Interdependencies among technical systems: The why, what and how

Wolfgang Kröger, Sven Dietz, ETH Switzerland

Characteristics and peculiarities of large-scale technical systems, in particular critical infrastructures (1/2)

- A network of large-scale human-made systems that function synergistically to produce a continuous flow of essential services
- Designed to satisfy specific social needs but shape social change at much broader and complex level (recall Internet)
- Highly complex, inter-dependent, both physically and through a host of industrial ICT; subject to rapid changes
- Face multiple threats (technical-human, natural, physical, cyber, contextual; unintended or malicious)

Characteristics and peculiarities ... (2/2)

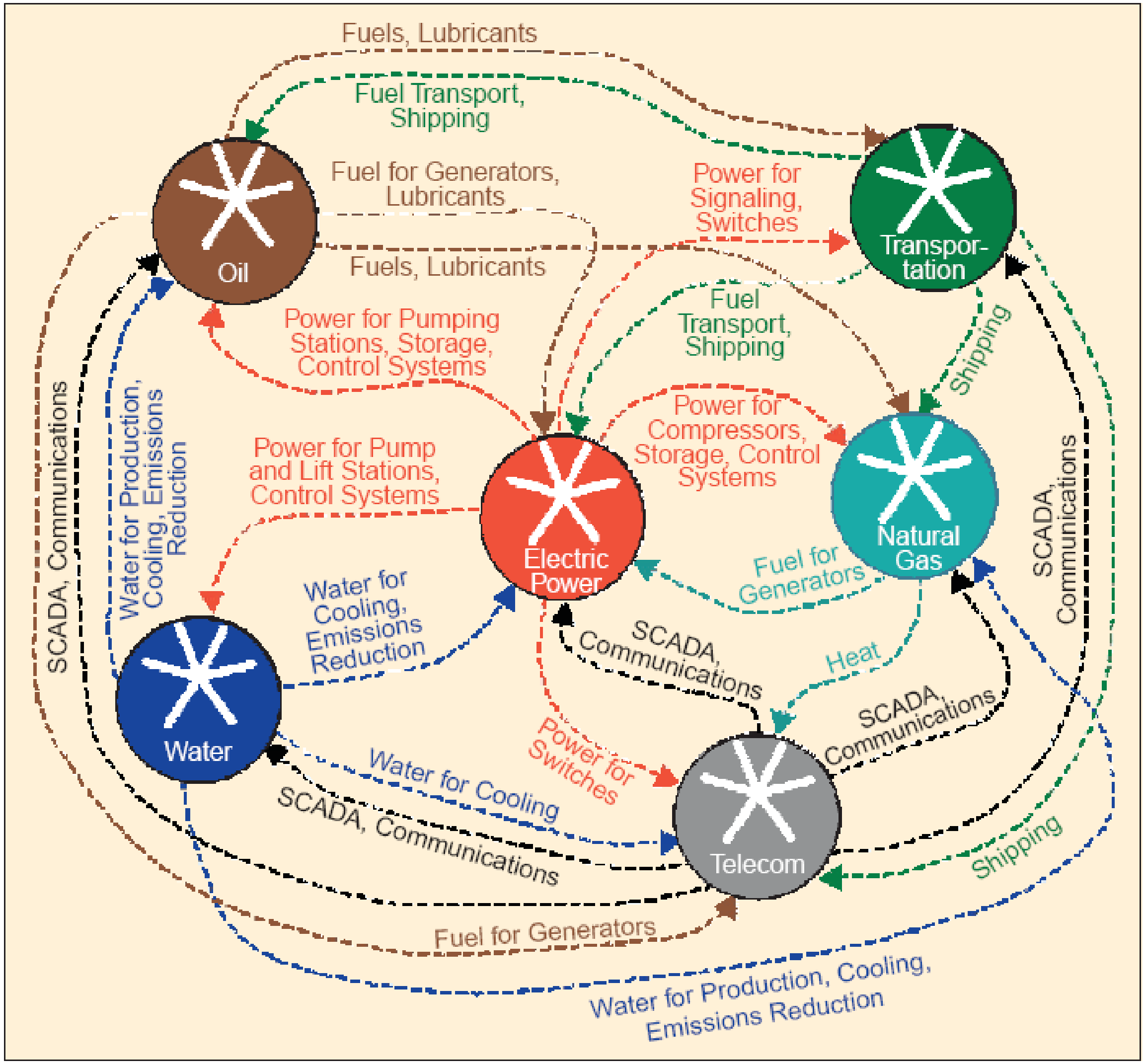
- May pose risks themselves
- Disruptions may cascade (recall “blackouts”)
- No single owner / operator / regulator; base on different logics

- Infrastructures are considered critical when “their incapacitation or destruction would have a debilitating impact on defence or economic security“ (US PCCIP, 97) of any state

Set of multiple threats disclosing vulnerabilities

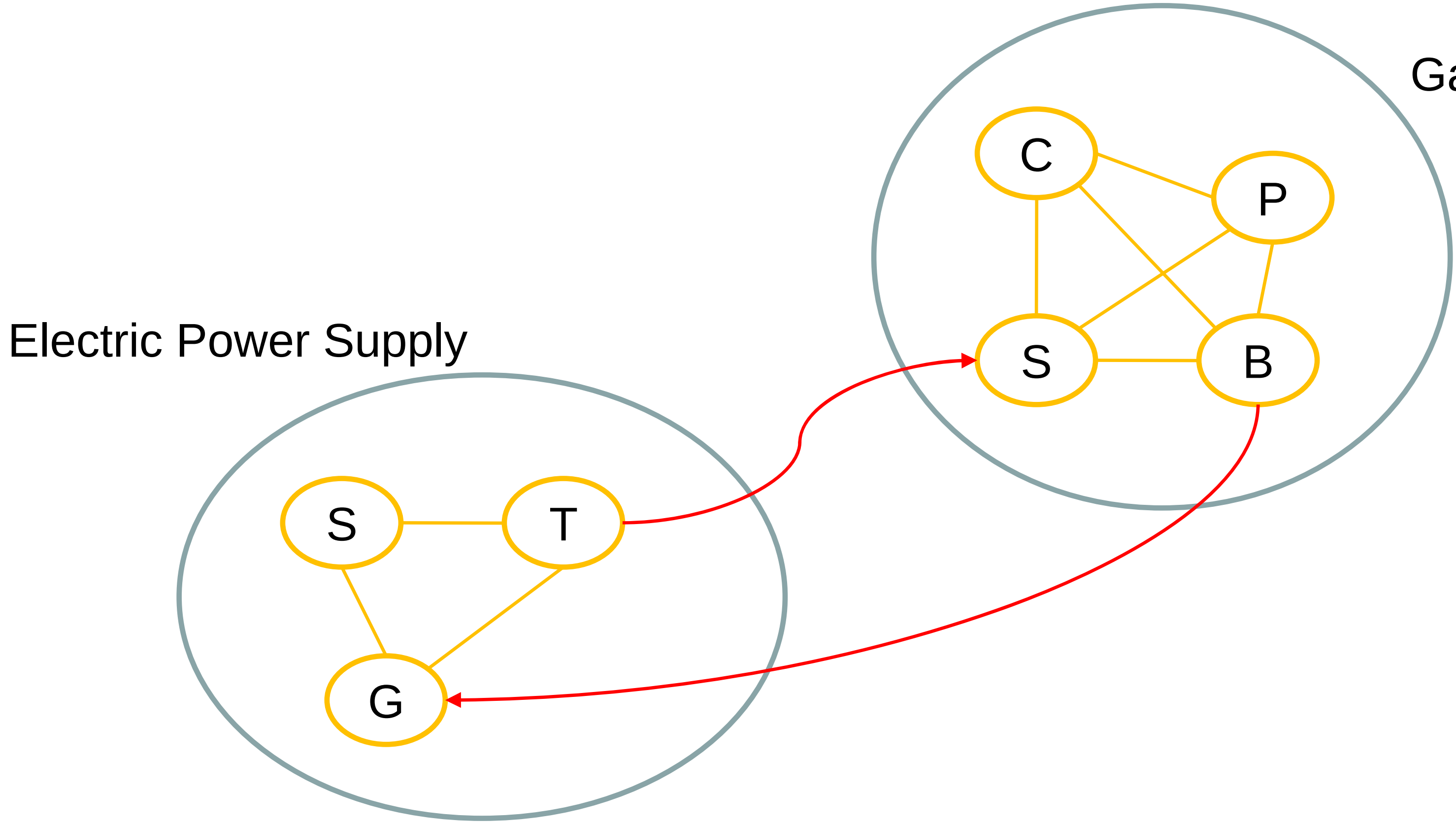
- **Natural events** such as earthquakes, hurricanes, tornados, severe flooding, or other (increasing) extreme weather conditions
- **Accidents or technical factors** leading to the debilitation of plants, networks and operations
- **Market factors** such as instability associated with major producer groups, or economic pressure trading-off security factors
- **Policy factors** such as artificial supply limitations or negative pricing outcomes or misusing “energy” for political purposes
- **Human factors** such as unintended failures, physical or cyber-attacks
- **Mutual dependencies** need to be recognized

