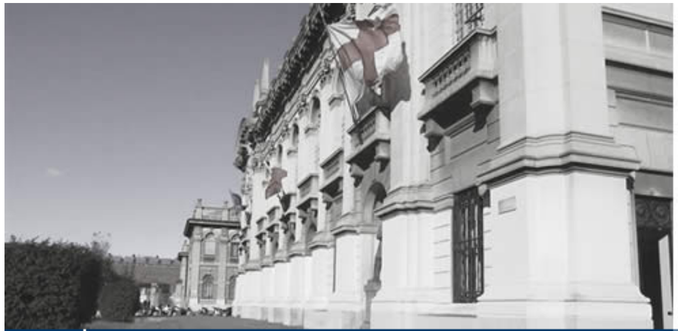


laboratory of signal and risk analysis

CENTRE DE RECHERCHE
SUR LES RISQUES
ET LES CRISES

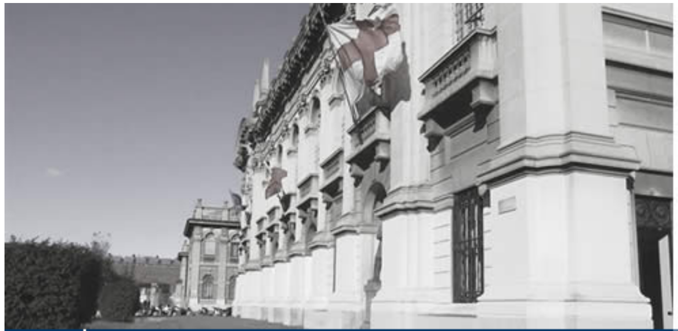
POLITECNICO DI MILANO

From systems to complex systems: from risk assessment and management to engineering resilience

Enrico Zio

- **Centrre de Recherche sur les Risques et les Crises, France,** enrico.zio@mines-paristech.fr https://www.crc.mines-paristech.fr/en/
- **Energy Department, Politecnico di Milano, Italy** enrico.zio@polimi.it www.lasar.polimi.it



POLITECNICO DI MILANO

Risk and Resilience of critical infrastructures

Concepts, definitions and frameworks

Enrico Zio

- Centrre de Recherche sur les Risques et les Crises, France, enrico.zio@mines-paristech.fr https://www.crc.mines-paristech.fr/en/
- Energy Department, Politecnico di Milano, Italy enrico.zio@polimi.it www.lasar.polimi.it

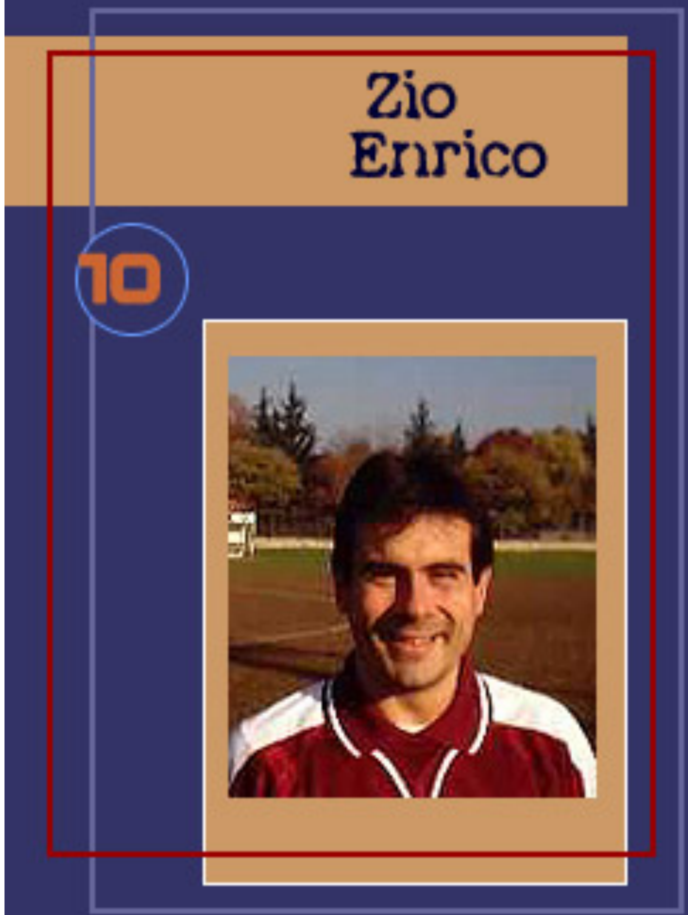
Enrico Zio

Enrico Zio received the MSc degree in nuclear engineering from Politecnico di Milano in 1991 and in mechanical engineering from UCLA in 1995, and the Ph.D. degree in nuclear engineering from Politecnico di Milano and in probabilistic risk assessment at MIT in 1996 and 1998, respectively.
He is currently full professor at the Centre for research on Risks and Crises (CRC) of Ecole de Mines, ParisTech, PSL University, France, full professor and President of the Alumni Association at Politecnico di Milano, Italy, distinguished guest professor at Tsinghua University, Beijing, China, adjunct professor at City University of Hong Kong, Beihang University and Wuhan University, China and Co-Director of the Center for REliability and Safety of Critical Infrastructures (CRESCI) and the sino-french laboratory of Risk Science and Engineering (RISE), at Beihang University, Beijing, China.

In 2020, he has been awarded the prestigious international Humboldt Research Award in Germany.
In 2021, he has been appointed as 4TU.Resilience Ambassador by the 4TU Centre for Resilience Engineering of the four Dutch Technical Universities.
In 2021, he has been named Fellow of the of the Prognostics & Health Management Society.
In 2023, he has been appoointed Scientific Director of Datrix SpA.

He is IEEE and Sigma Xi Distinguished Lecturer.

Speaker



signed for Panthers: July 1998

Better known "***Little knee***" for his ease in running.

After the much talked retirement of the "*Divine Ponytail*" (Roberto Baggio), he stands as the last true and pure artist of the Italian soccer. He remains a patrimony to be safeguarded, in spite of the " *tactical problem*" he represents for the Panthers team.

Fancy on the field and even brilliant off the field: meeting him disguised as Santa Claus at weddings or as deejay in popular Milano's bars, one would never realize that he is an internationally renowned luminary.

Hazard

Hazard: concepts and definitions

- Hazard (threat): … 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

- Hazard (threat): … a possible / potential source of danger….
- Danger: a state, factor [circumstance], or action which may cause damage to persons, the environment and/or goods. Examples: tank filled with gasoline, a knife.

Hazard: concepts and definitions

- Hazard (threat): … a possible / potential source of danger….
- Danger: a state, factor [circumstance], or action which may cause damage to persons, the environment and/or goods. Examples: tank filled with gasoline, a knife.
- Disasters in the past revealed that "hazard-centric" perception / concepts are too limited because

"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).

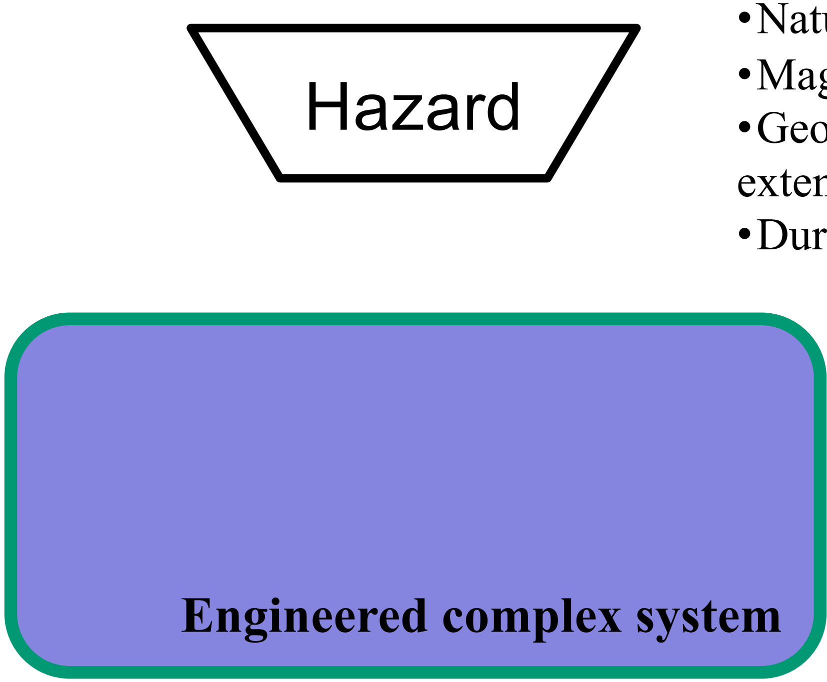
Vulnerability

Vulnerability and failures

Hazard

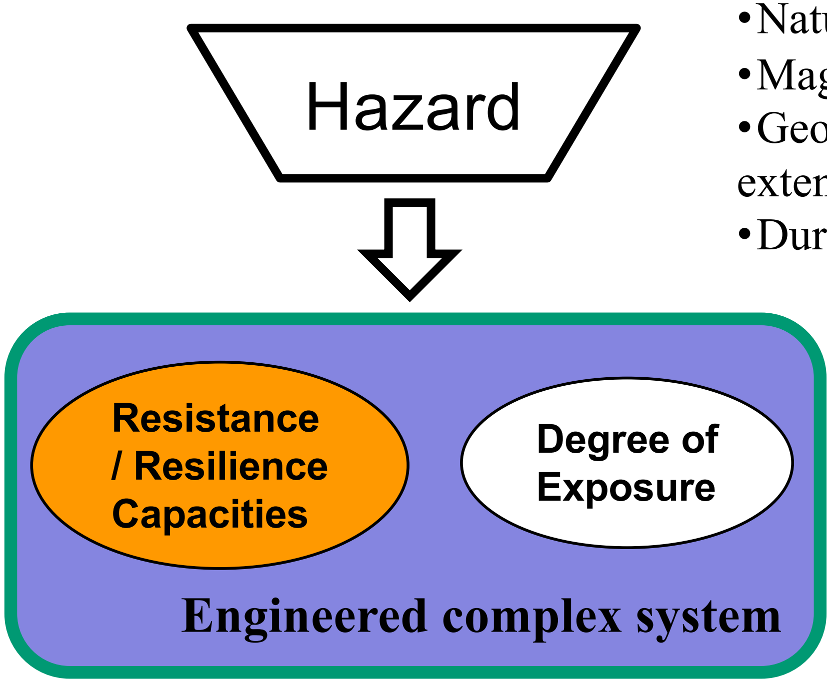
- Nature
- Magnitude
- Geographical extent
- Duration
- Spatial dispersion
- Speed of onset
- Frequency/Probability

Vulnerability and failures



- Nature
- Magnitude
- Geographical extent
- Duration
- Spatial dispersion
- Speed of onset
- Frequency/Probability

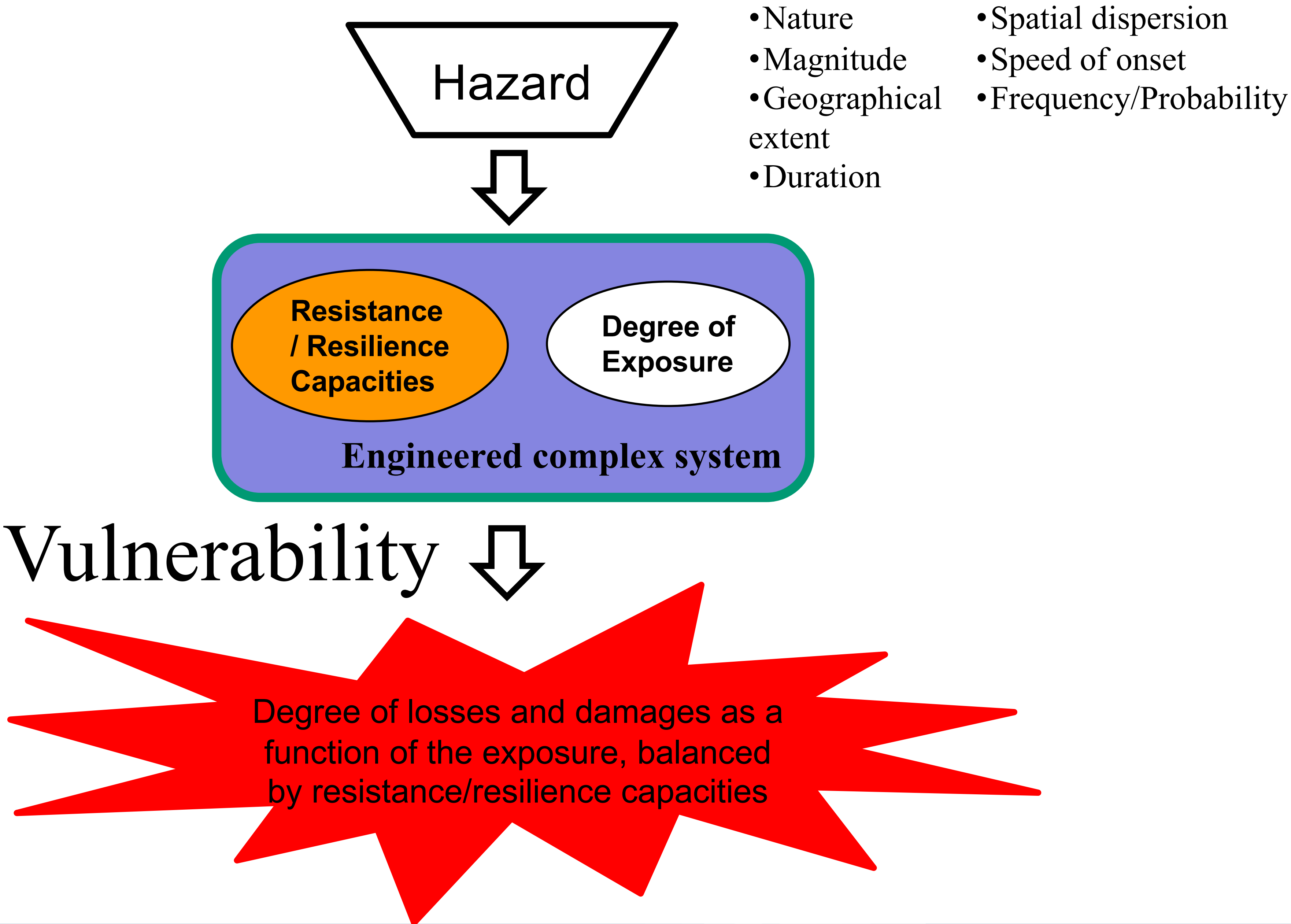
Vulnerability



- Nature
- Magnitude
- Geographical extent
- Duration
- Spatial dispersion
- Speed of onset
- Frequency/Probability

Vulnerability

Vulnerability and failures



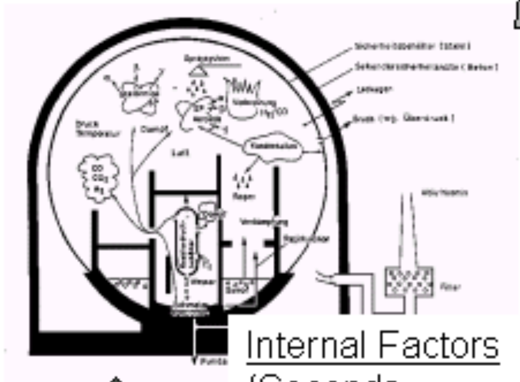
Vulnerability - Technical Example

External Threats

Short Distance Threat
(700 km/h)

Long Distance Threat
(10 m/s)

Short or Long Distance
Threat / Intentional
Software Attack
(Speed of Light)



Internal Factors
(Seconds,
Minutes, Hours)

Earthquake

- Information gathering
- Beyond the existing experience
- Intentional attack (sabotage and /or war)

Vulnerability - Societal Example

Intentional Attack (Cargo Airplane)

External Threats

Accidental Situation
(Transportation Dangerous Goods)

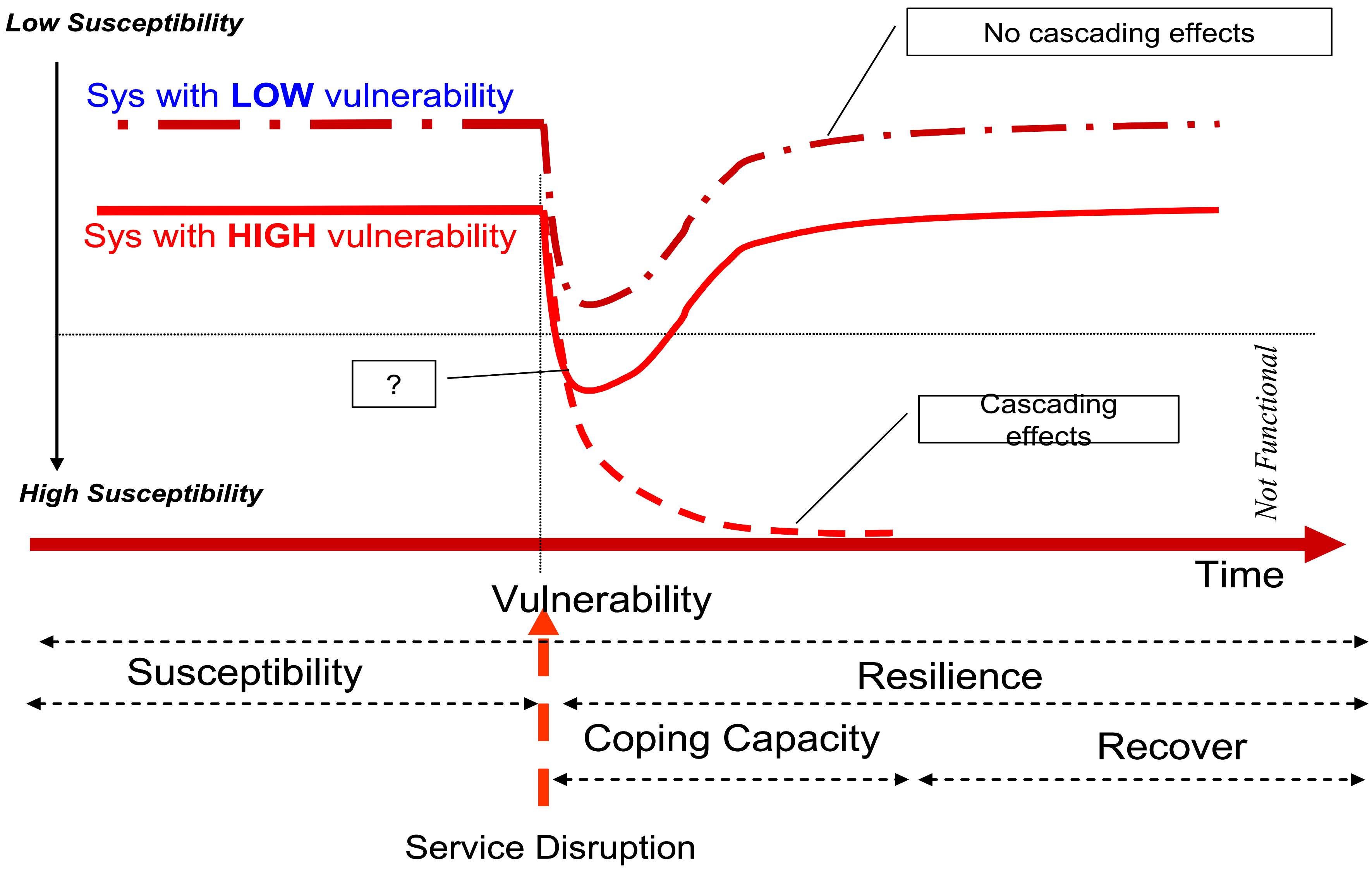
Congested
and/or crowded
areas

Internal Factors

- Technical Failure
- Panic
- Un-managed police intervention
- Weak management of the establishment

