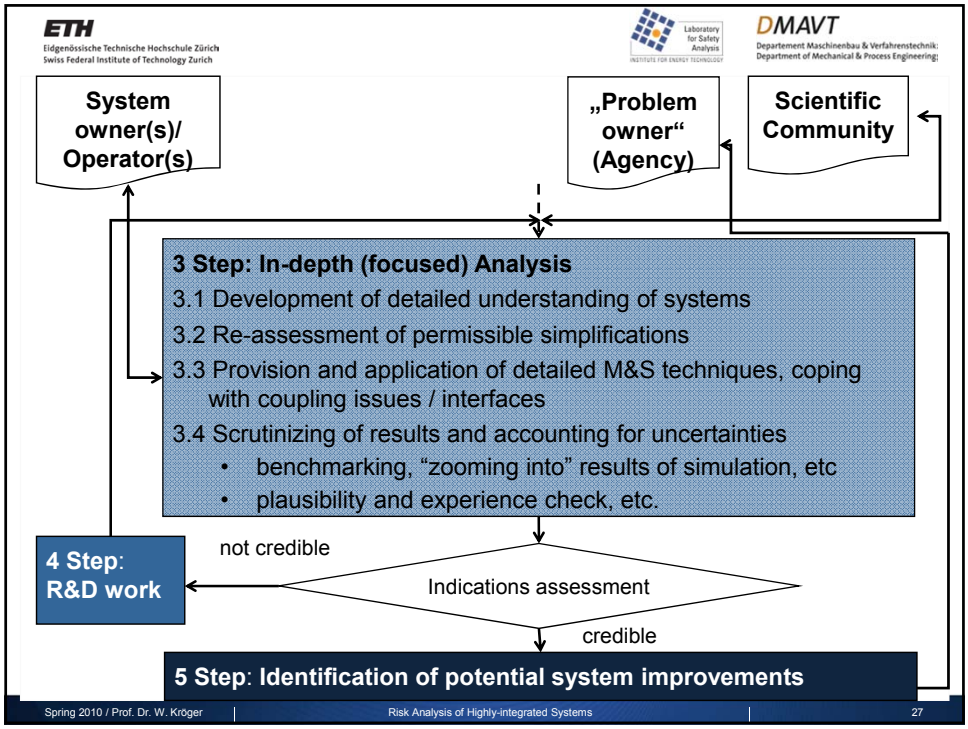


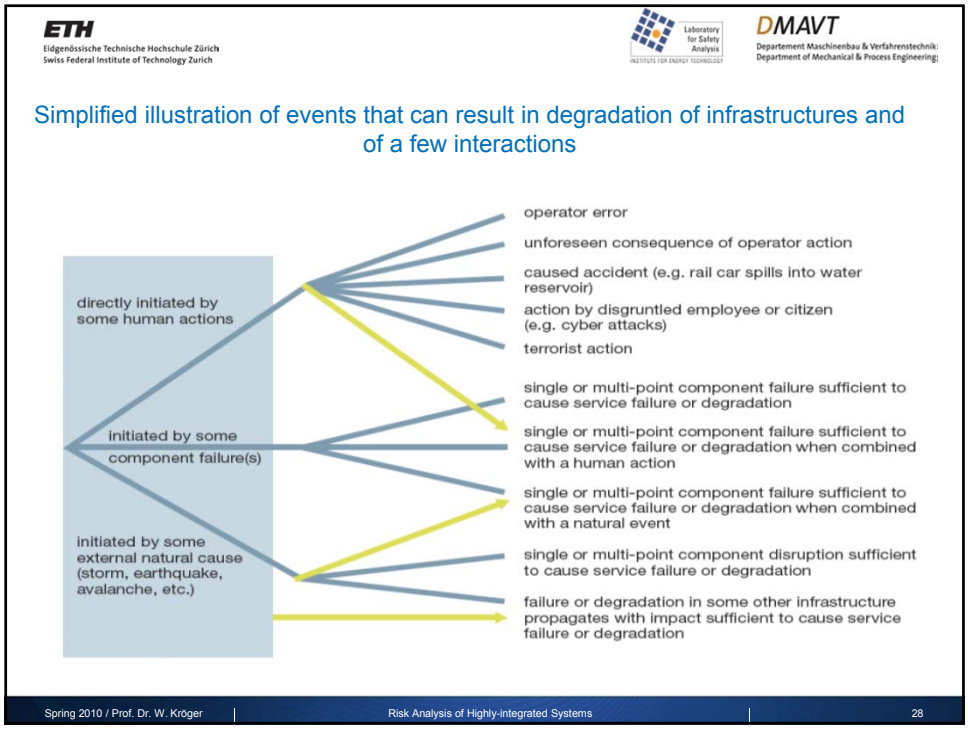


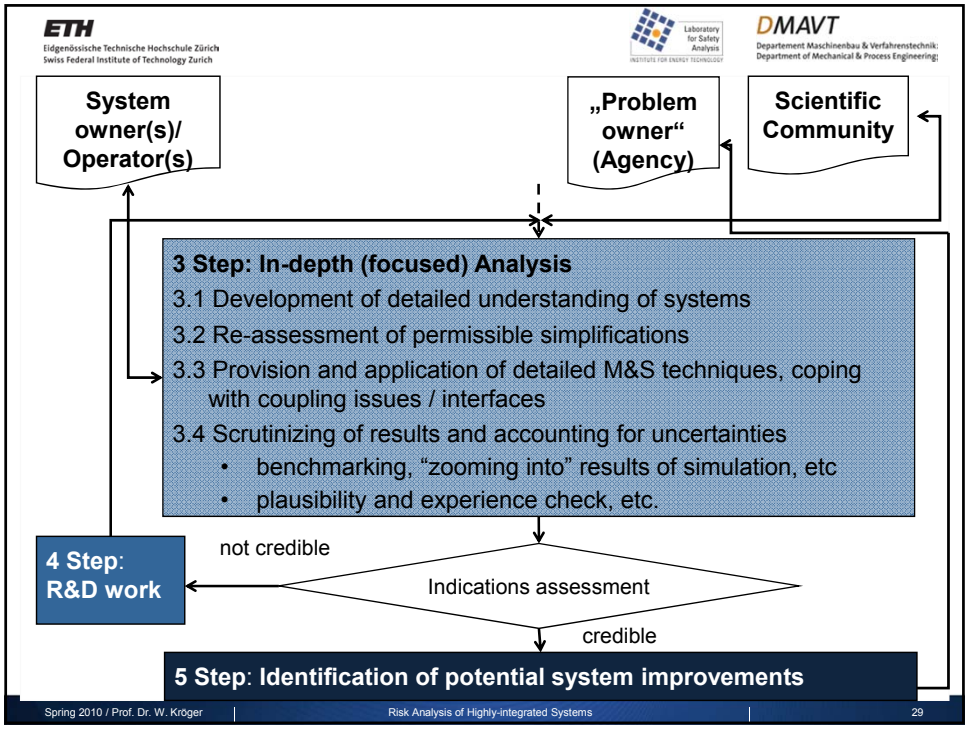


Electric Power Supply Infrastructure and its environment, detailed for a nuclear power generating unit interacting with ICS




ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis
DMAVT
Departement Maschinenbau & Verfahrenstechnik:
Department of Mechanical & Process Engineering
System owner(s)/ Operator(s)
„Problem owner“ (Agency)
Scientific Community
3 Step: In-depth (focused) Analysis
3.1 Development of detailed understanding of systems
3.2 Re-assessment of permissible simplifications
3.3 Provision and application of detailed M&S techniques, coping with coupling issues / interfaces
3.4 Scrutinizing of results and accounting for uncertainties
• benchmarking, “zooming into” results of simulation, etc
• plausibility and experience check, etc.
not credible
4 Step: R&D work
Indications assessment
credible
5 Step: Identification of potential system improvements
Spring 2010 / Prof. Dr. W. Kröger
Risk Analysis of Highly-integrated Systems
27