Adressing interdependencies in and among infrastructures



Source: Rinaldi 2001

Closer look at interdependencies among infrastructures



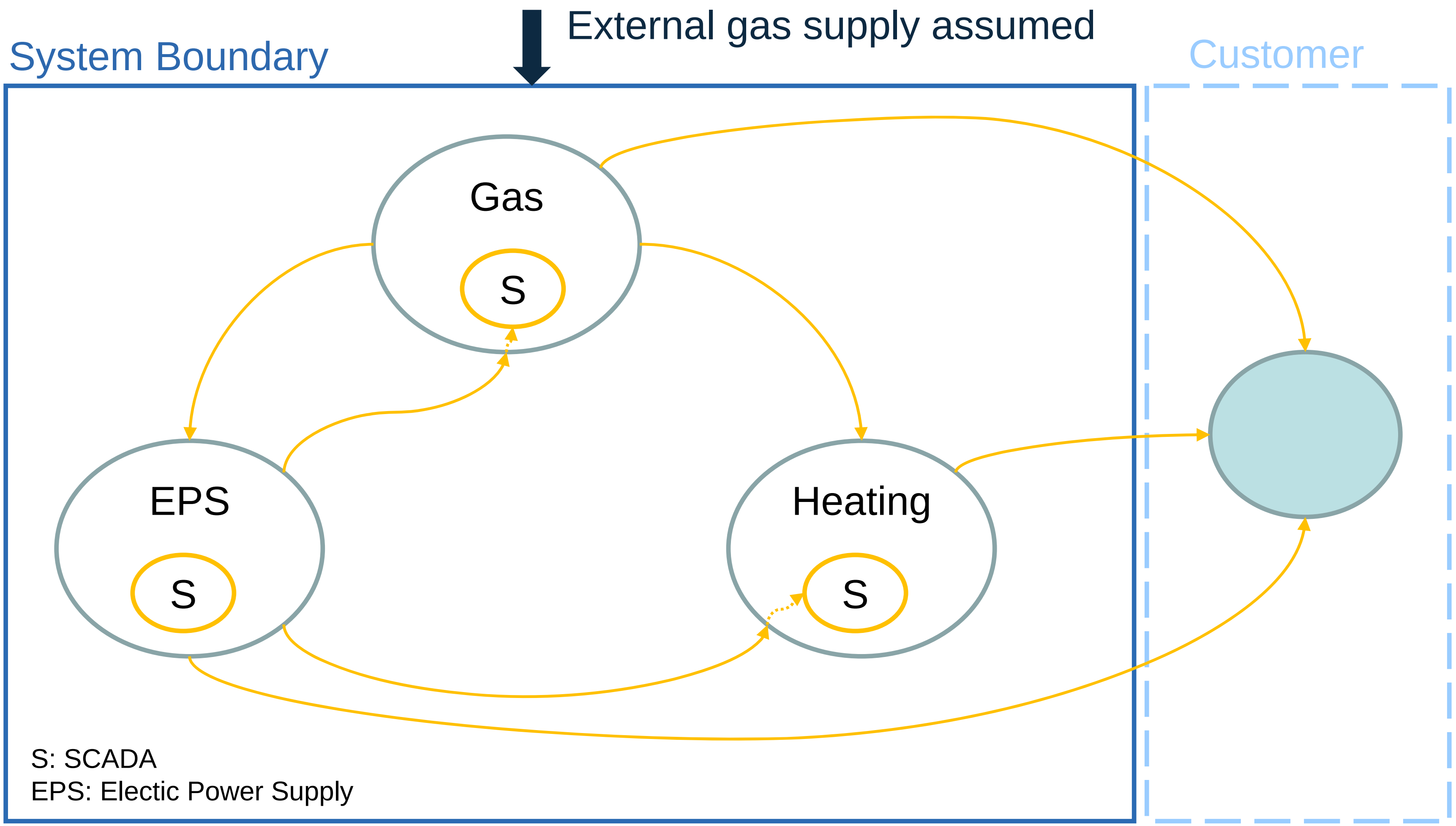
P: Pipelines
B: Buffer
C: Compressors
S: SCADA