Vulnerability Assessment

Vulnerability Scenarios

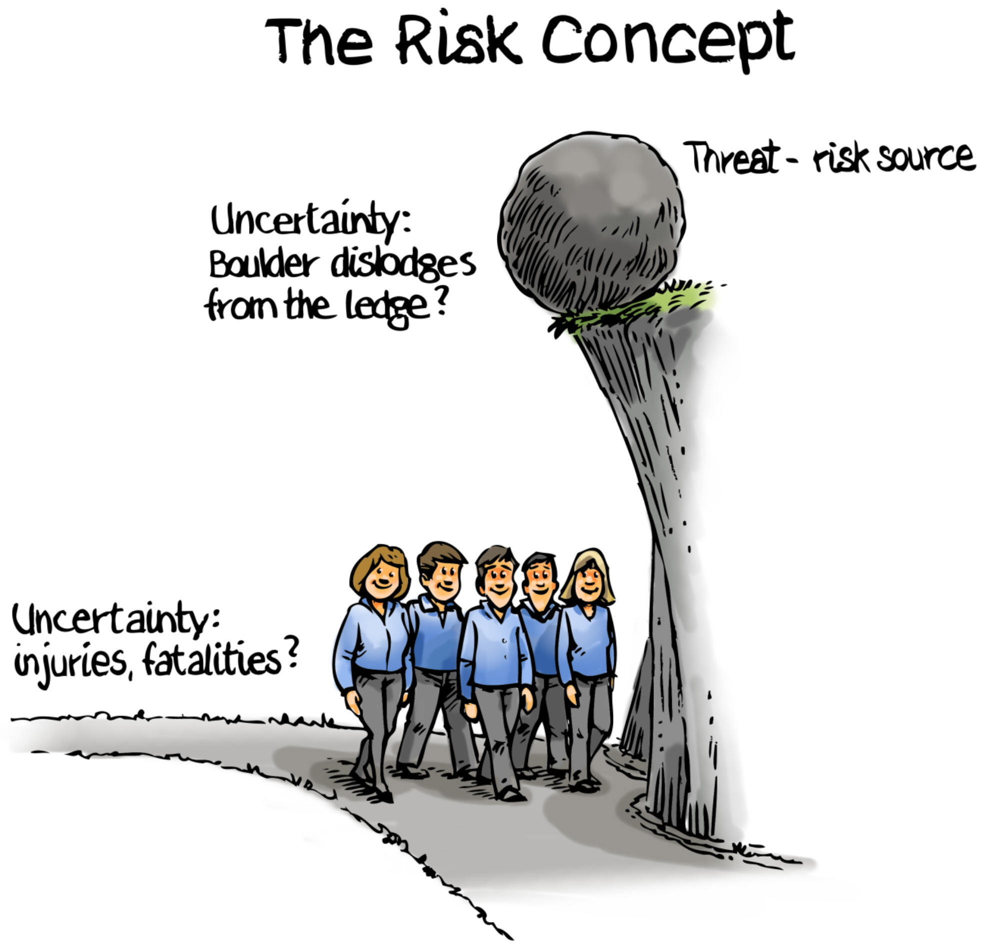


RISK

Consequences

Events with some effects

Some effects are undesirable



Uncertainty

The risk concept

How to measure or describe risk ?

Consequences & Uncertainty

•RISK = POTENTIAL DAMAGE + UNCERTAINTY

Dictionary: RISK = possibility of damage or injury to people or things

1) What undesired conditions may occur? → Accident Scenario, S
2) With what probability do they occur? → Probability, p
3) What damage do they cause? → Consequence, x

$$\text{RISK} = \{S_i, p_i, x_i\}$$

S. Kaplan. B.J. Garrick, On the quantitative definition of risk, Risk Analysis, 1981

RISK ASSESSMENT

RISK ASSESSMENT:

Systemic Analysis of system performance under undesired conditions (uncertain space)

⬇

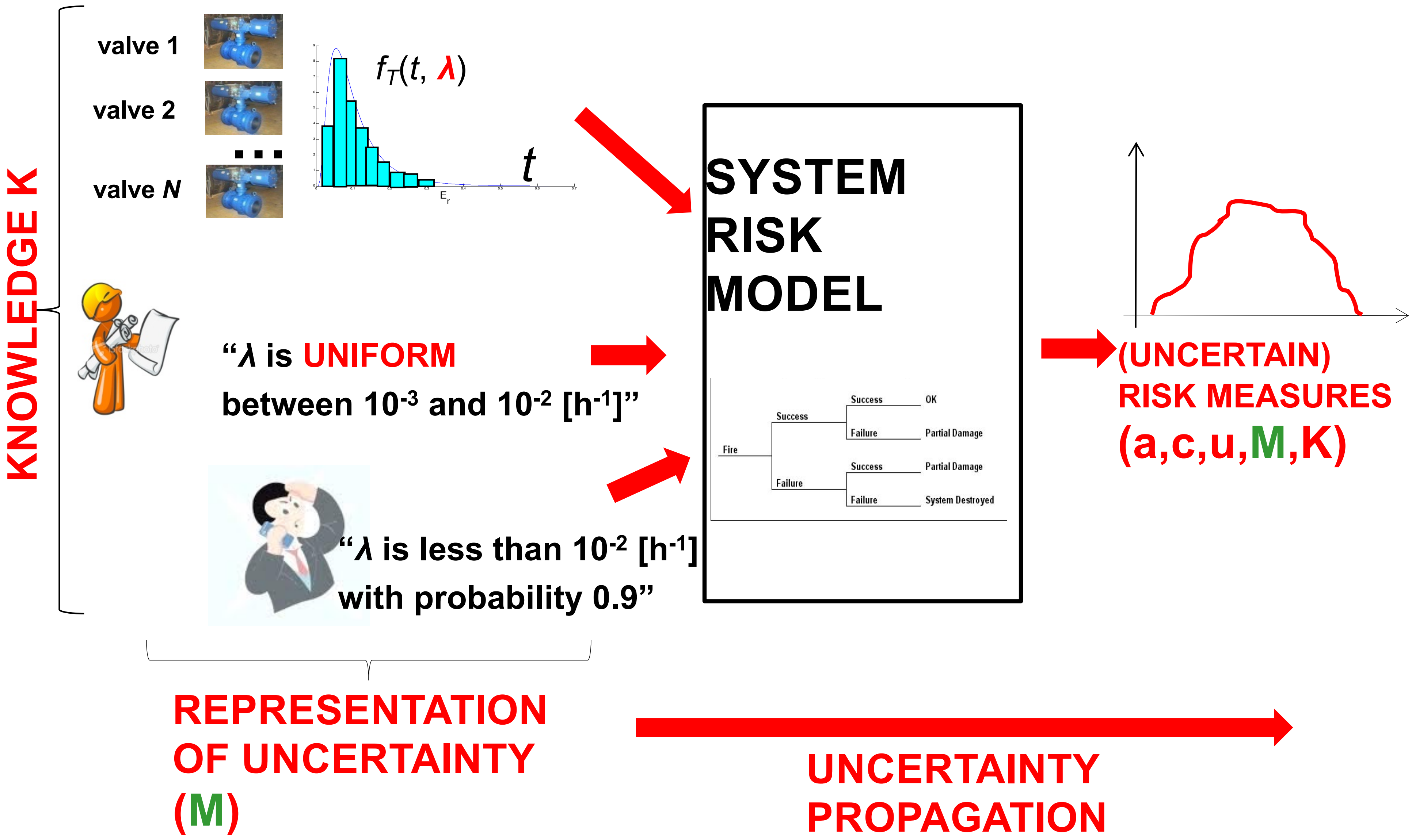
System/Man/Environment interactions under uncertainty

⬇

PROBABILISTIC RISK ASSESSMENT

(QUANTITATIVE RISK ASSESSMENT)

Risk Assessment



Probabilistic Risk Assessment

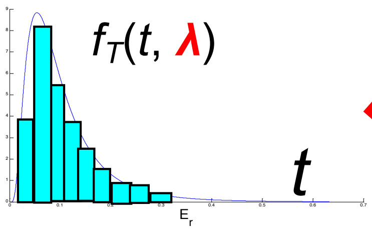
KNOWLEDGE K

valve 1

valve 2

...

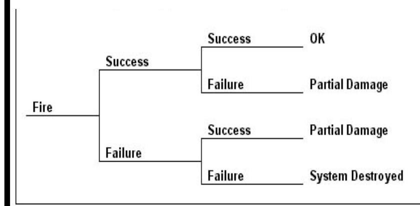
valve *N*

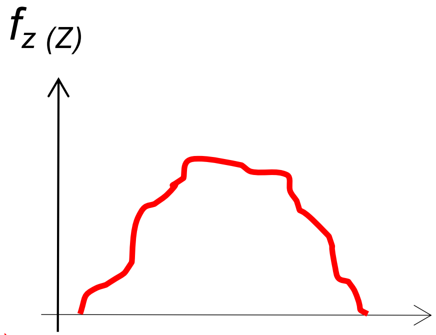


"λ is **UNIFORM** between 10^{-3} and 10^{-2} [h^{-1}]"

"λ is less than 10^{-2} [h^{-1}] with probability 0.9"

SYSTEM RISK MODEL





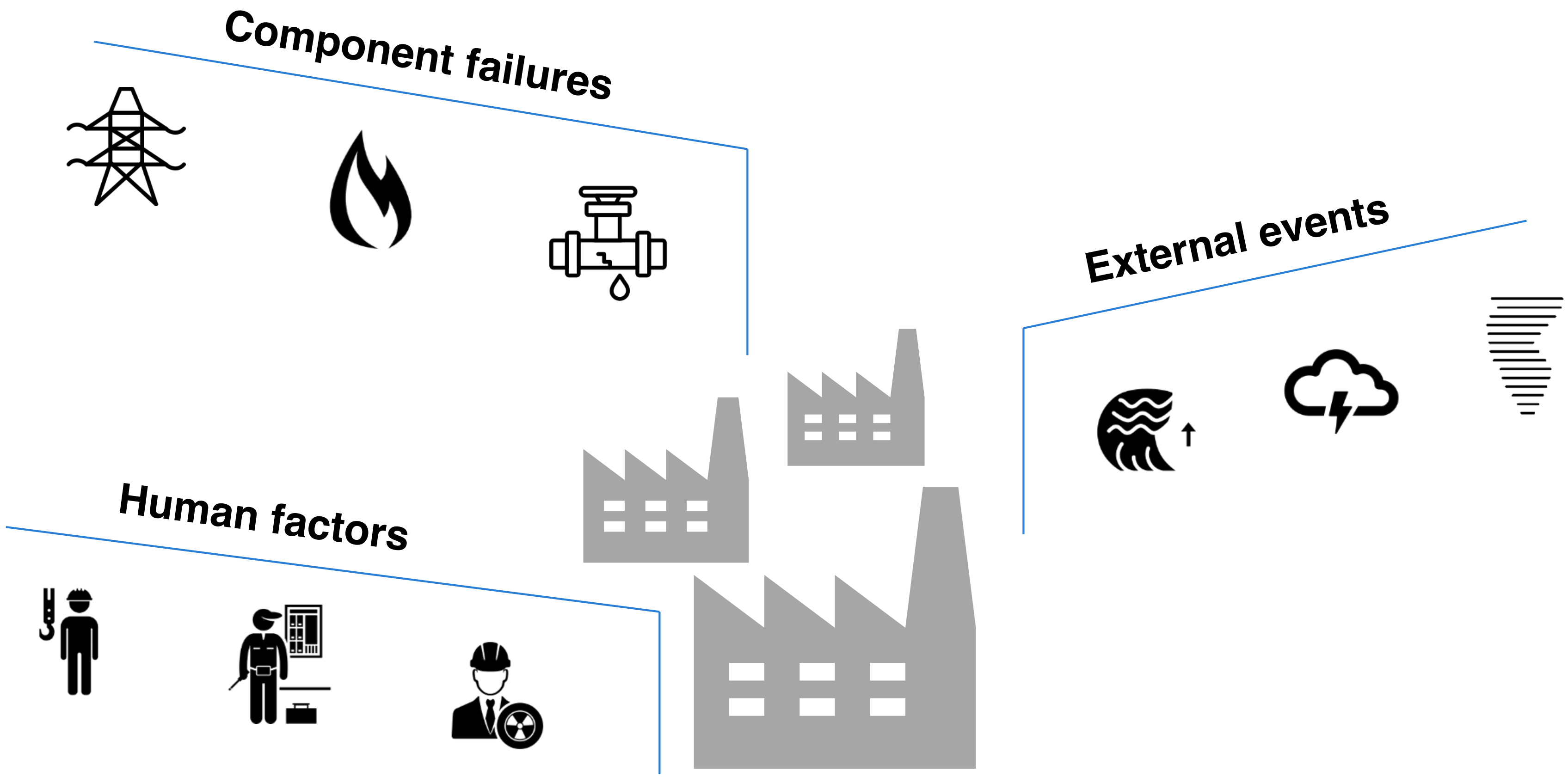
(PROBABILISTIC) RISK MEASURES

(a,c,u,P,K)

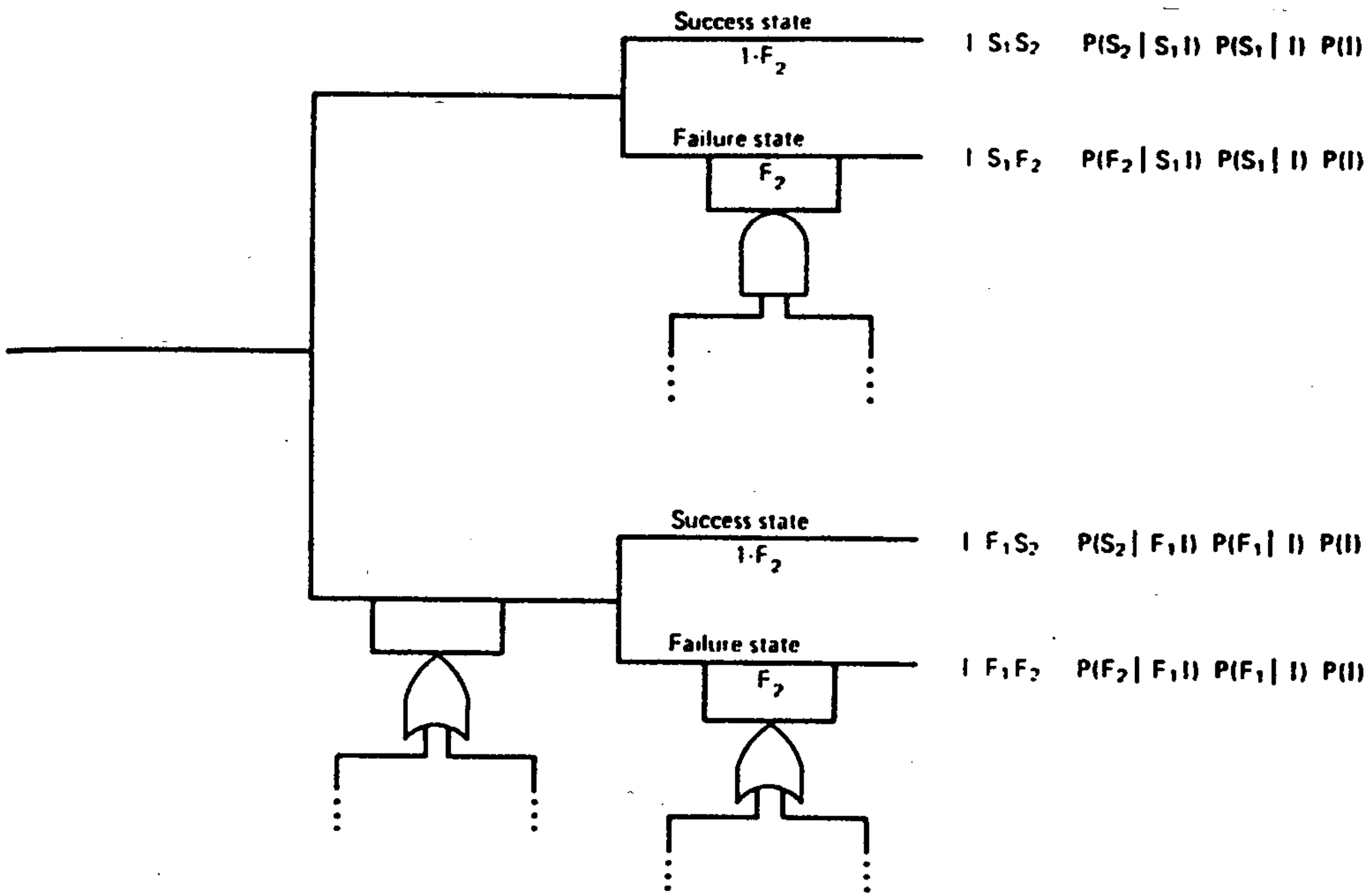
PROBABILISTIC REPRESENTATION OF UNCERTAINTY (M=P)