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis
DMAVT
Departement Maschinenbau & Verfahrenstechnik:
Department of Mechanical & Process Engineering
Simplified illustration of events that can result in degradation of infrastructures and of a few interactions
directly initiated by some human actions
initiated by some component failure(s)
initiated by some external natural cause (storm, earthquake, avalanche, etc.)
operator error
unforeseen consequence of operator action
caused accident (e.g. rail car spills into water reservoir)
action by disgruntled employee or citizen (e.g. cyber attacks)
terrorist action
single or multi-point component failure sufficient to cause service failure or degradation
single or multi-point component failure sufficient to cause service failure or degradation when combined with a human action
single or multi-point component failure sufficient to cause service failure or degradation when combined with a natural event
single or multi-point component disruption sufficient to cause service failure or degradation
failure or degradation in some other infrastructure propagates with impact sufficient to cause service failure or degradation
Spring 2010 / Prof. Dr. W. Kröger
Risk Analysis of Highly-integrated Systems
28



Robust and Resilient Energy Infrastructures

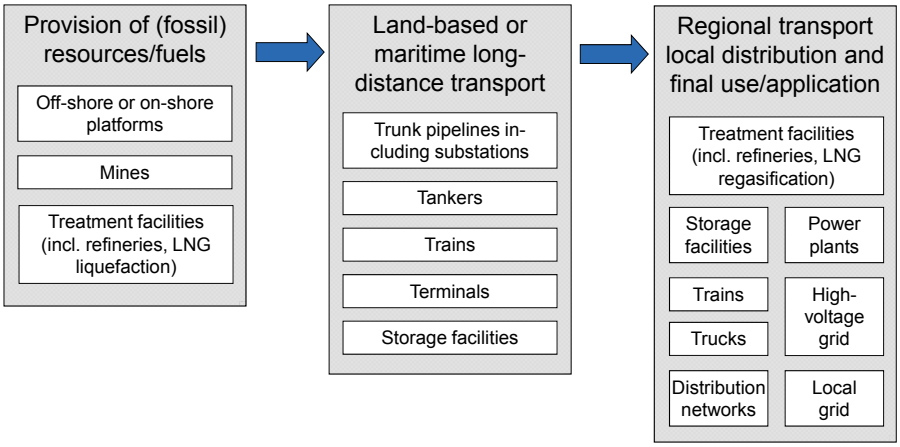
Aim: Being capable of coping with “variations” with minimal damage and/or absorbing “impact” and getting back to initial conditions

⇨ Avoid severe accidents and/or disruption of service in case of damaging events, guarantee short recovery times

⇨ Ensure continuation of service, if main system fails

Scope: Entire supply chain from production via transport to consumption; multifaceted set of technical and human failures, natural hazards and various threats including malicious attacks and criminal acts

Energy Supply Chain from Producing Areas to Consuming Countries



Relevance of technical fixes to reduce vulnerabilities against terrorist and cyber attacks

most sensitive areas	avoid, reduce	redun-dancy	reserves	robust topology	extended respond times	'island solutions' (cyber)	physical protection	spatial se-paration	other
choke points (tankers)	n.r.	-	(X)	-	-	-	-	-	political / military
wide-area gas & oil pipelines	n.r.	X	X	X	-	n.r.	n.r.	X	
large storage & treatment facilities	X (remote siting)	-	X	-	-	-	n.r.	n.r.	
hydro dams	n.r.	-	-	-	-	-	X (?)	-	military (?)
NPPs	n.r.	X*	-	-	X	X	X	X*	
distribution networks (UCTE)	-	X	X	X	X	X	n.r.	X	
n.r. not realistically		* at systems' level							

Avoid obvious vulnerabilities: Oil transport through critical choke-points