T: Transmission Lines
G: Generators
S: SCADA

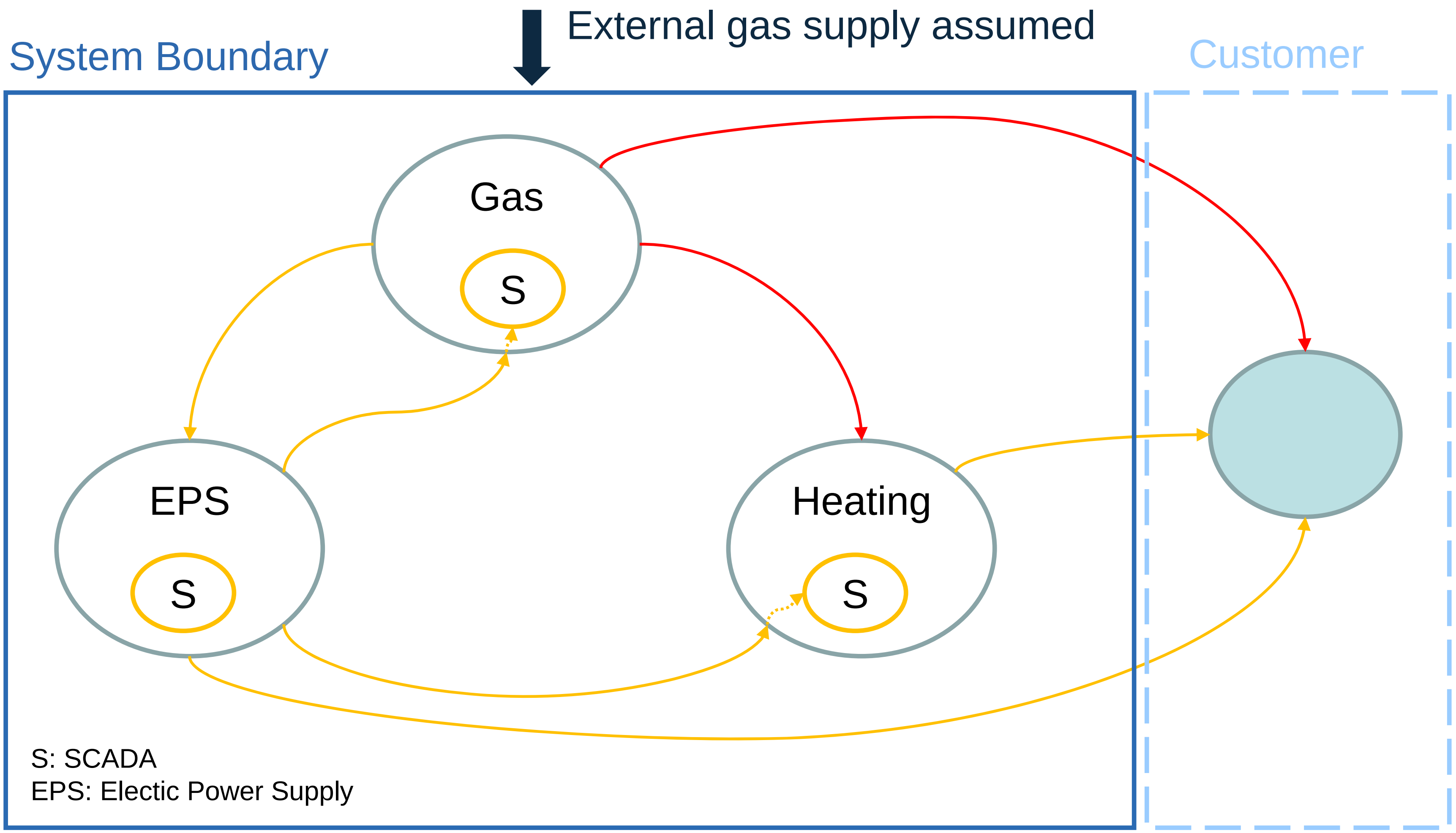
Issue framing: Continental gas supply

Issue framing: Regional gas supply ...

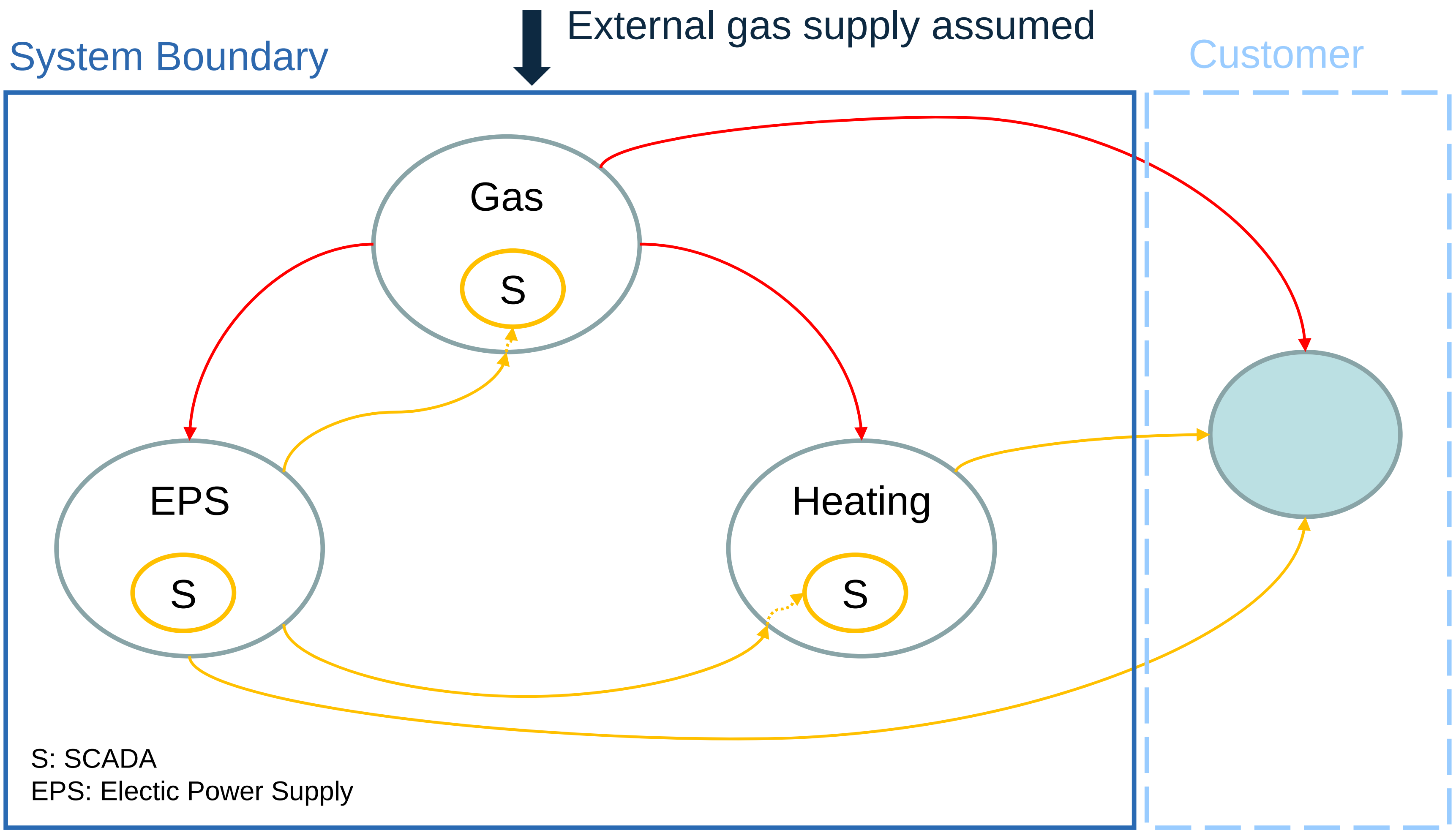
Issue framing: ... interdependencies among infrastructures