UNCERTAINTY PROPAGATION

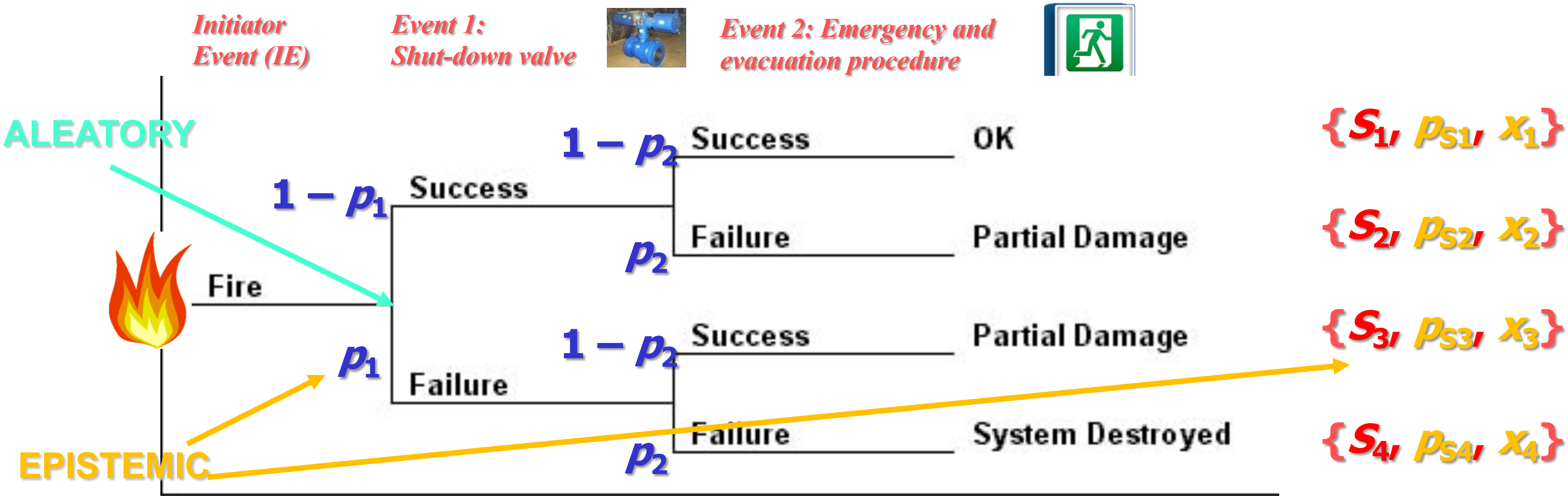
HAZARDS



Event Trees/Fault Trees



(aleatory and epistemic) Uncertainty



Aleatory: variability, randomness (in occurrence of the events in the scenarios)

Epistemic: lack of knowledge/information (probability and consequence models)

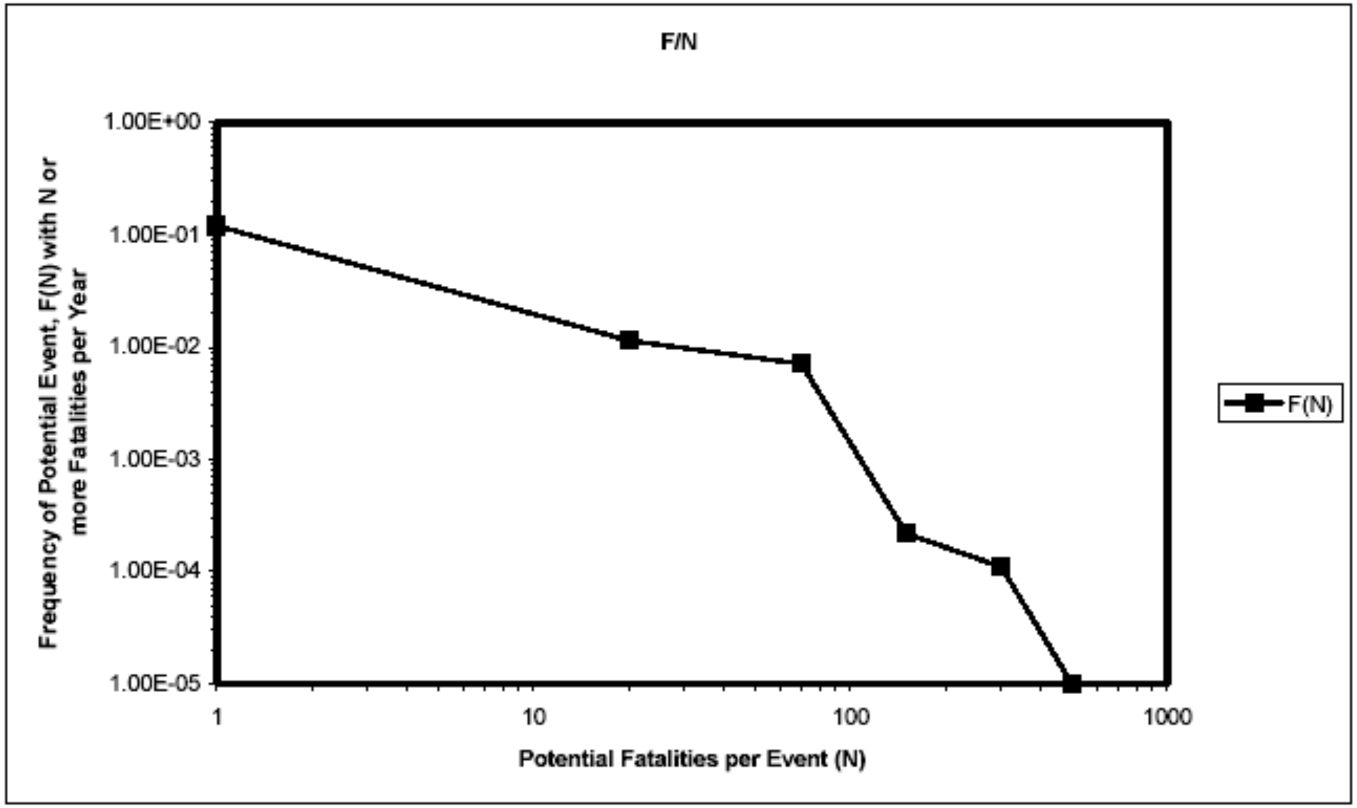
PRA results:

$\{S_i, p_i, x_i\}$

S	p	x
S_1	p_1	x_1
…	…	…
S_N	p_N	x_N

Example of F/N graph

Scenario	Number (N) of Potential Fatalities	Frequency of Scenario per Year	Frequency of Incidents with Potential (N) or more Fatalities per Year
1	1	0.1	0.12021
2	20	0.014	0.01141
3	70	0.0075	0.00713
4	150	0.00023	0.00022
5	300	0.00009	0.00011
6	500	0.00001	0.00001



RISK MATRIX:

The level of risk is broadly acceptable and generic control measures are required aimed at avoiding deterioration.

Consequence					Increasing Annual Frequency					
					0	A	B	C	D	E
Severity	People	Environ.	Assets	Reputation	Practically non-credible occurrence	Rare occurrence	Unlikely occurrence	Credible occurrence	Probable occurrence	Likely/Frequent occurrence
					Could happen in E&P industry	Reported for E&P industry	Has occurred at least once in Company	Has occurred several times in Company	Happens several times/y in Company	Happens several times/y in one location
1	Slight health effect / injury	Slight effect	Slight damage	Slight impact			Continuous Improvement			
2	Minor health effect / injury	Minor effect	Minor damage	Minor impact					Risk Reduction Measures	
3	Major health effect / injury	Local effect	Local damage	Local impact						
4	PTD(*) or 1 fatality	Major effect	Major damage	National impact						Intolerable Risk
5	Multiple fatalities	Extensive effect	Extensive damage	International impact						

The level of risk can be tolerable only once a structured review of risk-reduction measures has been carried out

The level of risk is not acceptable and risk control measures are required to move the risk figure to the previous regions.

RISK ASSESSMENT

Risk Assessment is conditioned on the Knowledge

Possible Accident Scenarios

Knowledge Available

$$\boldsymbol{Risk} = (\mathcal{A}, \mathcal{C}, \mathcal{Q}; \mathcal{K})$$

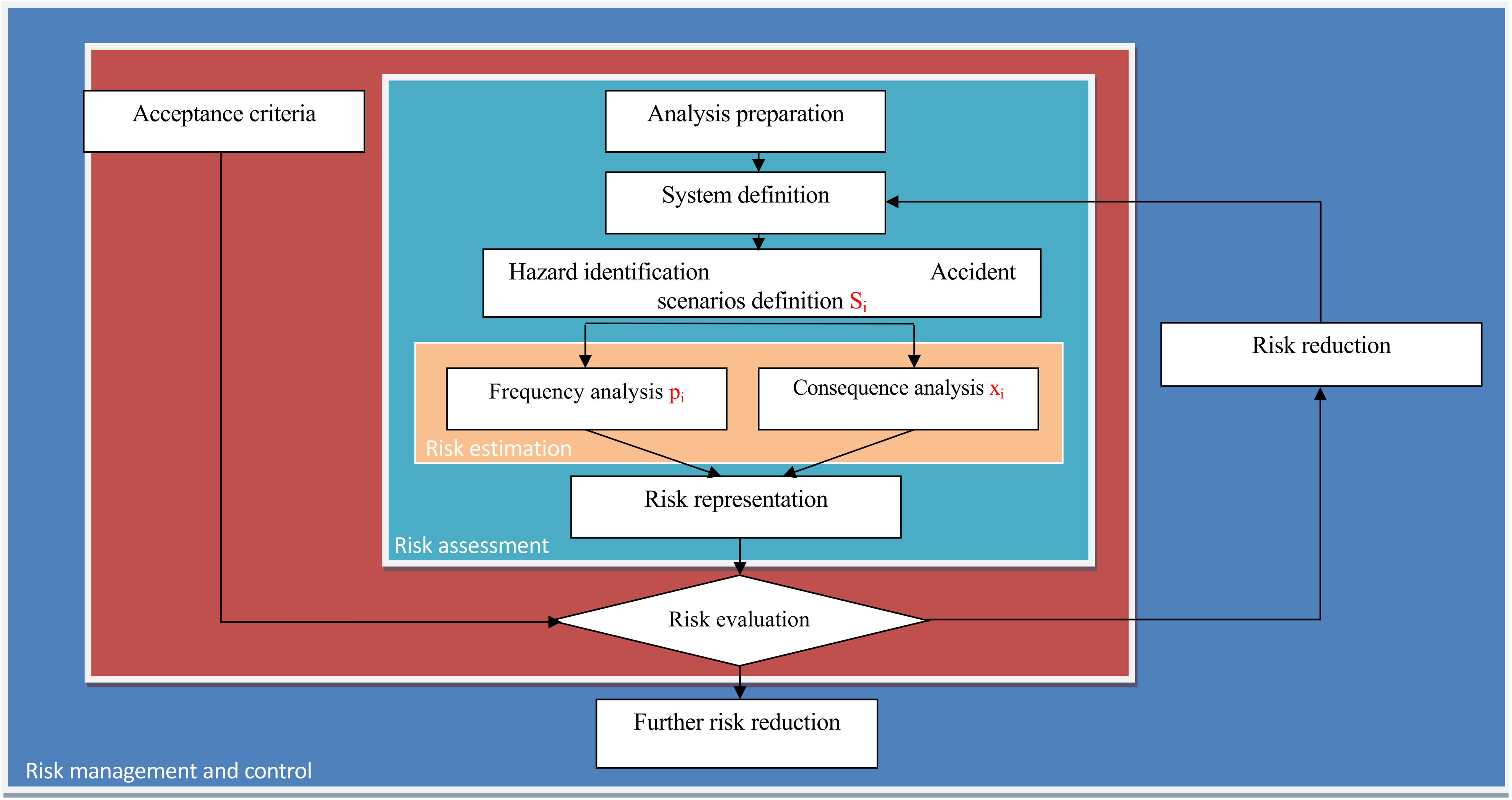
Consequences

Uncertainty

Risk Assessment: main steps

1. System description and modeling
2. Historical analysis of past accidents
3. Hazard identification
4. Selection of most critical hazards and identification of Initiating Events (IEs)
5. Analysis of the accident sequences deriving from the IEs
6. Evaluation of risk → decision-making process

Risk Assessment and Management



Main strategies for handling risk

Codes and standards – simple problems

Risk assessment informed

Robustness, resilience-based strategies

Cautionary/ precautionary principles

Dialogue

Balancing other concerns

Balance

Development and protection

Develop,
creating values

Take risk

Reduce the risks
and uncertainties

Cost-benefit analyses

ALARP

cautionary-
precautionary

Risk acceptance criteria

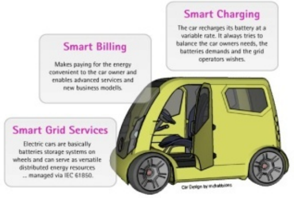
WORLD 4.0

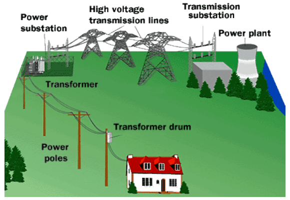
Systems, structures and infrastructures

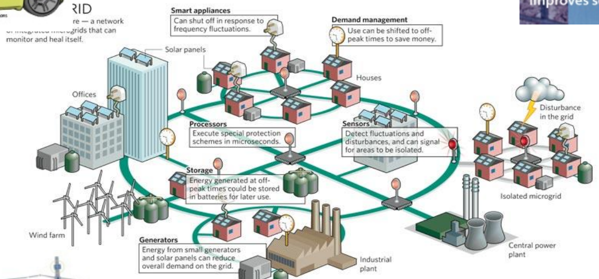
WORLD 4.0: smart systems

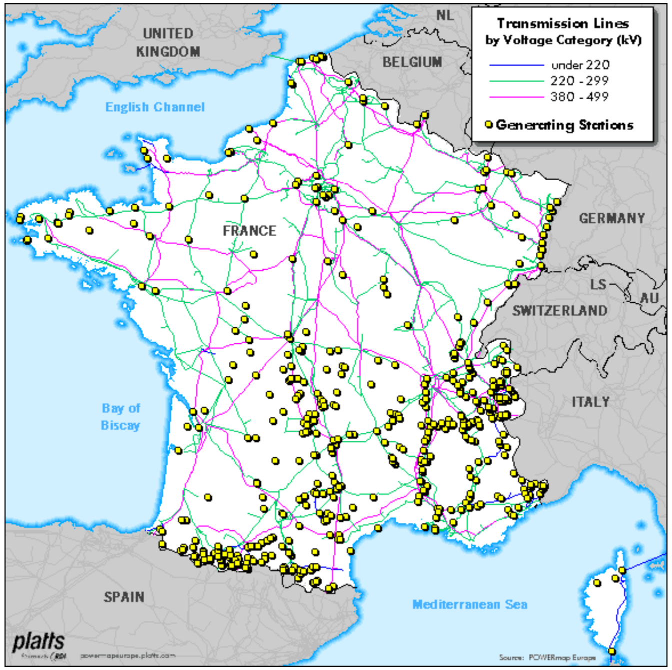
Complex Systems

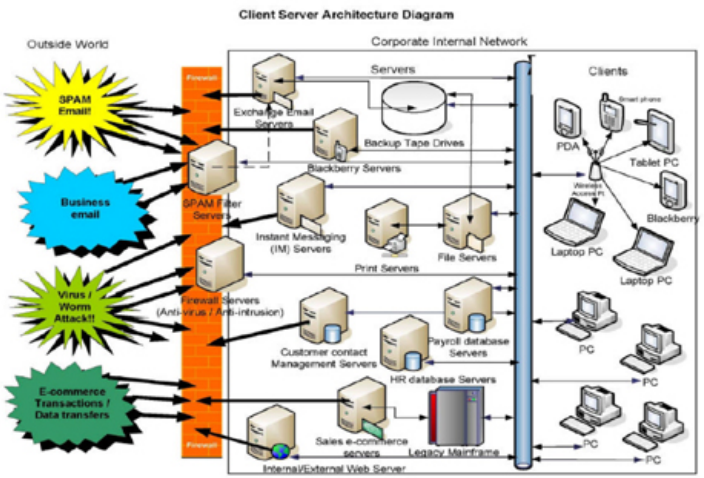
Complex (technical) systems



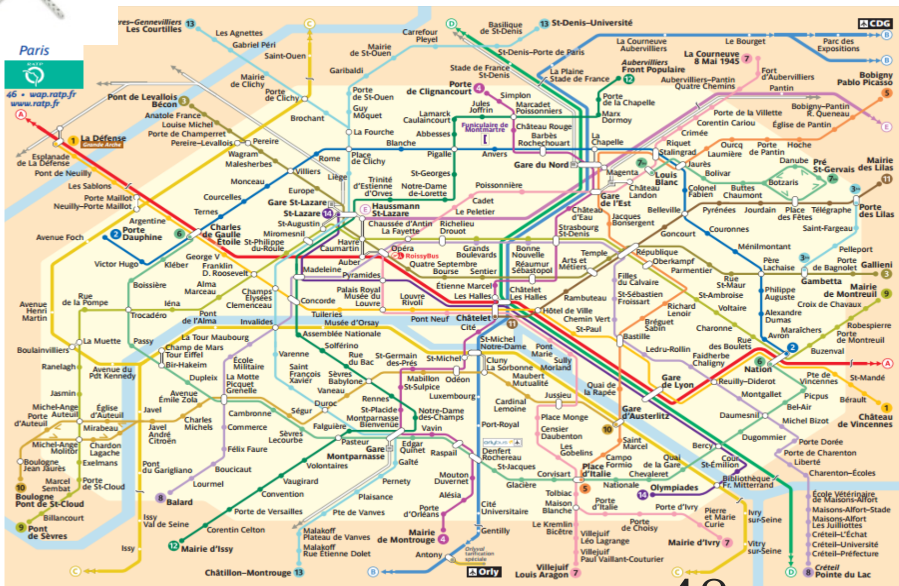








Microsoft submission to Federal Rules Committee



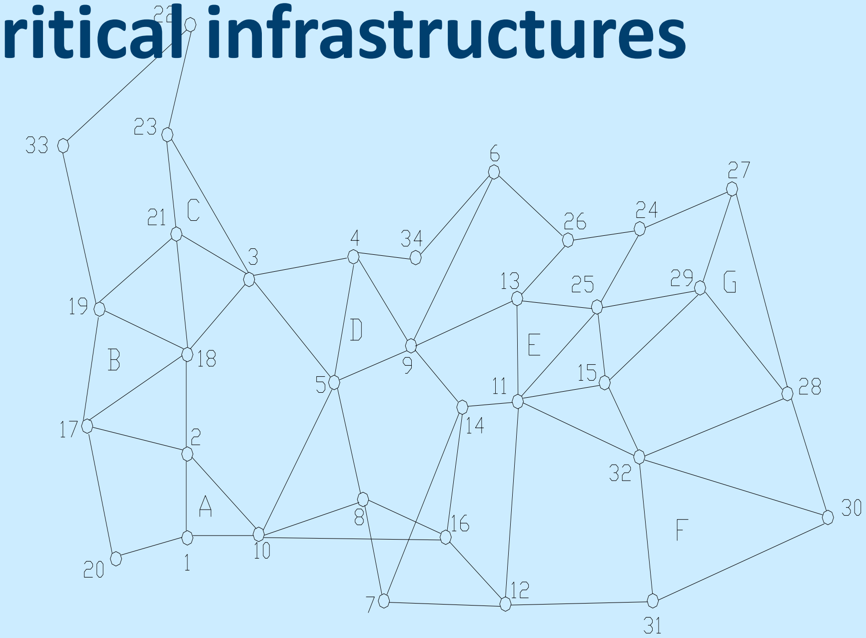
Complex (technical) systems

- Network of many interacting components
- Components of heterogeneous type
- Hierarchy of subsystems
- Interactions across multiple scales of space and/or time