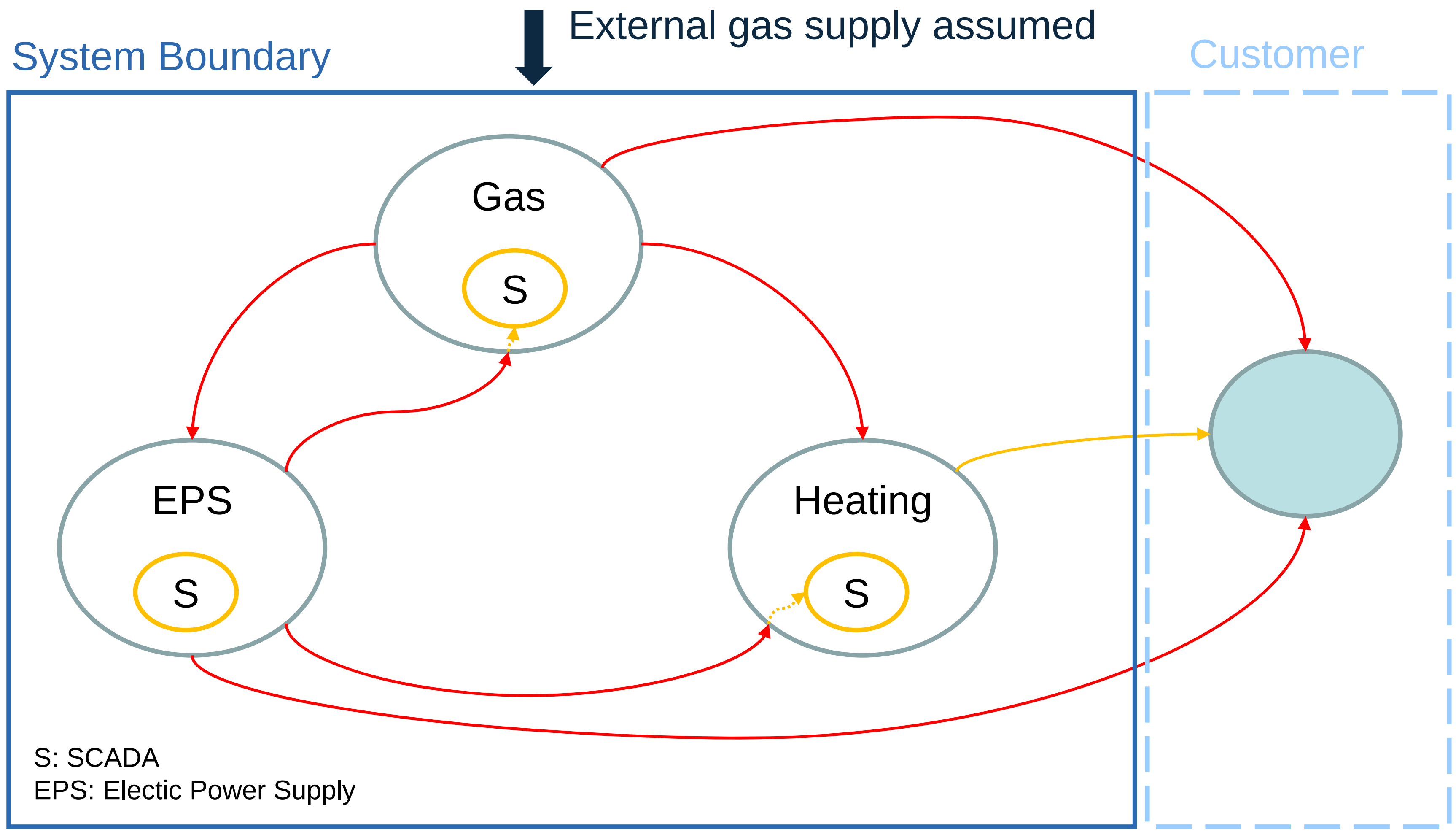
Failure propagation: immediate effects



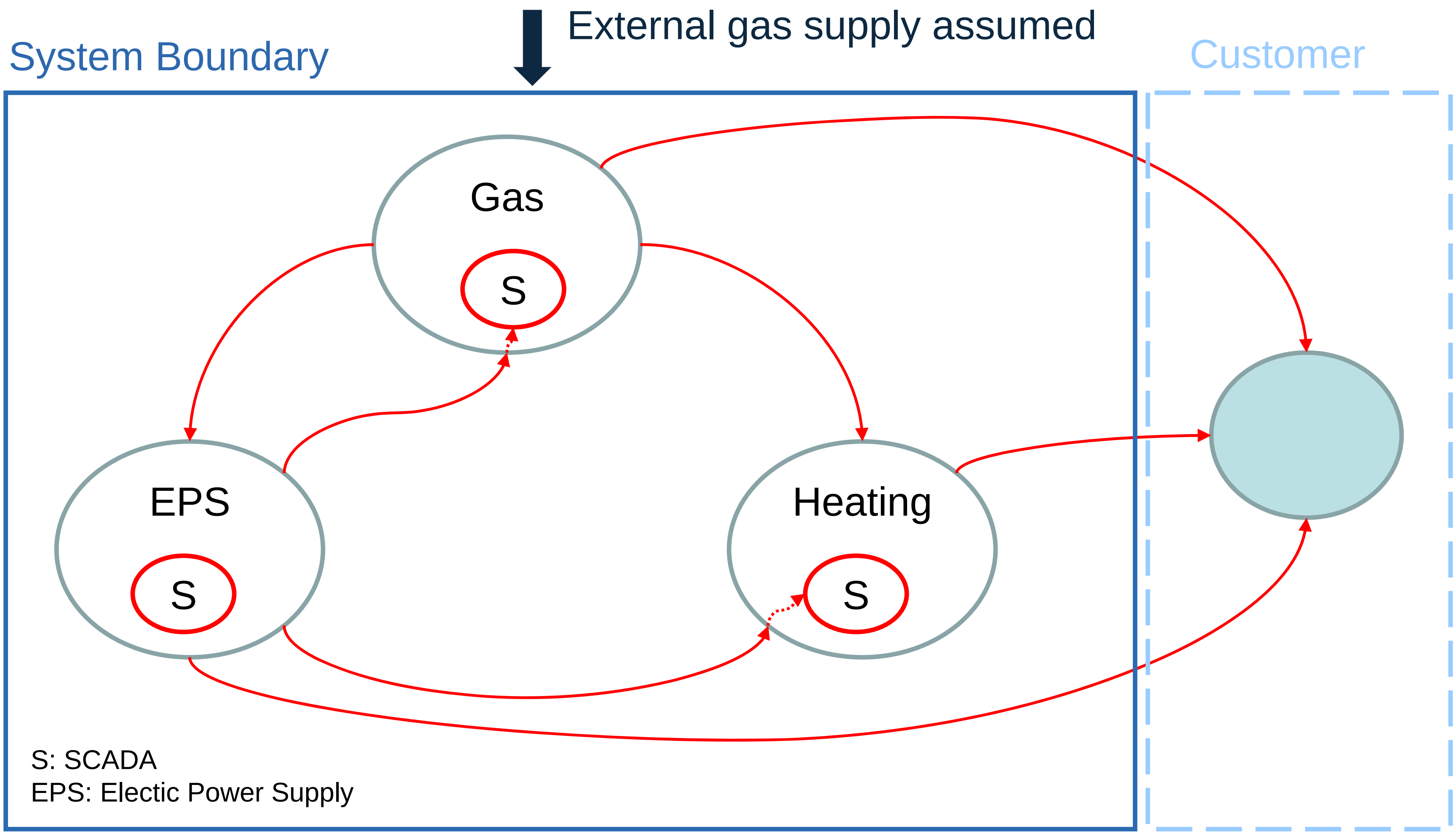
Failure propagation: delayed effects



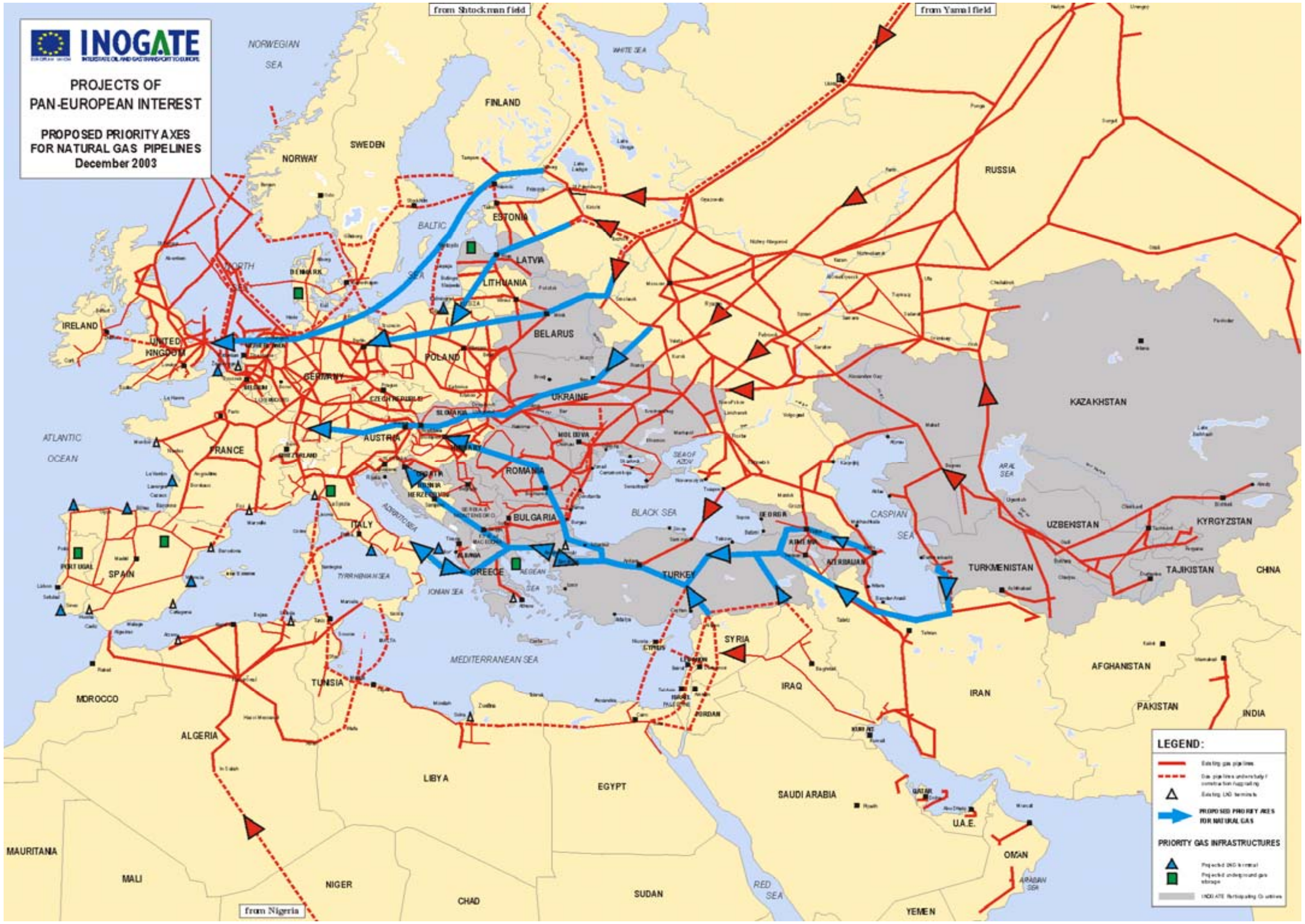
Failure propagation: delayed and 2nd order effects



Failure propagation: delayed and higher order effects



System boundary expansion to Eastern Europe and Asia



Stressed importance of wide-area and geopolitical hazards including 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 kilotons – Hiroshima 14-20 kilotons

Characteristics of interdependencies

Types of interdependencies:

- Input
- Mutual
- Co-located
- Shared
- Exclusive

Interaction levels:

- Physical
- Cyber
- Geographic
- Logical

Coupling:

- Coupling order
- Relative degree of coupling (Tightness of linkage)

Evidenced importance: Telco mini blackout (1/3)

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

- At 5.30 a.m. breakage of a pipe, carrying cooling water of the air-conditioning plant, 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
- Breakage of tube had to be repaired and plant radiators filled before restoring own services

Source IRRIIS

Telco mini blackout (2/3)

- Several boards/devices failed for short circuit
- Main power supply went out of service
- Emergency power supply was constituted by diesel generators and UPS system linked to banks of batteries
- 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

Telco mini blackout (3/3)

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 substations managed by the unmanned (Flaminia) Control Centre

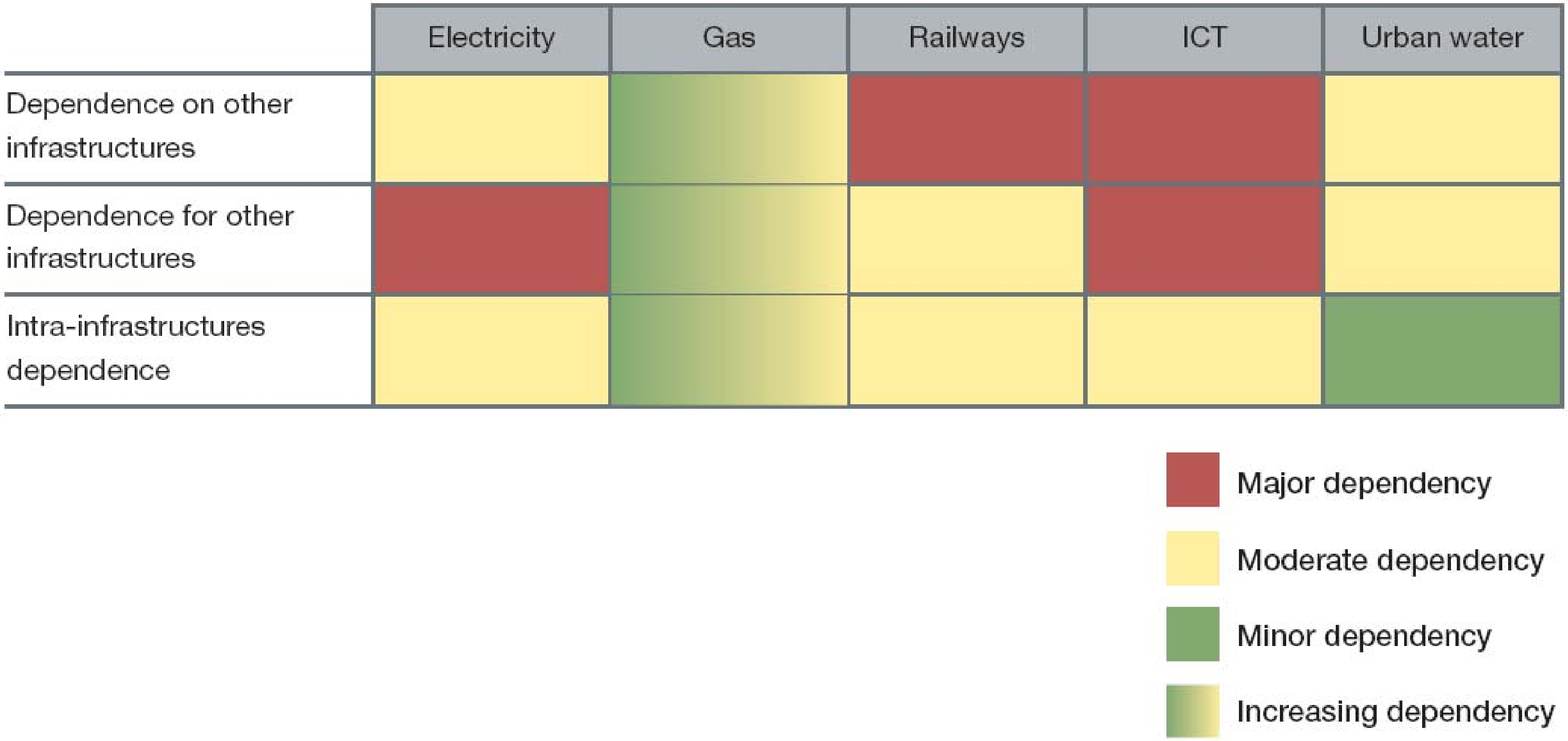
No control actions required to its RTU, within the duration of the blackout

Assesment matrix for five coupled infrastructures
(red: high, green: low, yellow: medium)

Infrastructure characteristics			Electricity	Gas	Railways	ICT	Urban Water
	Complexity	Physical	red	green	yellow	red	green
		Organisational	red	green	yellow	red	green
		Speed of change	yellow–red	green	yellow	yellow	yellow
	Dependence (interconnected-ness)	On other infrastructures	yellow	green	red	red	yellow
		For other infrastructures	red	green	yellow	red	yellow
		Intra-infrastructure	yellow	green	yellow	yellow	green
		ICT control	yellow–red	yellow	red	red	yellow
	Vulnerability	External impact*	red	red	yellow	green	yellow
		Technical/human failure	yellow	green	yellow	red	green
		Cyber attacks	yellow	yellow	yellow	red	yellow
		Terrorist target	red	yellow	red	yellow	red
	Market environment	Degree of liberalisation	yellow–red	yellow–red	yellow	green	yellow
		Adequacy of control	red	yellow	yellow	yellow	green
		Speed of change	yellow	green	yellow	yellow	yellow

Source: IRGC White Paper 3 2006

Dependencies of selected critical infrastructures



Source: IRGC Policy brief 2007

Requirements to methods dealing with interdependencies

Ablility to capture

- high complexity and interconnectedness of modern, open „system of systems“;
- all kind of human factors and the full spectrum of threats including malicious behavior and attacks;
- dynamic, non-linear, emergent behavior;
- dependence from contextual factors, like market and operating environment.

Capabilities of „classical“ methods to model and analyse interdependencies (simplified examples)

Key requirements	FTA / ETA	Petri Nets
Whole system approach	No (decomposition / causal chains)	Restricted, relevant states of the system and transitions (decomposition)
Dynamic, non-linear behavior, feedback loops	No (static, logical failure combinations) / limited (chronological ordering) => dynamic trees	Yes, simulation tools allow for dynamic analysis but strong restriction on non-linearities
Human factors, inclusion of context	Yes, in principle (currently limited to errors of ommision, data limitation)	Yes, in principle possible. (Workflow analysis, human error)
	=> extension of methods and data base	
Scenario generating capabilities	Limited to „ovious“ failure combinations / causal event sequences	Yes, GSPNs allow analysis of stochastic behavior.