Dependences (uni-directional) and interdependences (bi-directional)

Critical Infrastructures

Critical infrastructures



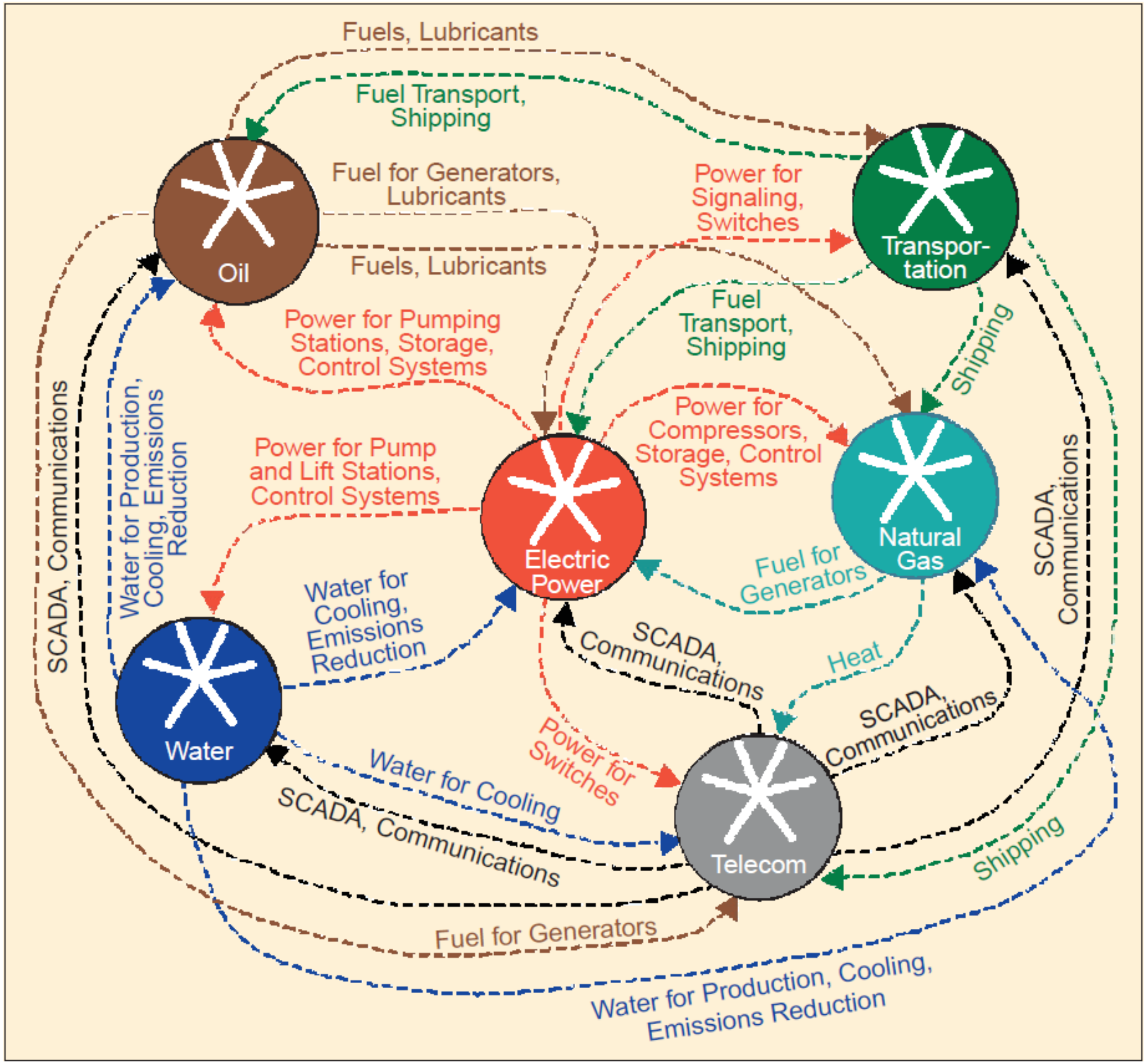

Water supply Systems


Gas supply Systems

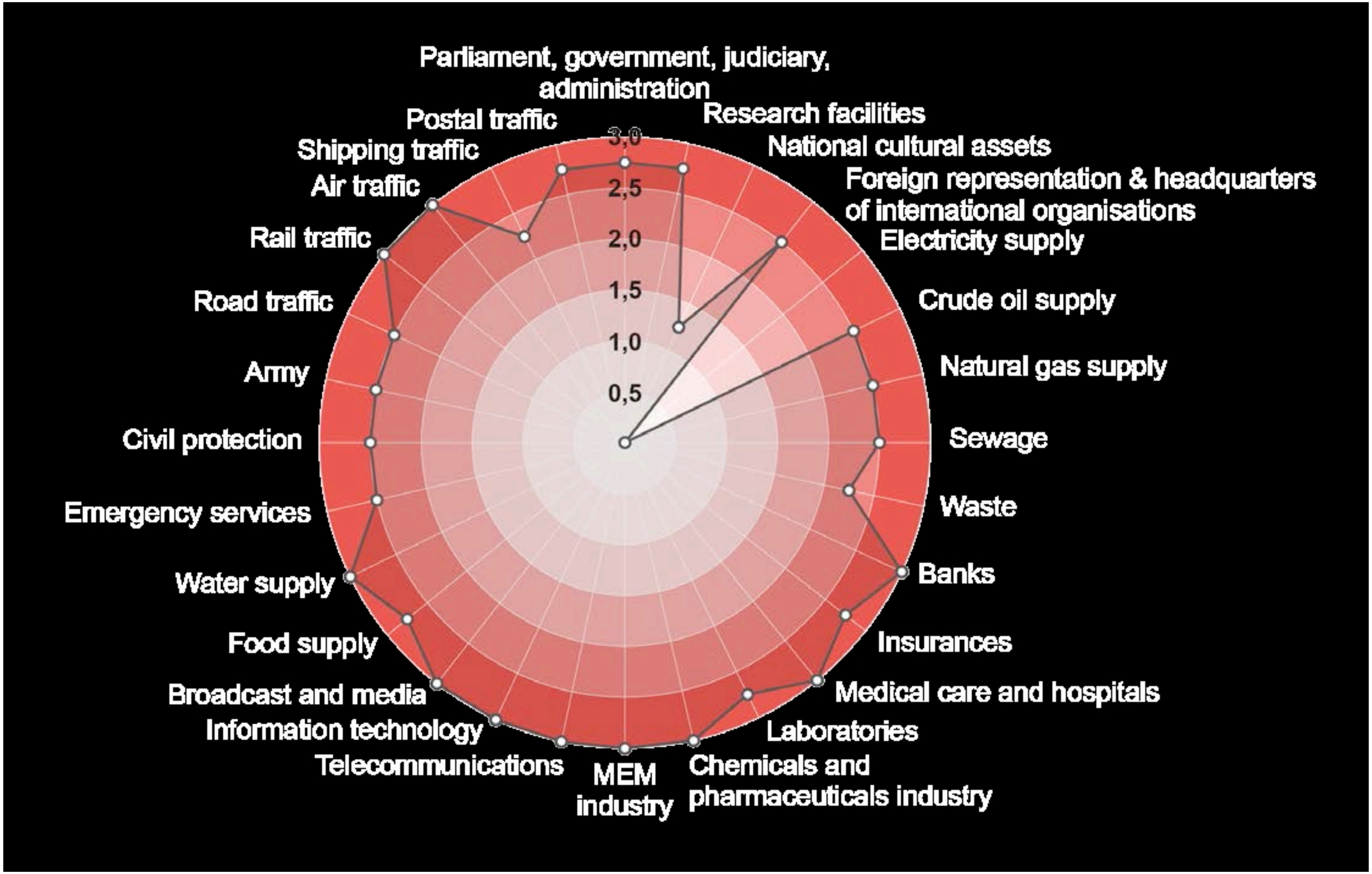

Electric Power Networks

Critical Infrastructures: structural complexity

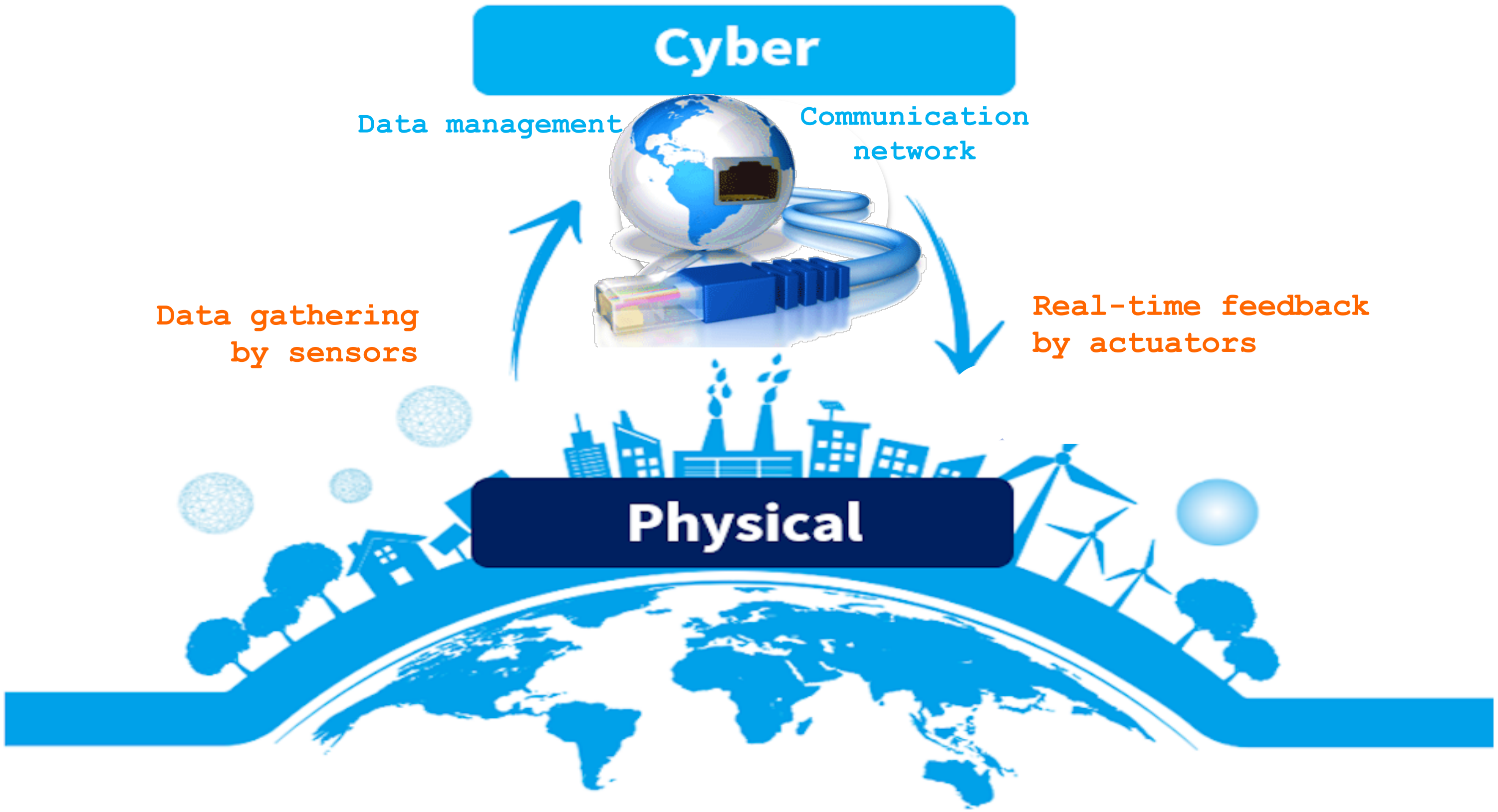
Example of infrastructures **interdependencies** [Rinaldi et al. 2001]



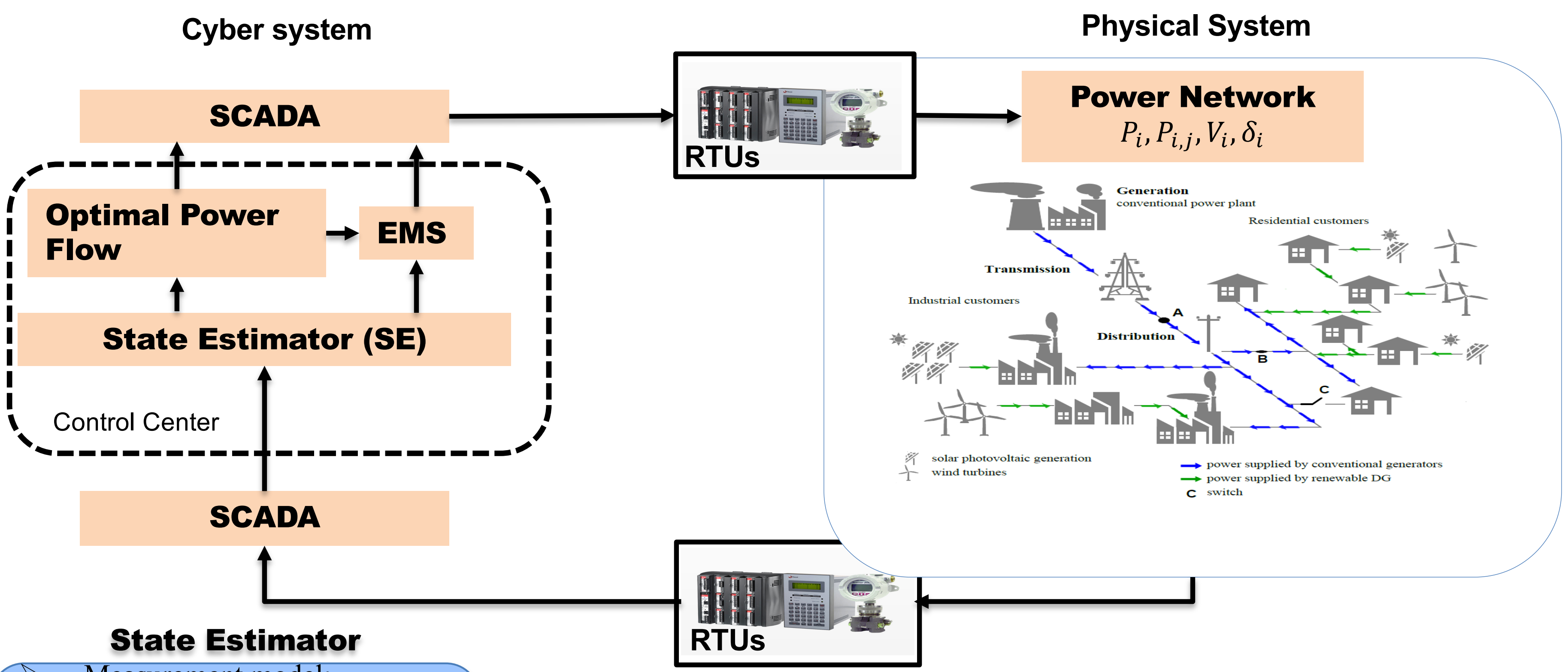
Critical Infrastructures and their interdependencies



Critical infrastructures: cyber-physical system of systems (CPS)



Critical infrastructures: cyber-physical system of systems (CPS)

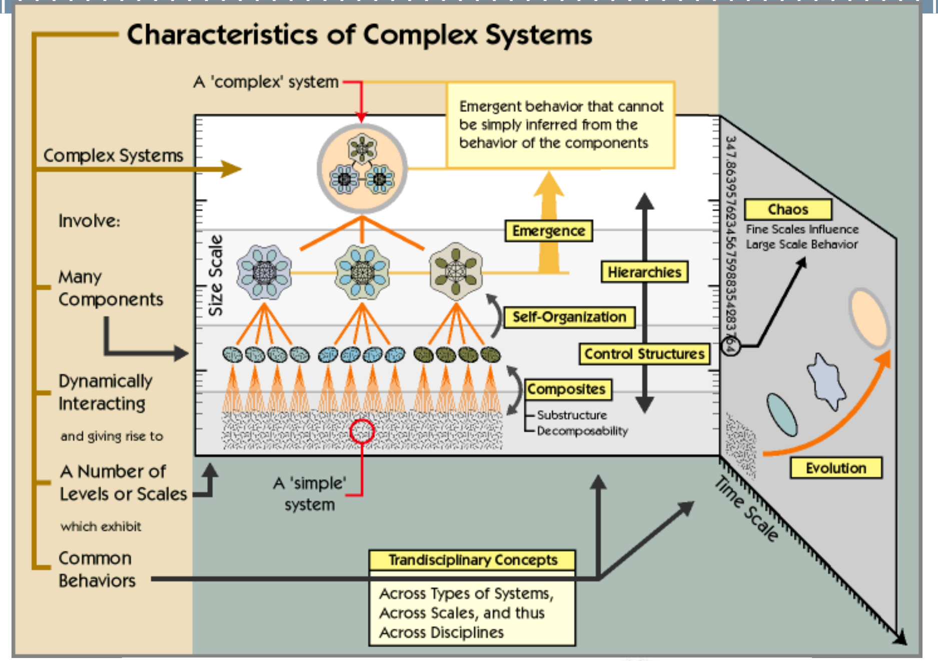


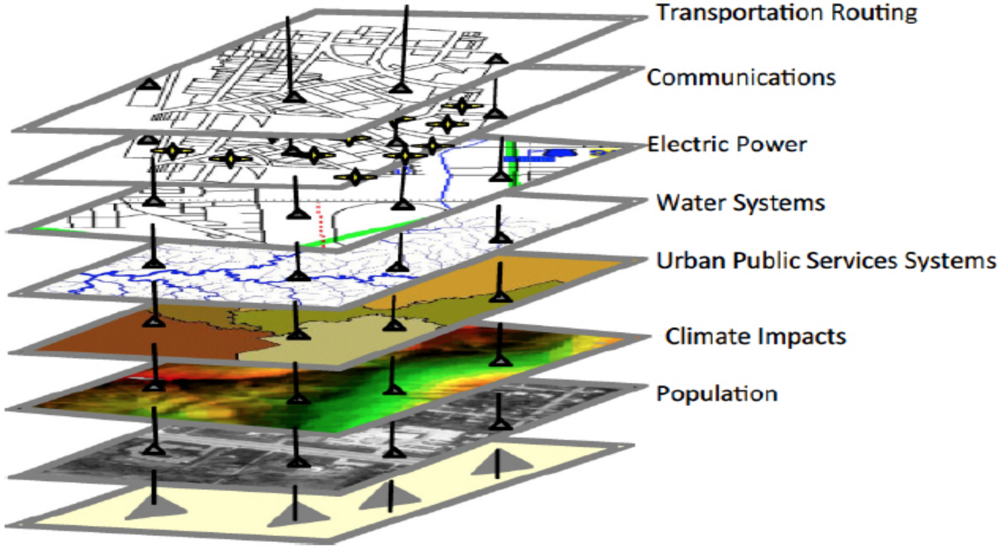
State Estimator

- Measurement model:
  $z = Hx + e$
- State Estimation :
  $\hat{x} = (H^T W H)^{-1} H^T W z$