Advanced methods: Evaluation criteria

	Modeling Focus	Design Strategies	Types of Interdependencies	Types of Events	Course of Triggered Events	Data Needs	Monitoring Area	Paradigm	Maturity
a)	Interdependency Analysis	Bottom up	Physical	Accidents	Cascading	High	Vulnerability Assessment	Discrete	High
b)	System Analysis	Top down	Cyber	Attacks	Escalating	Low	Failure Analysis	Continuous	Middle
c)			Geographic	Failures	Common cause		Mitigation/ Prevention		Poor
d)			Logical		Confined		Information gen		

Selected advanced methods and evaluation results

	Modeling Focus	Design Strategies	Types of Interdependencies	Types of Events	Course of Triggered Events	Data Needs	Monitoring Area	Paradigm	Maturity
Agent-based modeling	b)	a)	a),b),c), d)	a),b),c)	a),b),c), d)	a),b)	b), d)	a)	a)
System Dynamics	a),b)	b)	a),b)	c)	a),d)	b)	d)	a),b)	a)
Hybrid System Modeling	b)	b)	a),b),c), d)	a),b),c)	a),d)	b)	a),b),d)	a),b)	c)
Input-Output Model	a)	b)	a)	c)	a),d)	b)	b)	b)	b)
Hierarchical holographic modeling	a)	b)	a),c), d)	a),b)	c), d)	a)	a)	b)	b)
Critical Path Method	a),b)	b)	a),b),c), d)	c)	a), d)	a)	b), d)	a)	c)
High Level Architecture	a),b)	a),b)	a),b),c), d)	a),b),c),	a),b),c), d)	b)	b),c),	a)	c)
Petri Nets	a),b)	b)	a)	c)	a),c), d)	a),b)	b), d)	a)	b)

Advanced methods (excerpt)

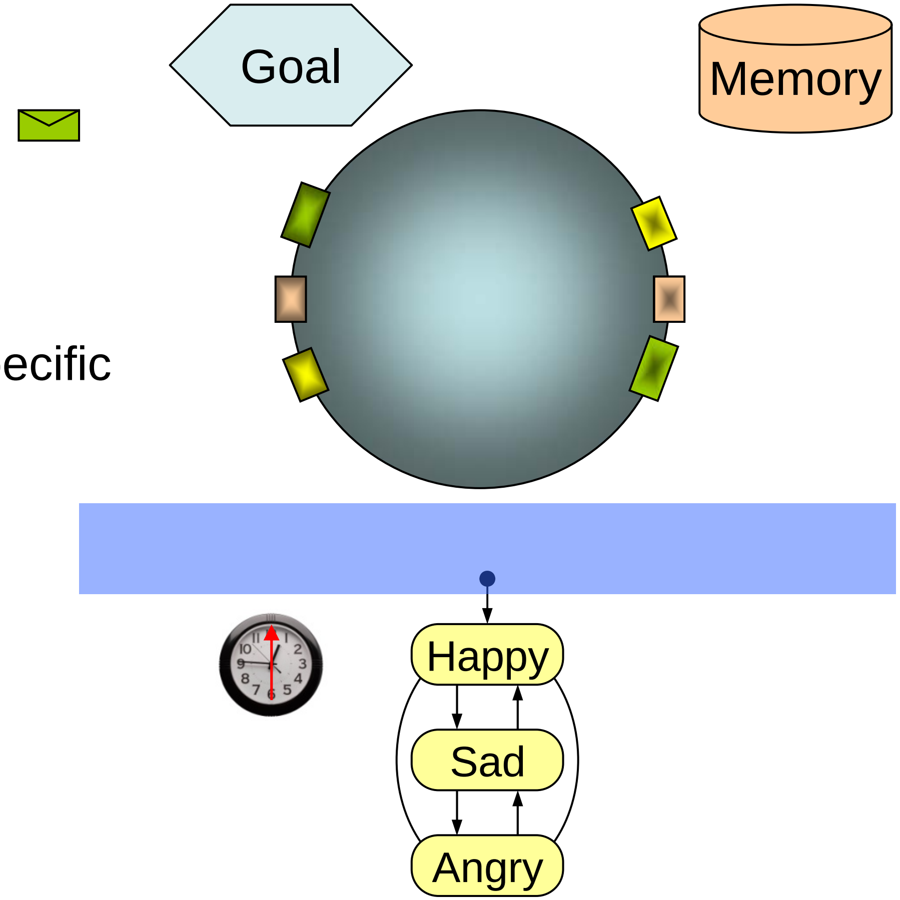
	Modeling Focus	Design Strategies	Types of Interdependencies	Types of Events	Paradigm	Relative Maturity
Agent-based modeling	System Analysis	Bottom up	Physical Cyber Geographic Logical	Accidents Attacks Failures	Discrete	High
System Dynamics	Interdependency Analysis System Analysis	Top down	Physical Cyber	Failures	Continuous Discrete	High
Petri Nets	Interdependency Analysis System Analysis	Top down	Physical	Failures	Discrete	Medium

Object-oriented modelling approach – framework

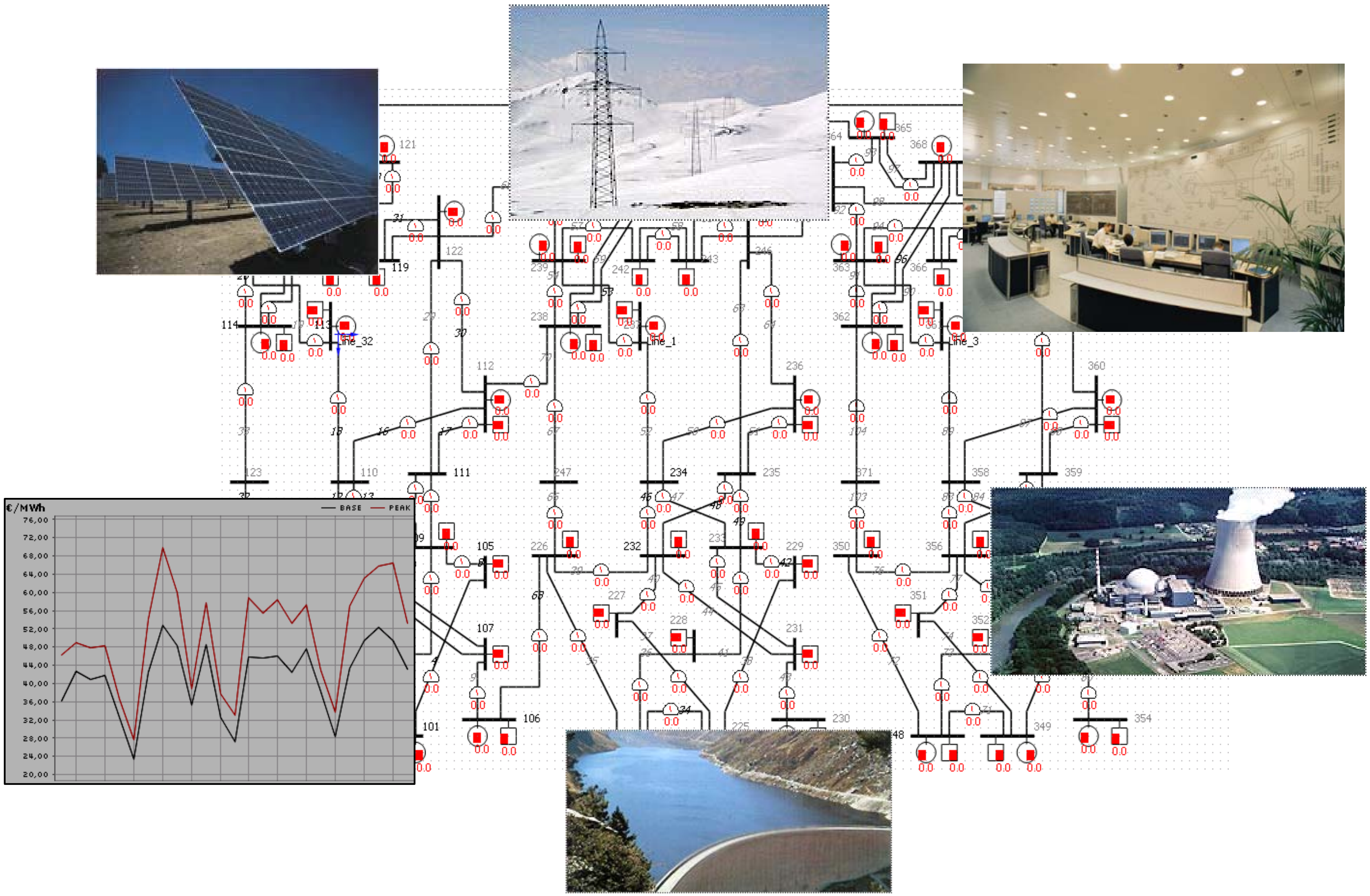
- Modelling the behaviour of the **components** (objects) and their interaction with the environment
- Stochastic simulation (Monte Carlo methods) of all components to investigate the **macro-behaviour** of the whole system
- The observed scenarios and system states are not predefined but emerge during the simulation (**emergence**)
- Frequency and consequence of events are determined “**experimentally**”