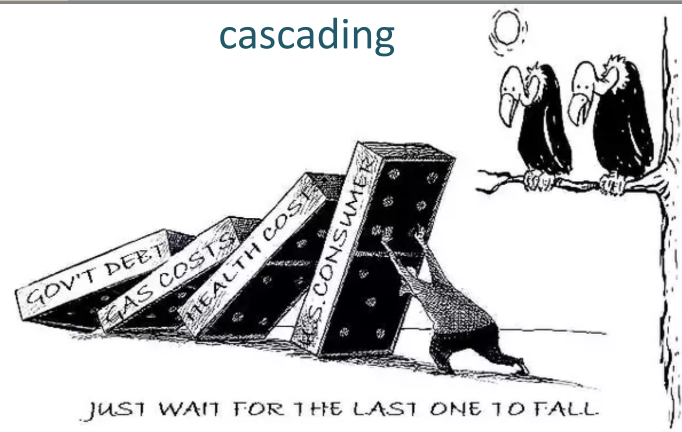
Complexity: structural & dynamic

Interdependency: engineered "system-of-systems"

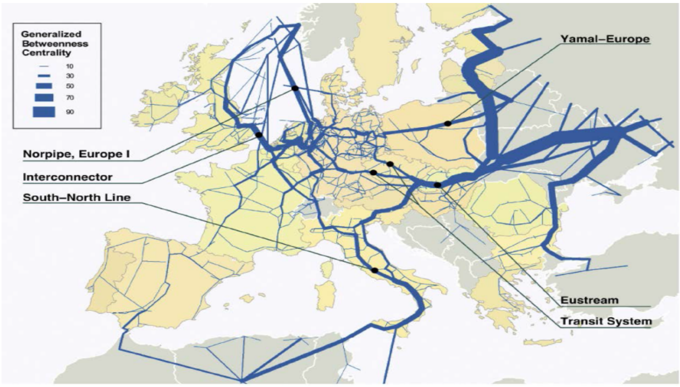


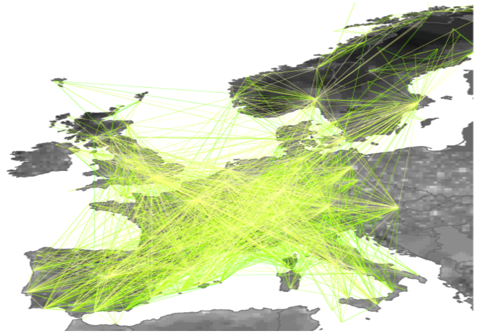


cascading

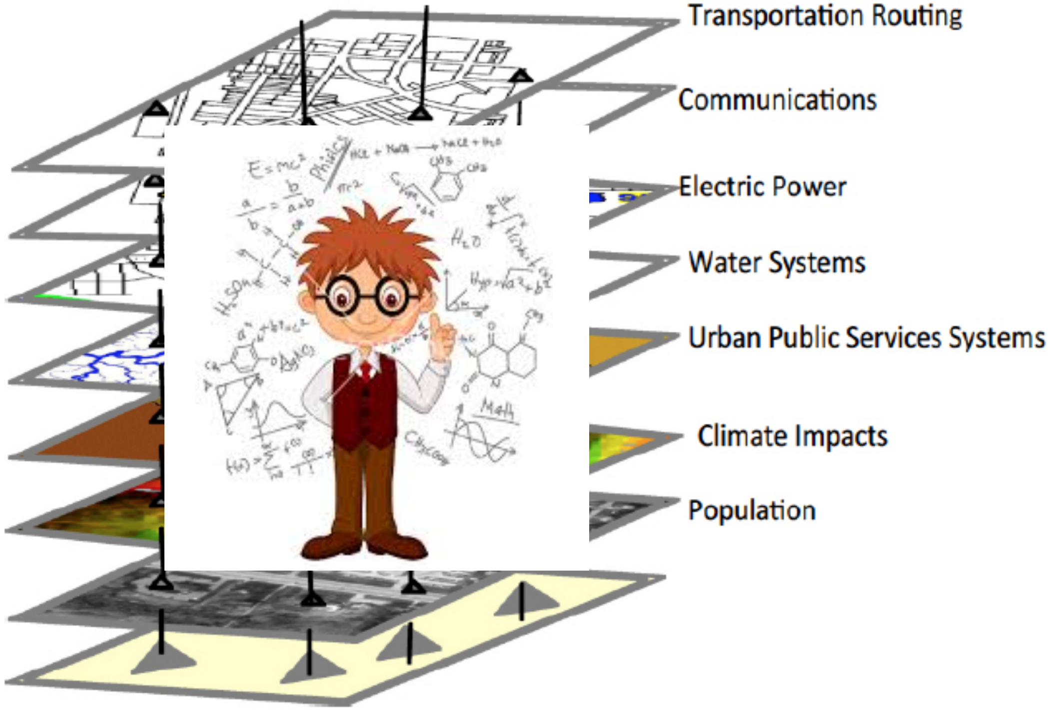


System of systems with…





…human in the middle



E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering and System Safety, 152, 2016.

Risk Assesssment and Management

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 million	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighboring 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 million	Two independent component failures (not covered by N-1 rule)
Sept 28, 2003	Italy	~30	up to 18	56 million	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs
July 12, 2004	Athens	~9	~3	5 million	Voltage collapse
May 25, 2005	Moscow	2.5	~4	4 million	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0.2	~3	200,000 passengers	Non-fulfillment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug 14, 2006	Tokyo	?	–5	0.8 million households	Damage of a main line due to construction work
Nov 4, 2006	Western Europe ("controlled" line cut off)	~14	~2	15 million households	High load flow D-NL, violation of the N-1 rule, poor inter TSO–coordination
Nov 10, 2009	Brazil, Paraguay	~14	~4	60 million	Short circuit on key power line due to bad weather, Itaipu hydro plant (18 GW) shut down

Italian Blackout, September 28, 2003

3:00 AM	Italy imports 6.9 GW, 25% of the country's total load, 300 MW **more than scheduled**
3:01	Trip of the 380 kV line Mettlen-Lavorgo (**highly loaded**) caused by **tree flashover**; overload of the adjacent 380 kV line Sils-Soazza
3:11	ETRANS (CH) informs GRTN (I): Request by phone to reduce the import by 300 MW (**not enough**)
3:21	GRTN reduces import by 300 MW
3:25	Trip of the Sils-Soazza line due to **tree flashover** (at 110% of its nominal capacity); the Italian grid loses its synchronism with the UCTE grid; almost **simultaneous tripping** of all the remaining connecting lines
3:27	Breakdown of the Italian system, which is not able to operate separately from the UCTE network (instabilities); **loss of supply**
9:40 PM	**Restoration** of the Italian system completed

Italian Blackout, September 28, 2003

Italian Blackout, September 28, 2003

Impact on Population - strong

- People affected: 56 Million
- Hundreds of people trapped in elevators.

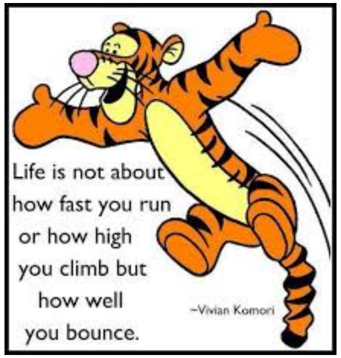
Economic Losses - moderate

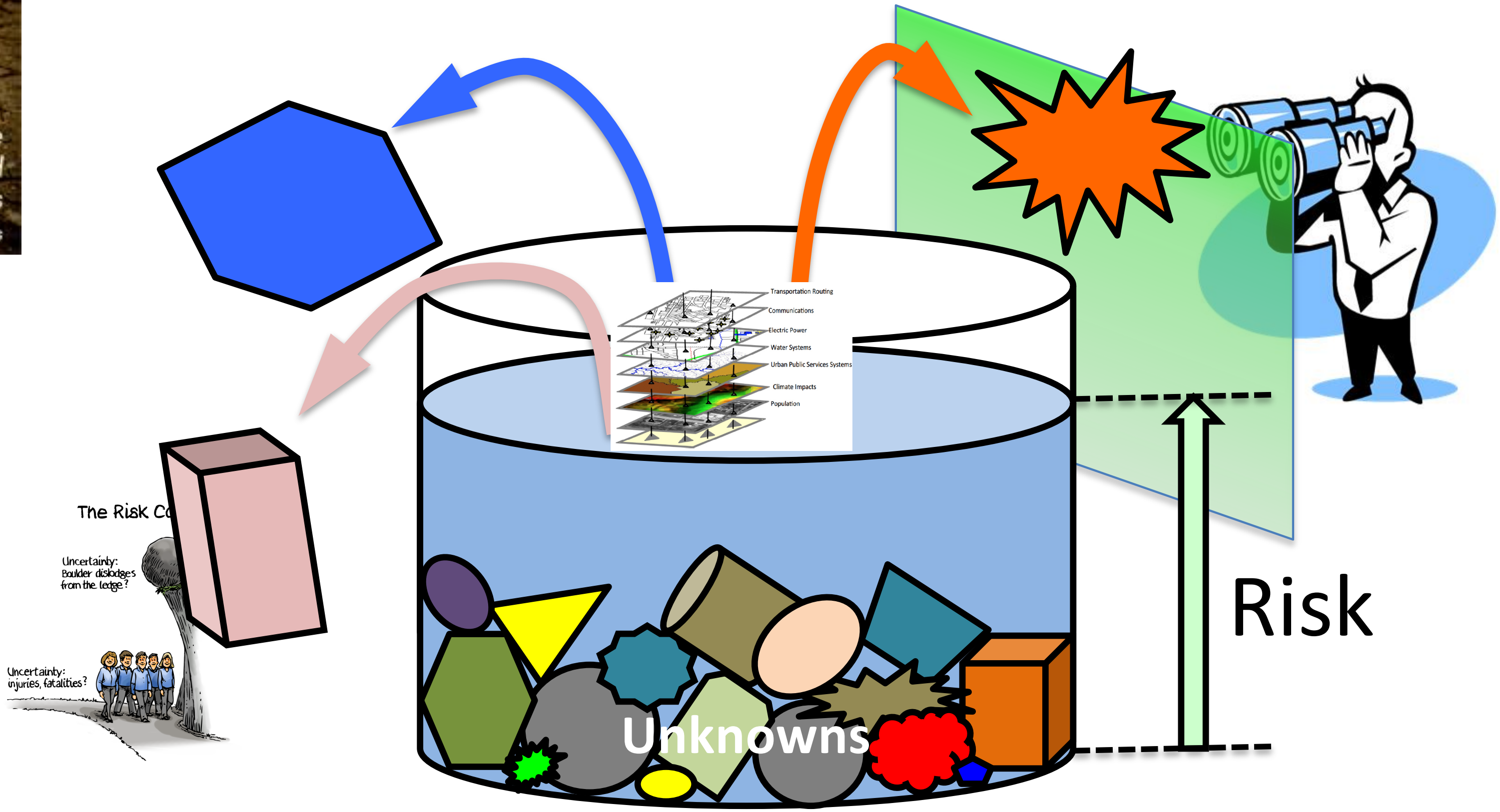
- About 120 million €
- Several hundred k € due to the interruption of continuously working industries.

Impact on Dependent Critical Infrastructures - varying

- Transportation: ~110 trains , 30'000 passengers, Subways in Rome and Milan. Flights cancelled or delayed. Outage of traffic lights partly led to chaotic situations in major cities, no severe accidents.
- Water supply: Interruptions for up to 12 hours.
- I & C: Telephone and mobile networks in a critical state. Internet providers shut down their servers (data transfer rate went down to 5% of normal).
- Hospitals: No serious problems due to the use of diesel-driven generators.

Risk Assessment and Management

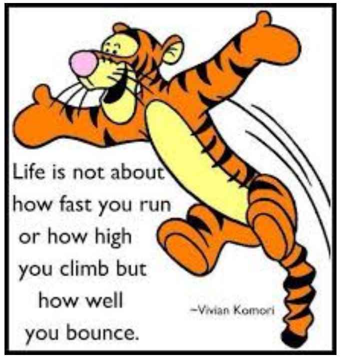


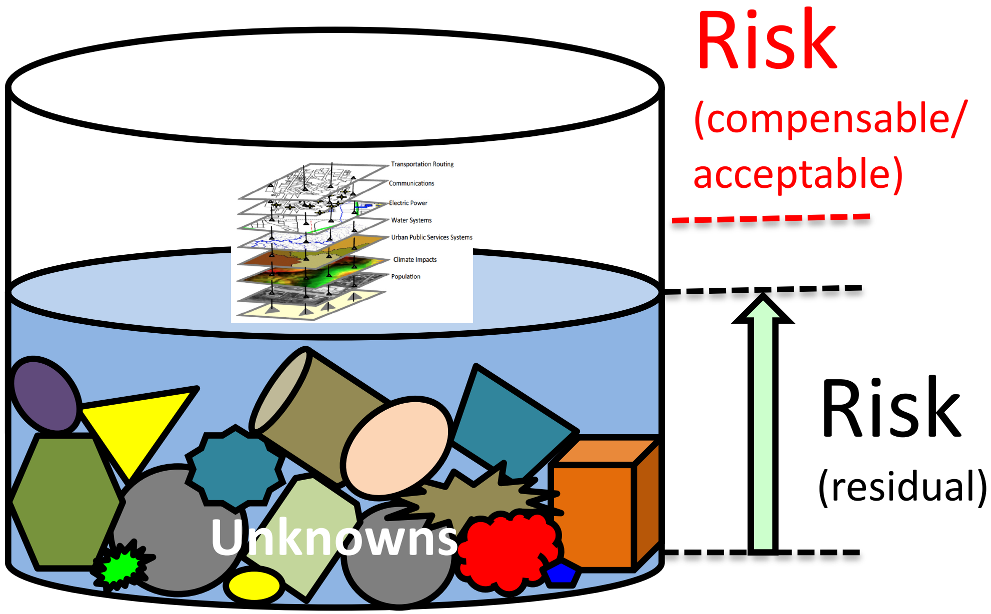


A. Yamaguchi, PSAM 12, 2016

T. Aven and E. Zio, Foundational Issues in Risk Assessment and Risk Management, Risk Analysis, Vol. 34(7), 2014

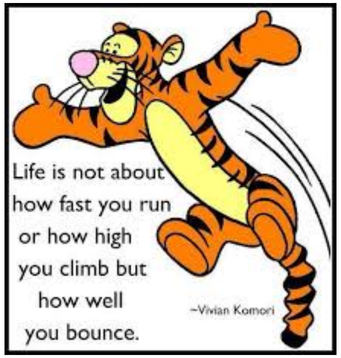
Risk Assessment and Management





A. Yamaguchi, PSAM 12, 2016

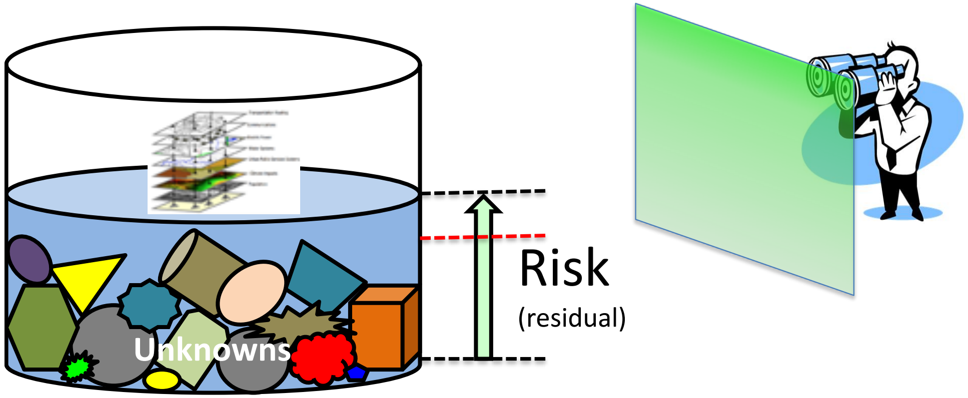
T. Aven and E. Zio, Foundational Issues in Risk Assessment and Risk Management, Risk Analysis, Vol. 34(7), 2014



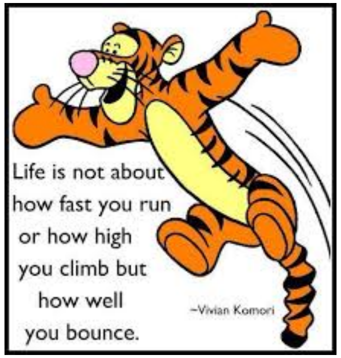
Modern societies:

Beck U., Living in the World Risk Society, Economy and Society, 2006

+ **to a large extent have succeeded in bringing under control (some) contingencies and uncertainties (with respect to accidents, violence and sickness…)**

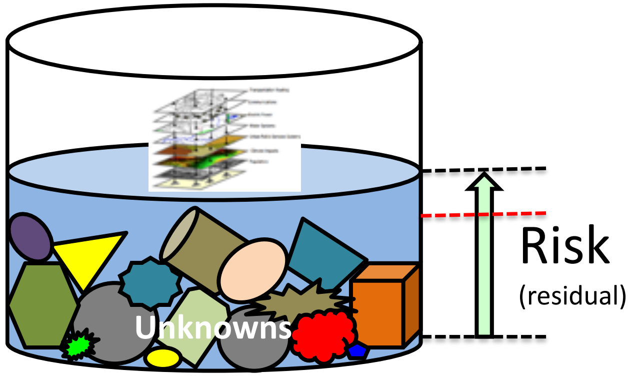


Risk Assessment and Management



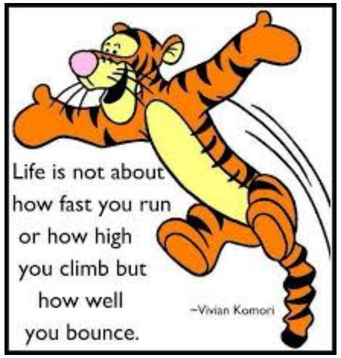
Modern (risk) societies: Beck U., Living in the World Risk Society, Economy and Society, 2006