Introducing the term "object"

- **Has different states (<u>F</u>inite <u>S</u>tate <u>M</u>achine, 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



Reliability analysis of Electric Power Systems

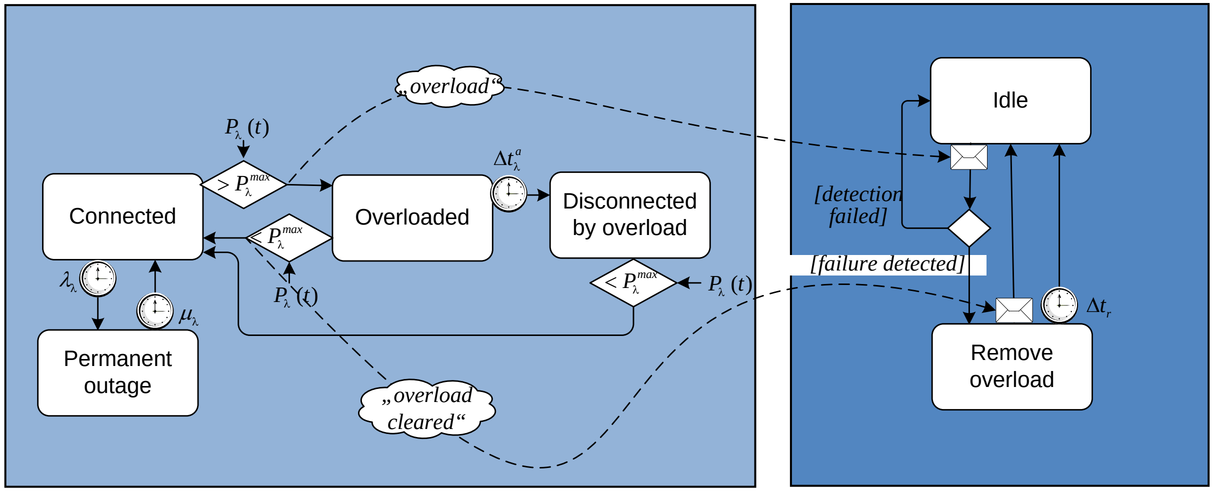


Building a simplified object-oriented model

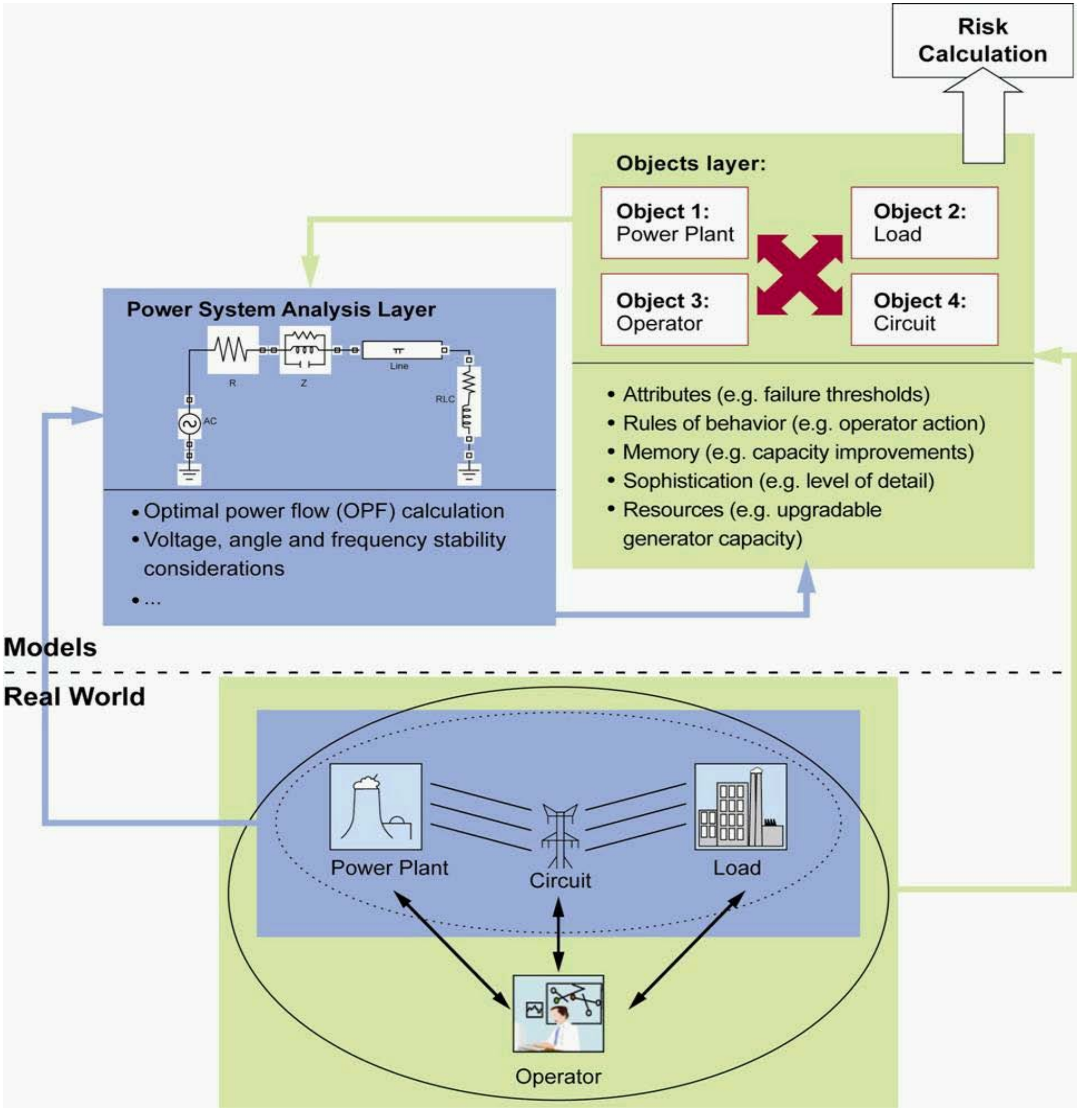
1. Identification of the components of the system:
   - Loads
   - Generators
   - Transmission lines
   - Operators

2.-4. Establishment the component states, their transitions by making use of FSM, and introducing the communication among the objects:

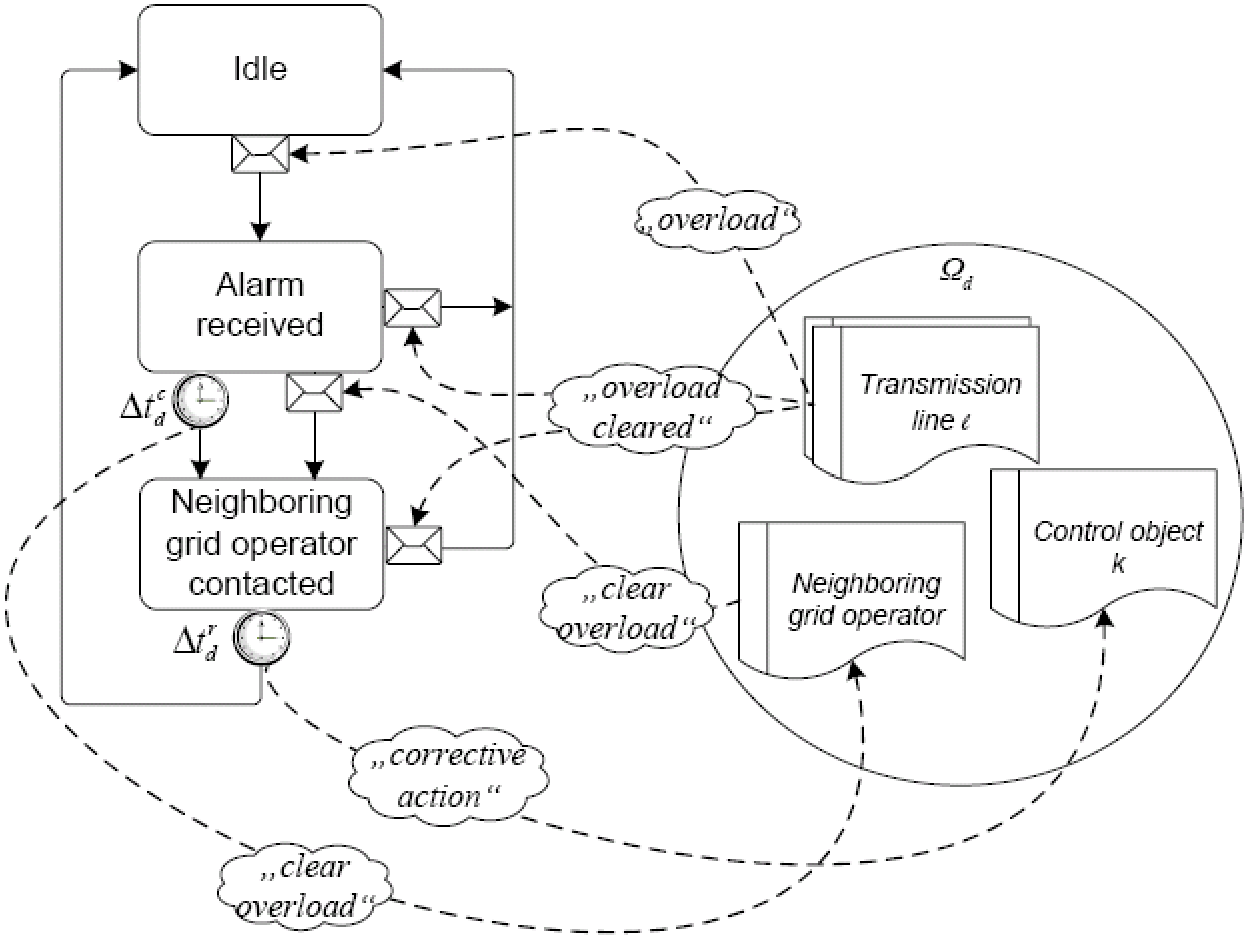
Transmission lines: Operator:



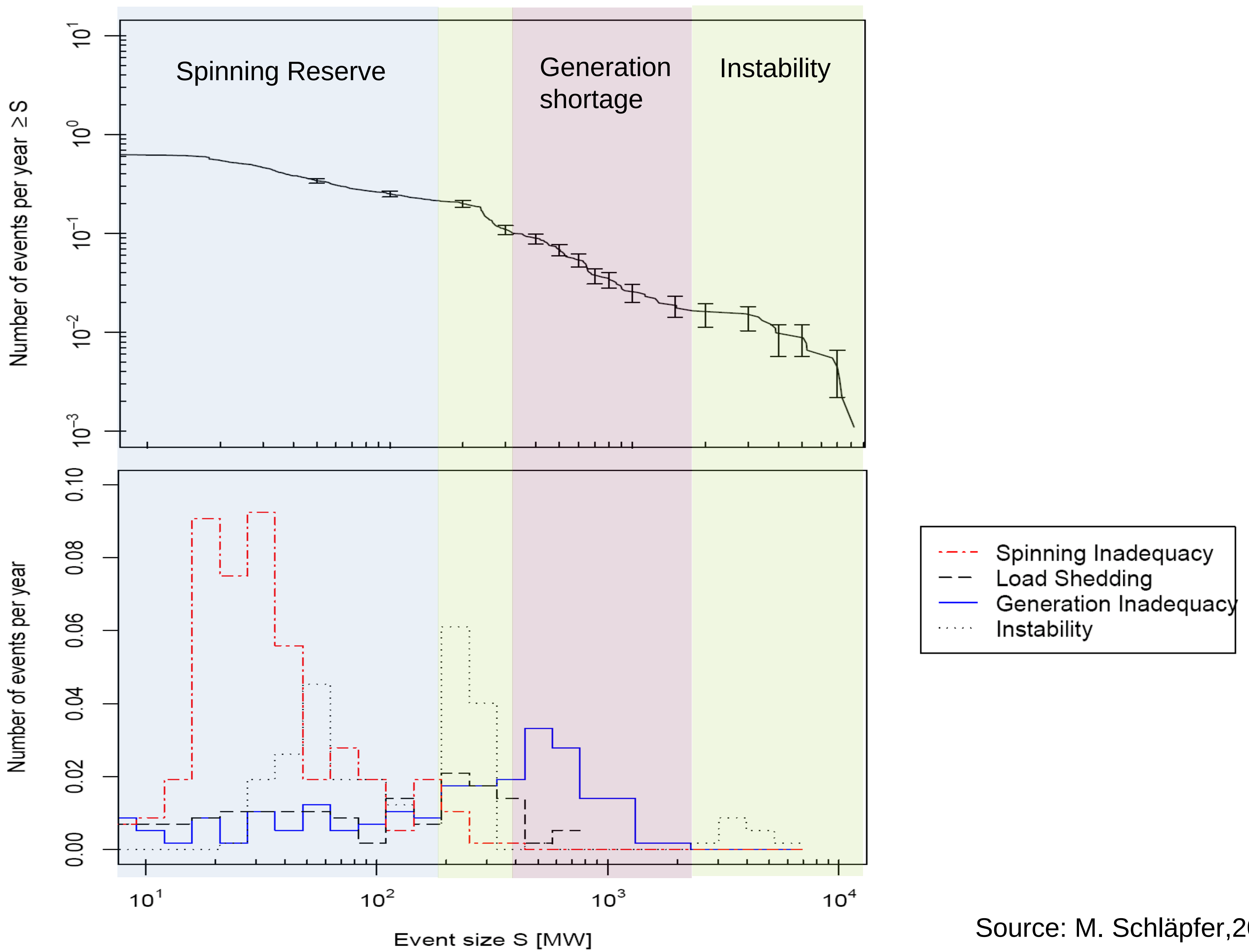
The Electric Power System – two-layer approach



Operator Action Model



The cumulative blackout frequency – and what's behind?



Source: M. Schläpfer,2008

Conclusions, take home messages

- Clear evidence that interdependencies are a real, challenging topic (not a buzzword)
- Requirements to analytical methods exceed capabilities of „classical“ methods
- Modelling and simulation techniques need to be further developed – tailored to „the problem“
- Object-oriented methods seem feasible and suitable; validation of tools and results remain a general issue