+ to a large extent have succeeded in bringing under control contingencies and uncertainties (with respect to accidents, violence and sickness…) **but many events in the past 15 years have shown how limited is the claim to risk control by modern societies which**



are increasingly occupied with preventing and managing risks (mostly self-produced by technology and social innovation → complexity and globalization)

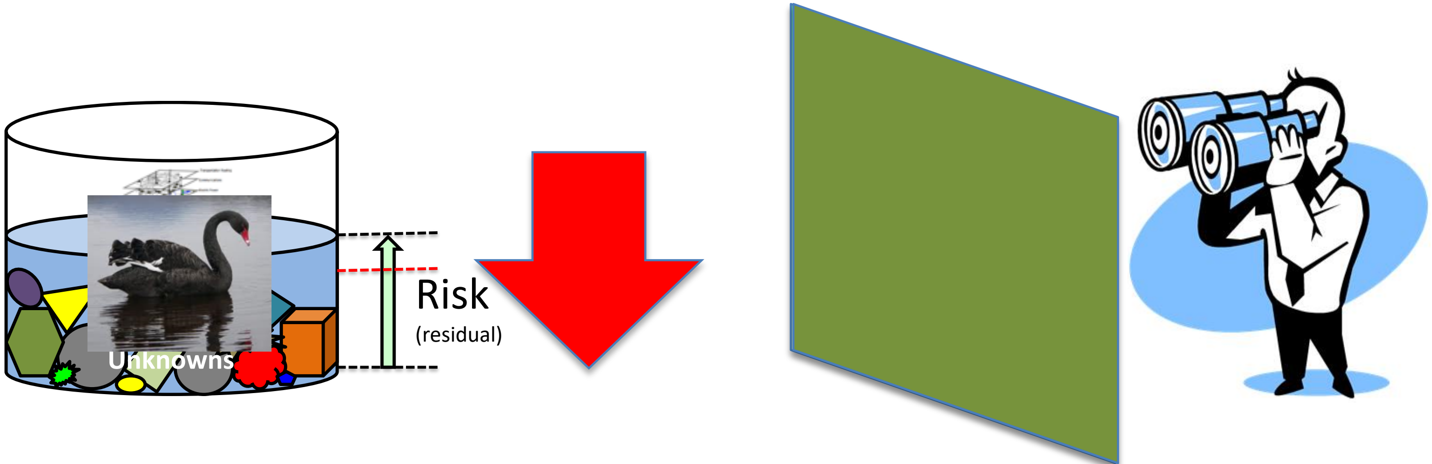
Risk Assessment and Management



Beck U., Living in the World Risk Society, Economy and Society, 2006

Modern (risk) societies:

- **have to take risk management decisions on the basis of more or less unadmitted not-knowing**



- **risk calculation based on experience (accident analysis) and rationality breaks down**
- **we don't know what it is that we don't know (unknown unknowns)…and from this… dangers arise**

Cross-border hazards

S. Menoni et al., Cross-border implications of critical infrastructures failures: assessment and management

Criteria to define cross-border	Explanation
Impact based	The failure in one asset in one country may impact the same system in other countries, with consequences that can be more or less extended depending on several protective measures, including redundancy and possibility to switch to other service providers
Hazard based	Cross-border triggering hazard affecting potentially wide regions: flood across countries, storm & snowstorm, very intense precipitation, strong winds, hailstorm), forest fires, earthquakes
Systemic Vulnerability based	Dependencies that are regional or even global ones as in the case of civil aviation or when supply occur at a global scale

Interconnected systems and cross-border hazards

S. Menoni et al., Cross-border implications of critical infrastructures failures: assessment and management

Date of occurrence	Infrastructure(s) involved	Countries involved	Initial triggering hazard/threat and initial conditions	Direct damage and failure to CI
1981- 2011	Transport system; Dam System and Hydroelectric Plant	France, Italy	Floods, landslides, avalanche's, flows (of mud and debris), collapses (falling of blocks)	Scenario of total or partial interruption of the road. Loss of functionality; Scenario of the dam structural collapse; Water and electricity supply lines
2002	Transport system	Germany, Czech Republic, Austria and Poland	Elbe river flood	Railway line
14 August 2003	Power System	North America	Tree flashovers; High temperature and load level; generators and 5 capacitor banks out of service	Water supply, Transportation, Communication, Hospitals
August 2003	Transport system	France, Portugal, the Netherlands, Spain, Italy, Germany, the United Kingdom, Switzerland, Ireland, Sweden	Heat wave	Rails buckling; Degradation of signalling systems of railway system; Deformations of road surfaces; Break of London underground trains
23 September 2003	Power System	Scandinavian Countries	5 transmission lines and 4 generation units out of service before the incident	Water supply, Transportation, Communication, Hospitals

Interconnected systems and cross-border hazards

S. Menoni et al., Cross-border implications of critical infrastructures failures: assessment and management

Date of occurrence	Infrastructure(s) involved	Countries involved	Initial triggering hazard/threat and initial conditions	Direct damage and failure to CI
28 September 2003	Power System	Italy and Switzerland	Tree flashovers; High power transfers toward Italy	Tripped power lines by trees flashover, high voltage line damaged. Water supply Hospitals, Transportation, Communication
2004	Gas pipeline	Belgium and France	-	Leakage and explosion
2006, 2007–2008 (2010, … 2018)	Power system; Wide areas of farmland, Bridges	Bulgaria, Turkey and Greece	Maritsa river flood	Supply interruption, connection interruption; Reduced dam reservoir levels; hydroelectric power generation loss; agricultural land loss
4 November 2006	Power System	Europe	Planned disconnection; System operation close to its limits	Water supply, Transportation, Communication, Hospitals
2006	Transport system	Austria, Czech Republic, Slovakia	Morava river flood, Danube river flood	Railway line. In Austria 3 dikes broke. The main line from Vienna to Prague and some roads were damaged or destroyed. In Slovakia, damage to municipal properties (including public roads damaged by heavy traffic during emergency operations as well as damage to facilities such as ports and ferries). In the capital Budapest, 39 public properties (buildings, roads and defence structures) were

Interconnected systems and cross-border hazards

S. Menoni et al., Cross-border implications of critical infrastructures failures: assessment and management

Date of occurrence	Infrastructure(s) involved	Countries involved	Initial triggering hazard/threat and initial conditions	Direct damage and failure to CI
17-19 January 2007	Transport system	the United Kingdom, Norway, Ireland, France, Belgium, the Netherlands, Sweden, Austria, Germany, Czech Republic, Denmark, Slovakia, Slovenia, Switzerland, Poland	Winter storm	Abandonment of the container ship MSC Napoli in the English Channel; Roof damage of the railway stations in London and Amsterdam; Structural damage of the railway station in Berlin; Fall of trees onto rail tracks.
2007	Oil pipeline	Switzerland, France, Germany	-	Break in a liquid hydro-carbon pipeline
20 March 2010	Transport system	33 European Countries	Eruption of the Eyjafjallajökull volcano (Iceland)	-
8 August 2011	Power System	Arizona, California and Mexico	High temperature and load level; Some generation and transmission maintenance outages.	Water supply, Transportation, Communication, Hospitals
June 2013	Transport system	Austria, Bulgaria, Croatia, Germany, Hungary, Romania, Serbia, Slovakia	Danube river floods	Damage of roads and bridges were damaged

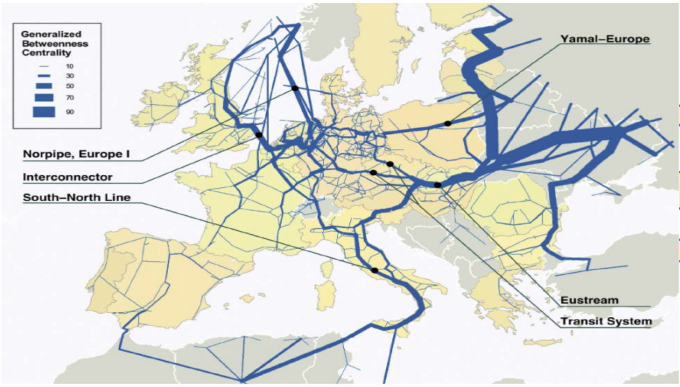
Interconnected systems and cross-border hazards

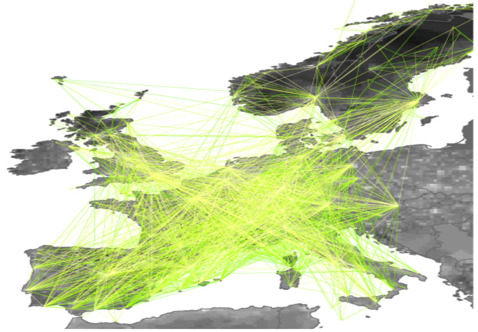
S. Menoni et al., Cross-border implications of critical infrastructures failures: assessment and management

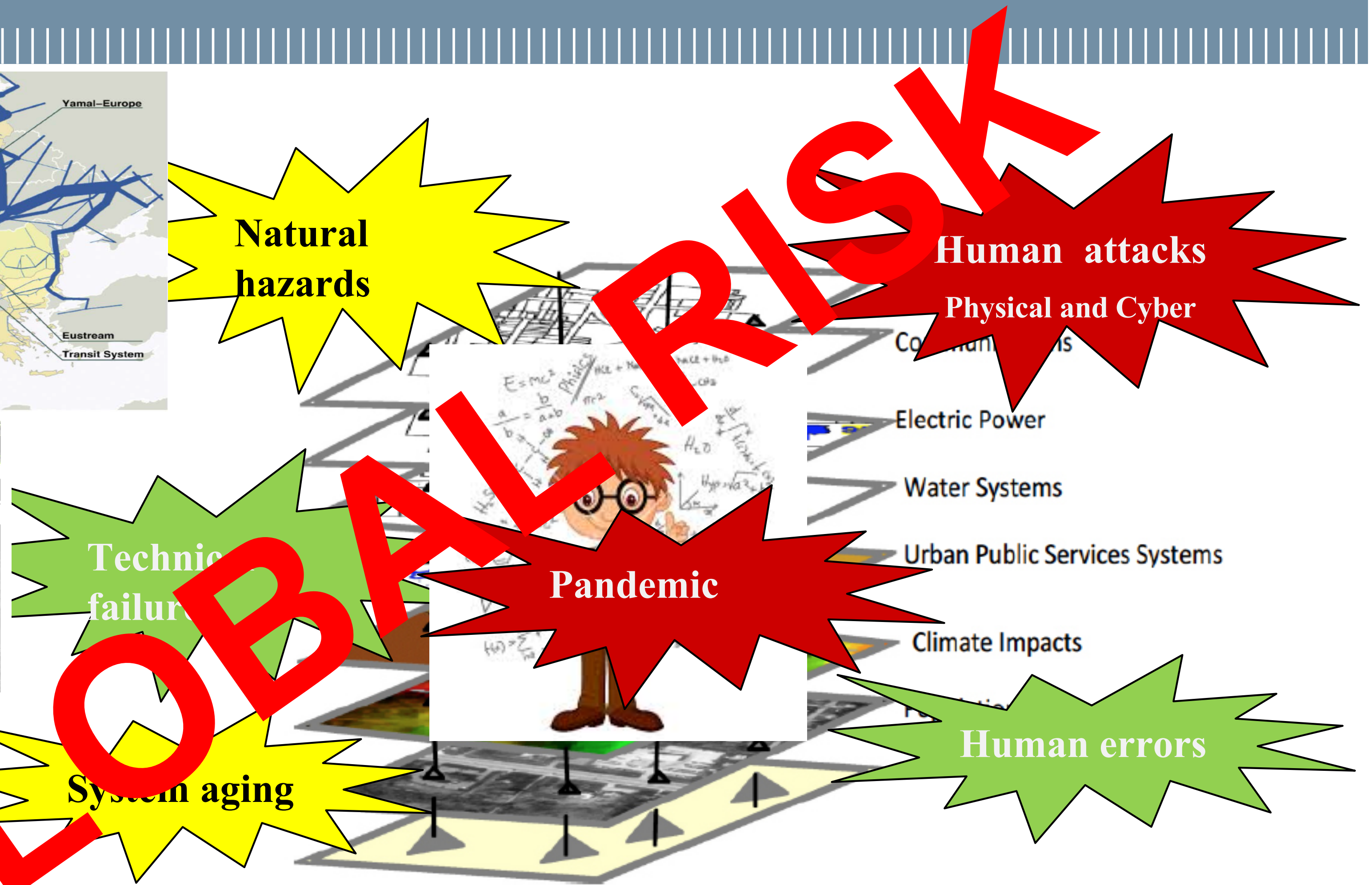
Date of occurrence	Infrastructure(s) involved	Countries involved	Initial triggering hazard/threat and initial conditions	Direct damage and failure to CI
28 October 2013	Transport system	Germany, the United Kingdom, the Netherlands, Denmark, France, Sweden, Estonia, Russia	Cyclone/Storm	Lost of several shipping containers; Roof damage of the railway stations in Denmark; Fallen trees and damage to the catenary of tram services in South Holland; in London, Tube lines were affected on account of debris on the tracks
January 2019	Transport system	Germany, Austria, Switzerland, Italy, Poland, Czech Republic, Greece	Winter storm	Many snow-related accidents; Hundreds of trees broke down; A French fighter jet disappeared from radar screens
16 June 2019	Power System	Argentina and Uruguay	To be investigated	Water supply, Transportation, Communication, Hospitals
September 2019	Water, Power and Transport… Systems	Bahamas, USA	Hurricane Dorian	
…				

Global Risk

World Risk Society: global risk



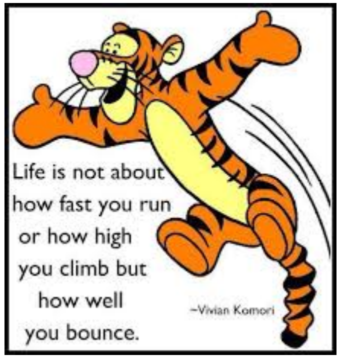




E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, Reliability Engineering and System Safety, 152, 2016.

Aven, T and Zio, E, 2020, "Globalization and global risk: How risk analysis needs to be enhanced to be effective in confronting current threats, Reliability Engineering and System Safety

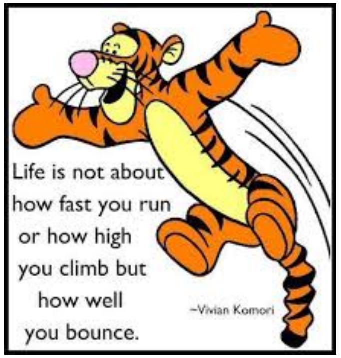
World Risk Society: Global risk



- **Global risk is the human condition in the 21st century**
- **Global risks are expression of global interdependence**
- **Global risks tear down national boundaries**
- **Global risks represent a shock for humanity (no one predicted such a development)**

Beck U., Living in the World Risk Society, Economy and Society, 2006

World Risk Society: Global risk



- **Global risk is characterized by :**

1. **De-localization: causes and consequences are not local**

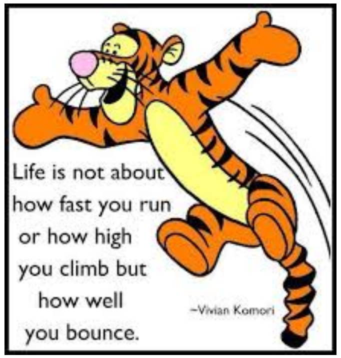
   de-localization of incalculable interdependency risk?

2. **Incalculableness: consequences are incalculable (and often probabilities too)**

   'hypothetical' risk

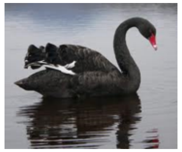
Beck U., Living in the World Risk Society, Economy and Society, 2006

World Risk Society: Global risk



3. Non-compensability: as long as accidents are compensable, acceptable risk can be defined, but

with unknown unknowns, the logic of compensation breaks down



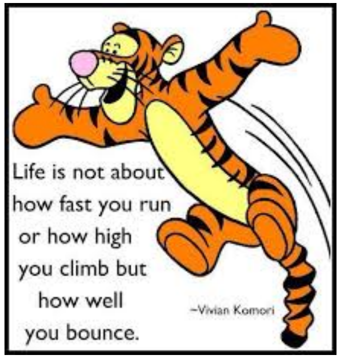
principle of precaution

+

resilience: anticipate, prevent, mitigate, recover from risks (some whose existence has not been proven)

Beck U., Living in the World Risk Society, Economy and Society, 2006

From risk prevention/mitigation to resilience



Risk analysis

1) What can happen? (***accident, A***)
2) How likely will it happen? (***uncertain occurrence, U***)
3) If it does happen, how bad will it be? (***uncertain consequence, C***)

Bad things have happened (and will happen again)

↓

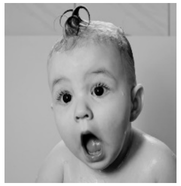
What bad things? **Hazards and Threats**

↓

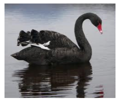
How likely? How bad? **Risk assessment**

↓

Prepare, mitigate **Risk management**



Surprise!!!

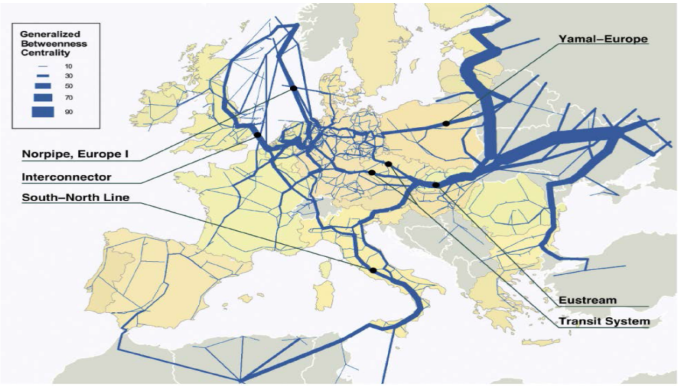


In addition to preparation…respond adaptively…
Make the system resilient!

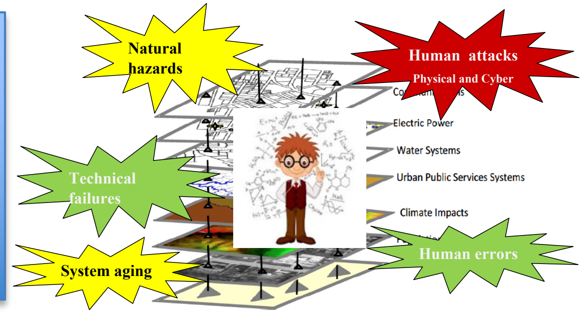
There will always be unforeseen events (due to the complexity of our systems) and, thus, means must be put in place to adequately respond to such events when they occur

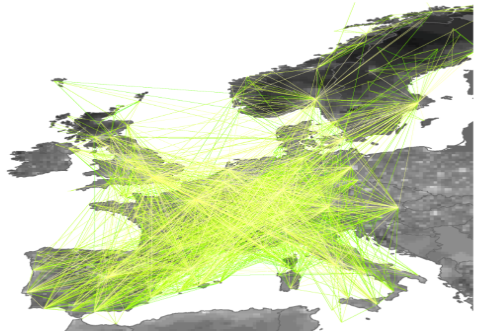
Zio, E., 2018. The future of risk assessment. Reliability Engineering & System Safety, 177, pp.176-190.

World Risk Society: Global risk

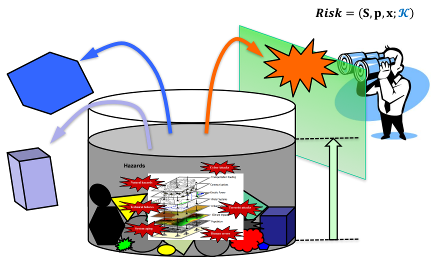


World Risk Society



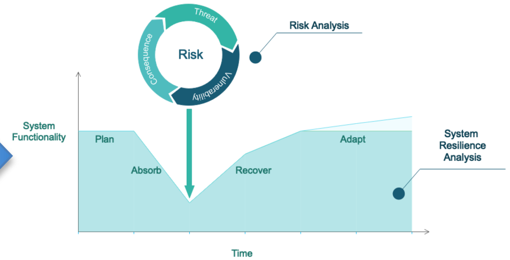


?



Surprise

Resilience

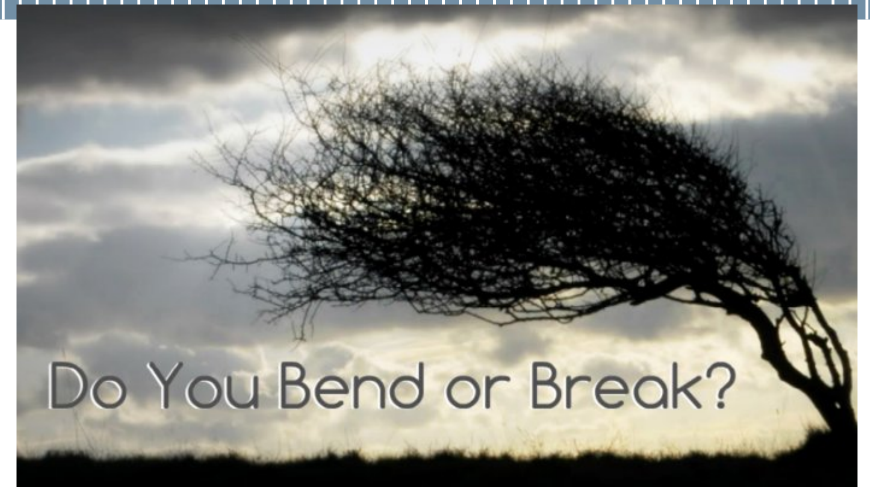


T. Aven and E. Zio, "Some Consideration on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making", Reliability Engineering and System Safety, Vol. 96,. 2011, pp. 64-74, 2011.

Resilience

Resilience


RESILIENCE
I AM STRONG.
I AM A SUPERHERO.
I AM ME!


Do You Bend or Break?


KEEP
CALM
AND
HAVE
RESILIENCE

What is system resilience?

The sum of the passive survival rate (**reliability**) and proactive survival rate (**restoration**) of a system, (Youn et al. 2011)

"Intrinsic ability of a system to **adjust** its functionality in the presence of a disturbance and unpredicted changes" (Hollnagel et al. 2006)

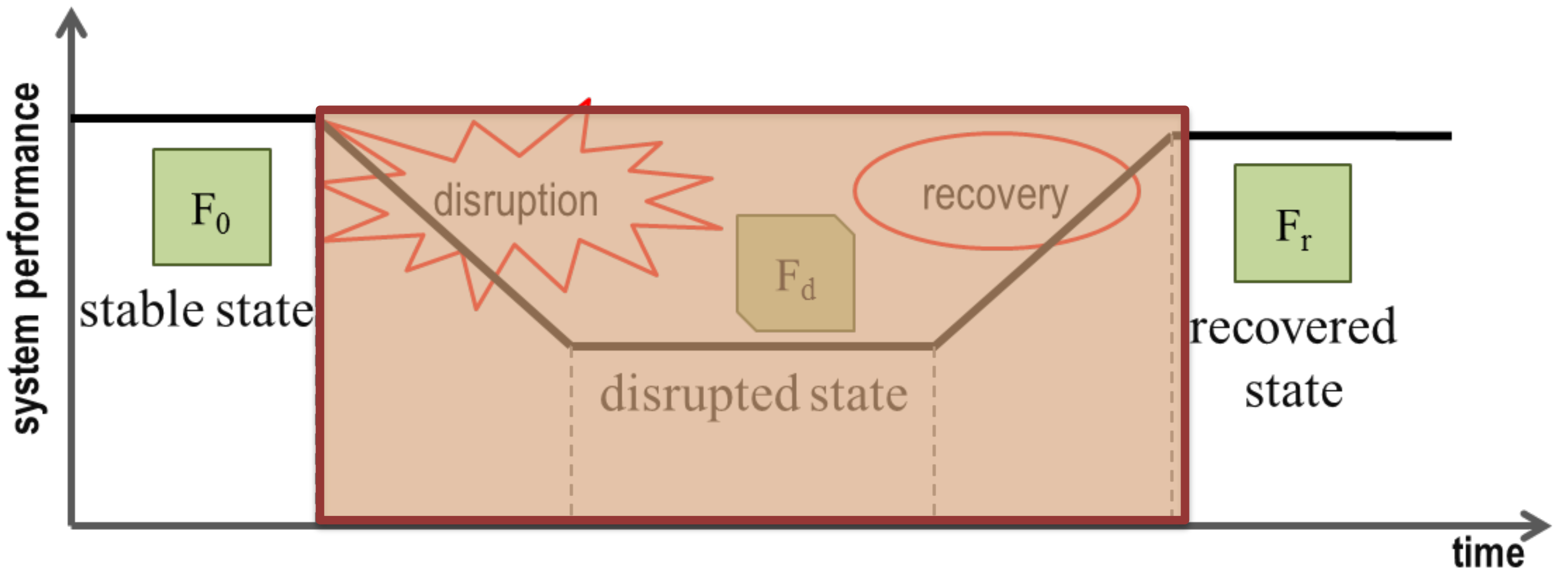
"The ability of a system to **sustain** external and internal **disruptions** without discontinuity of performing the system's function or, if the function is disconnected, to fully **recover** the function rapidly" (US ASME 2009)

"The resilience of infrastructure systems is their ability to **prevent**, **absorb**, **adapt**, and/or quickly **recover** from a disruptive event such as natural disasters" (US National Infrastructure Advisory Council NIAC, 2009)

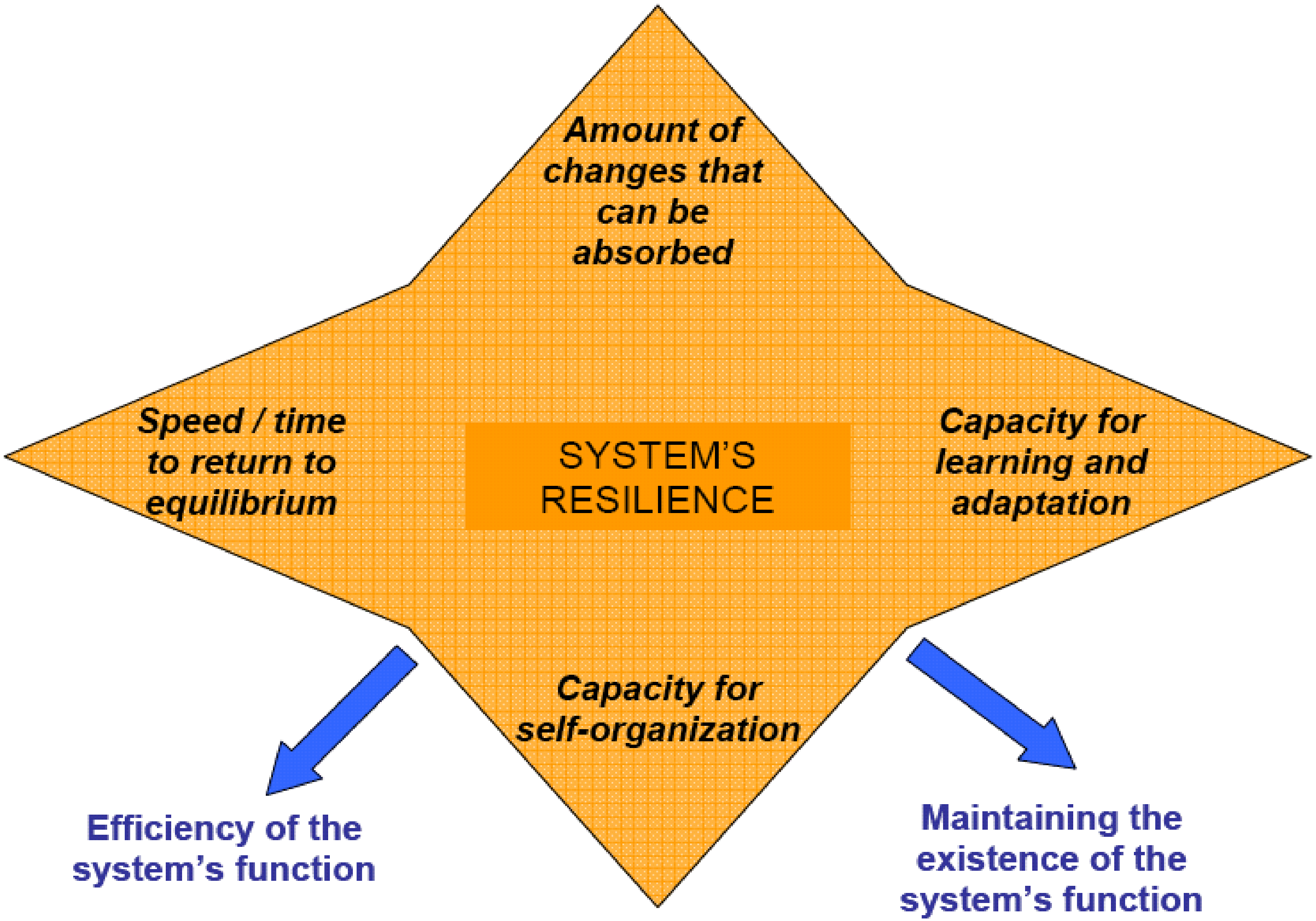
…

What is system resilience?

- **Resilience**: focus on the ability of a system to "**absorb**" and "**adapt**" to **disruptive events**, and "**recovery**" is considered as the critical part of resilience
- It considers the **whole response dynamics** of a system to any kind of disruptions



Features of system's resilience



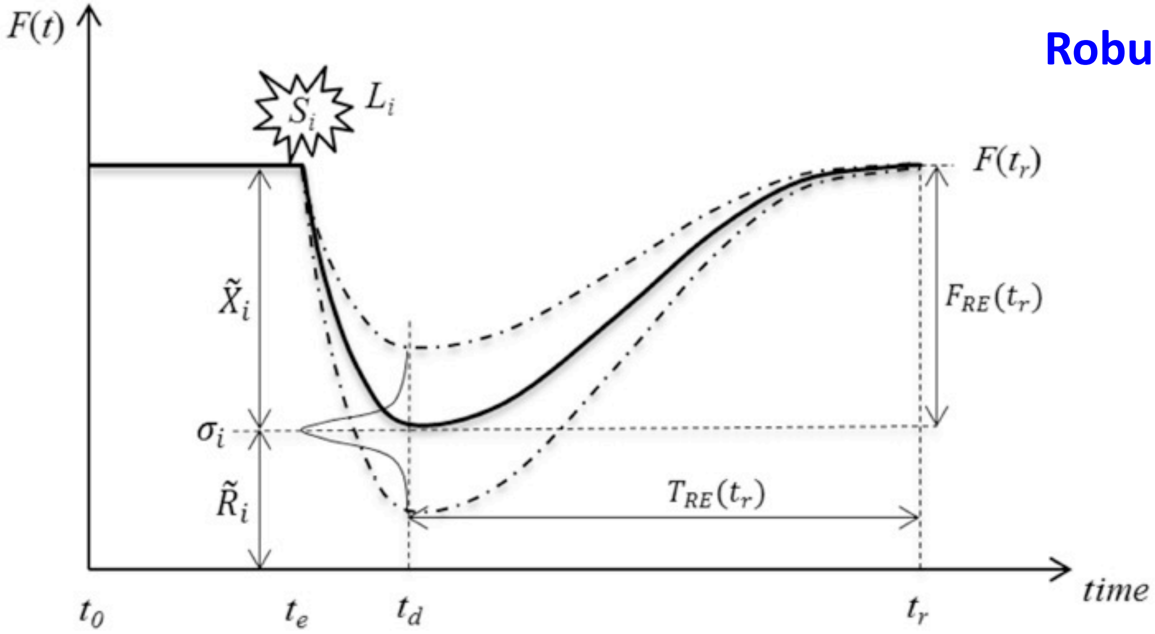
What is system resilience?

Risk = $\{\langle S_i, L_i, \tilde{X}_i(\sigma_i)\rangle\}$

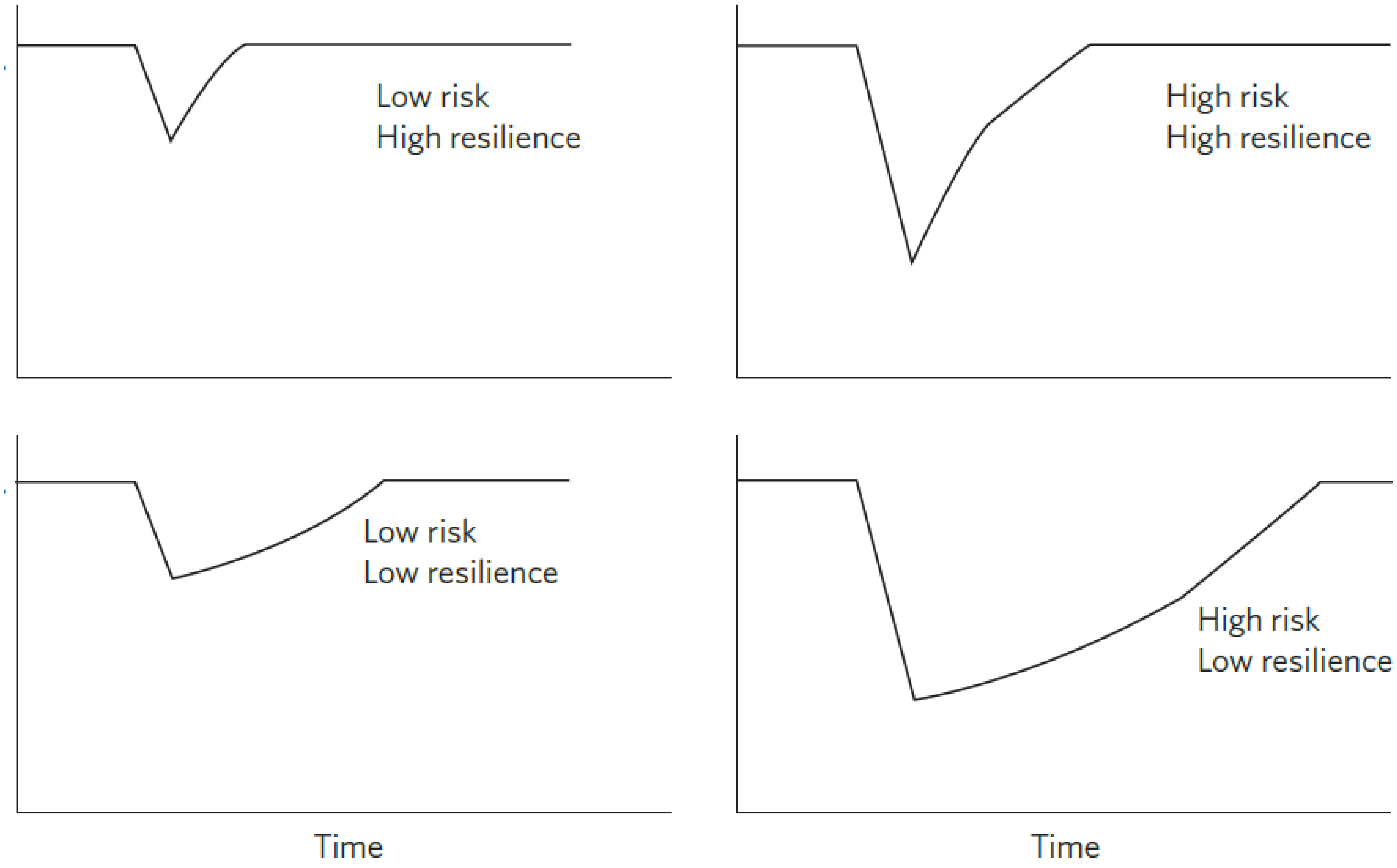
Robustness = $\{\langle \widetilde{R}_i \rangle\} = \{\langle F(t_0) - \tilde{X}_i(\sigma_i)\rangle\}$

Resilience = $\{\langle S_i, L_i, \widetilde{R}_i, T_{RE}(t_r), F_{RE}(t_r)\rangle\}$

Robustness **Recovery** **Rapidity**



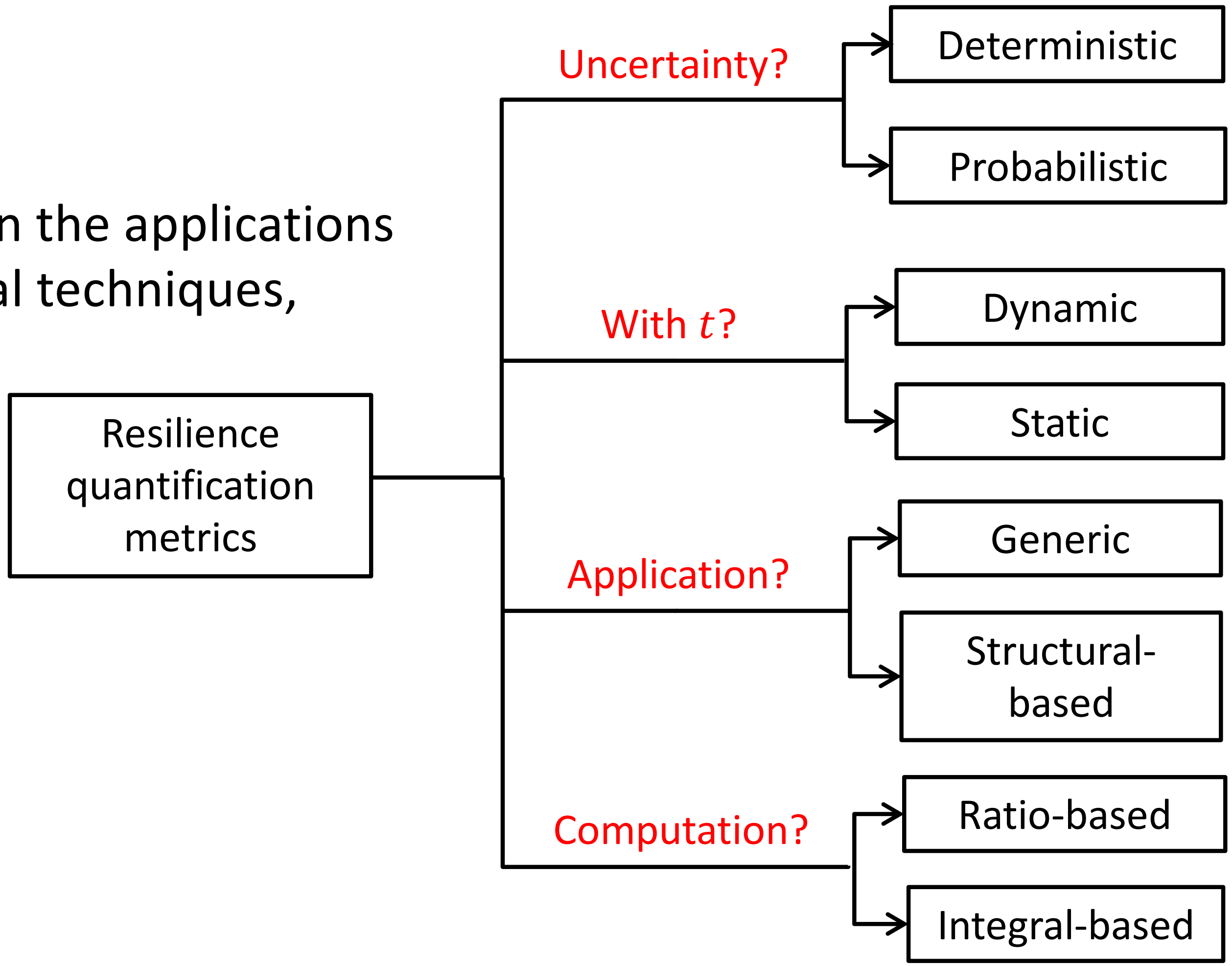
Resilience vs. risk



CI resilience quantification and assessment

Resilience metrics

- Classification: depends on the applications of interest, computational techniques, available data, etc.

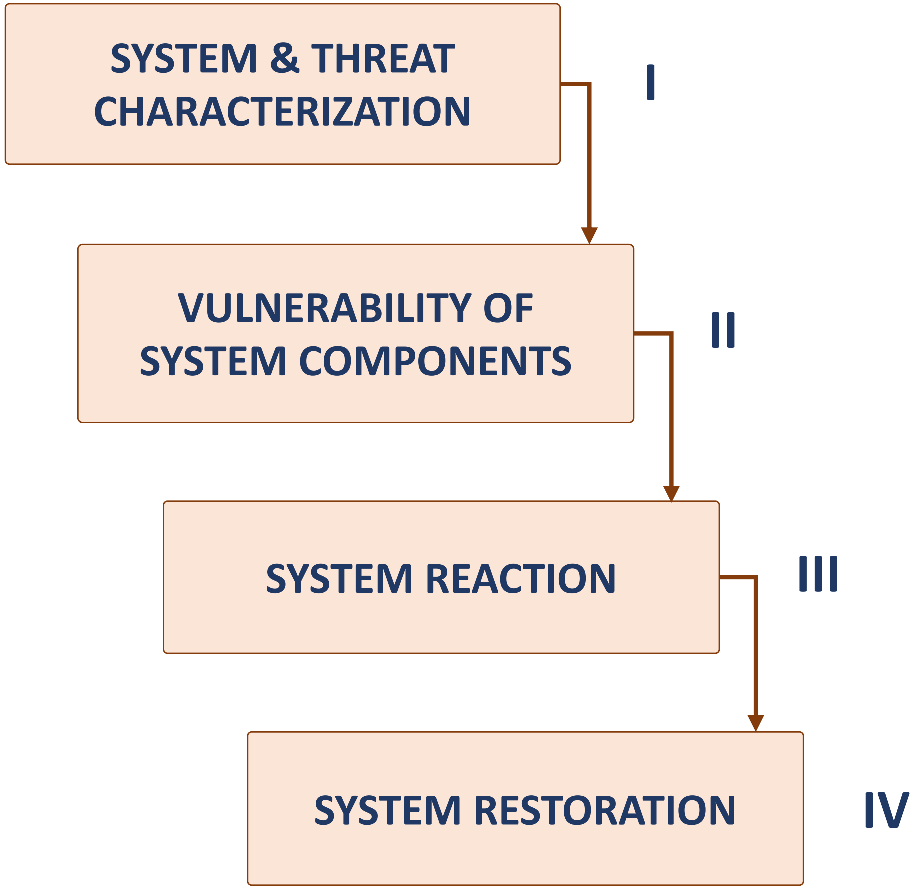


Resilience assessment framework

Resilience assessment

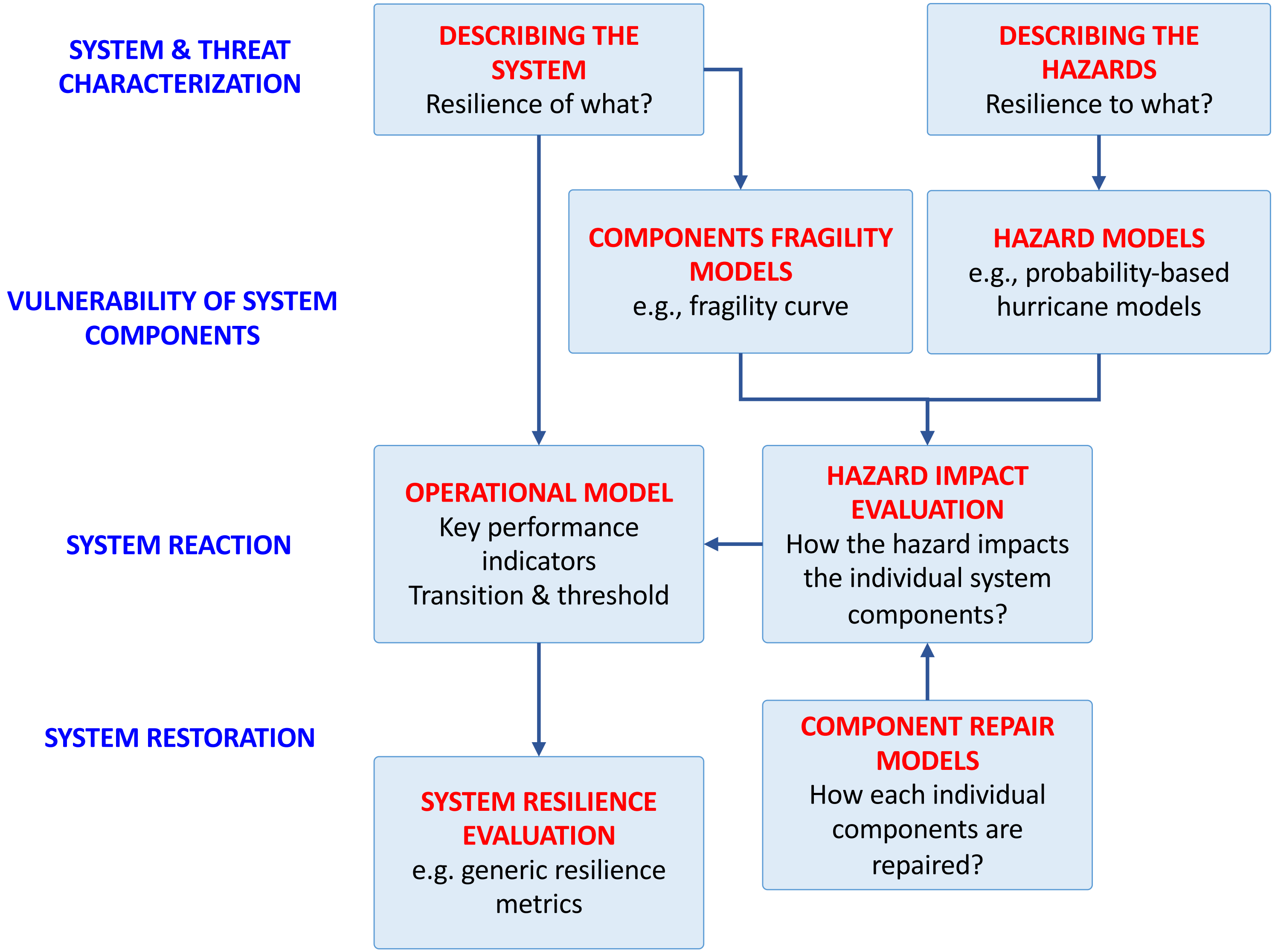
Simulation-based resilience assessment framework

- **Objective**: to evaluate the resilience of a system against specific hazards with computational methods
- Hazards are able to be modeled explicitly, e.g. hurricanes, via physical/parametric models



Resilience assessment

A threat(hazard)-based assessment framework: the flow chart

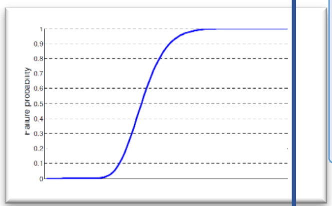


Resilience assessment

Example: power transmission system resilience under hurricanes

DESCRIBING THE SYSTEM
Resilience of what?

DESCRIBING THE HAZARDS
Resilience to what?



COMPONENTS FRAGILITY MODELS
e.g., fragility curve

HAZARD MODELS
e.g., physical hurricane models

- AC power flow model
- P(t) = Total energy unsupplied

OPERATIONAL MODEL
Key performance indicators
Transition & threshold

HAZARD IMPACT EVALUTION
How the hazard impacts the individual system components?
Monte Carlo simulation

- Operation states of transmission lines, substations, power generators, etc. at each time periods

- Computing resilience metrics
- Comparison under different scenarios

SYSTEM RESILEINCE EVALUTION
e.g. generic resilience metrics

COMPONENT REPAIR MODELS
How each individual components are repaired?

- Probability distribution of the restoration time

$$T_i = F(level\ of\ damage, resource)$$

System Resilience Assessment, Analysis and Optimization

- *Functional modelling*
- *Quantification*
- *Optimization/ decision making*

CIs modelling

- *How to describe resilient behaviour of CI systems?*

Resilience assessment

- *How to assess resilience?*

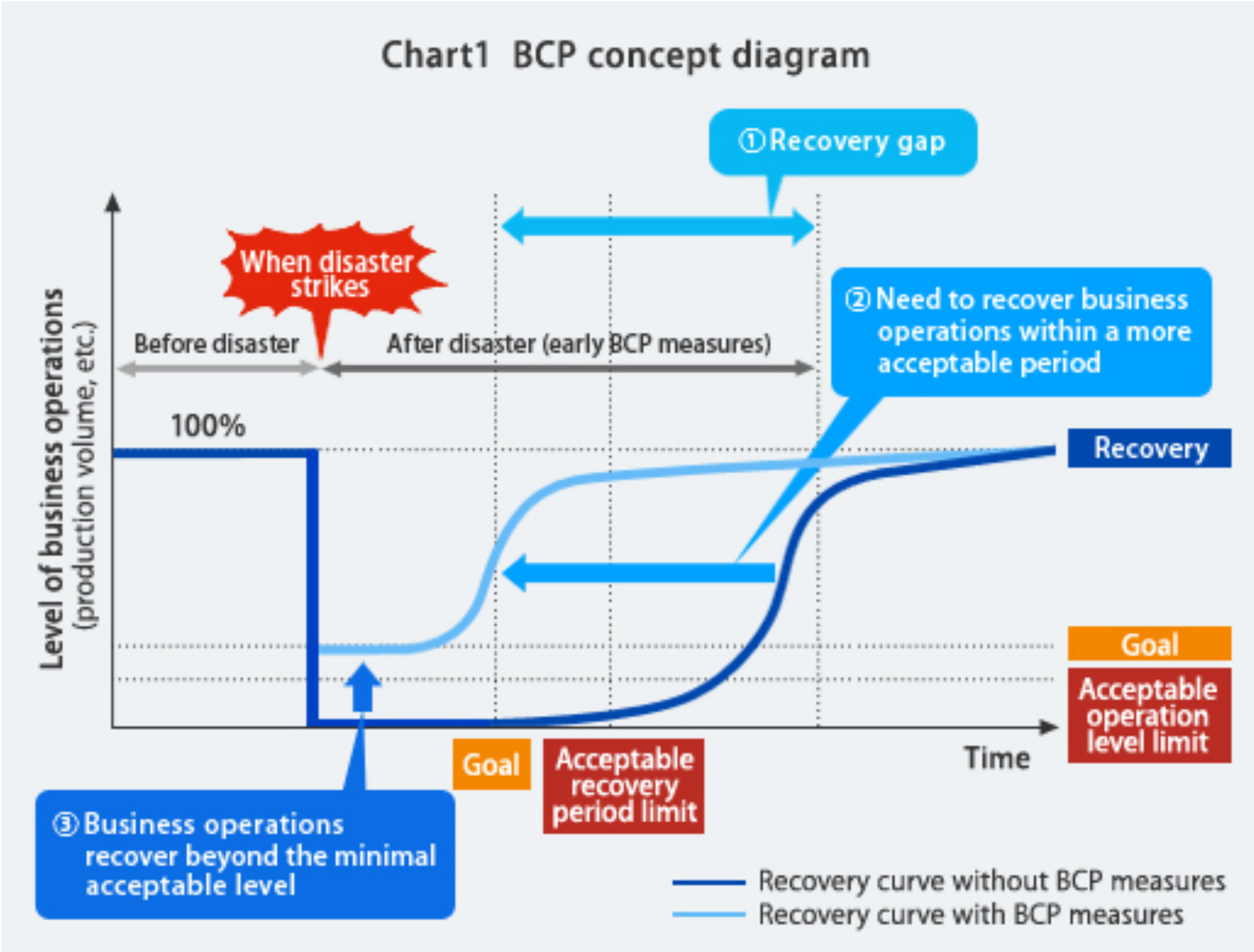
Resilience analysis

- *What affects resilience the most and the least?*

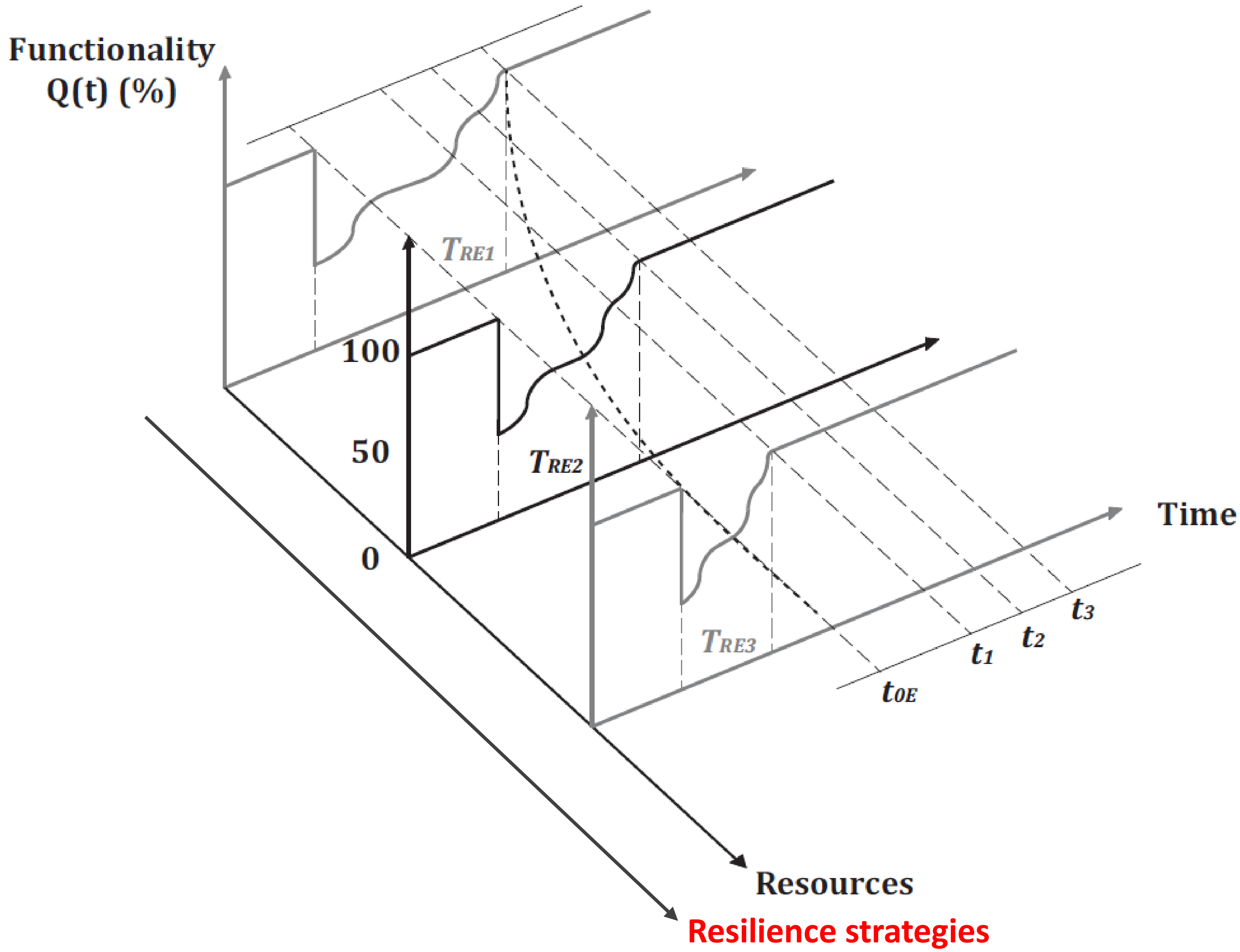
Resilience optimization

- *How to improve resilience?*

Resilience improvement



Resilience-oriented decision making

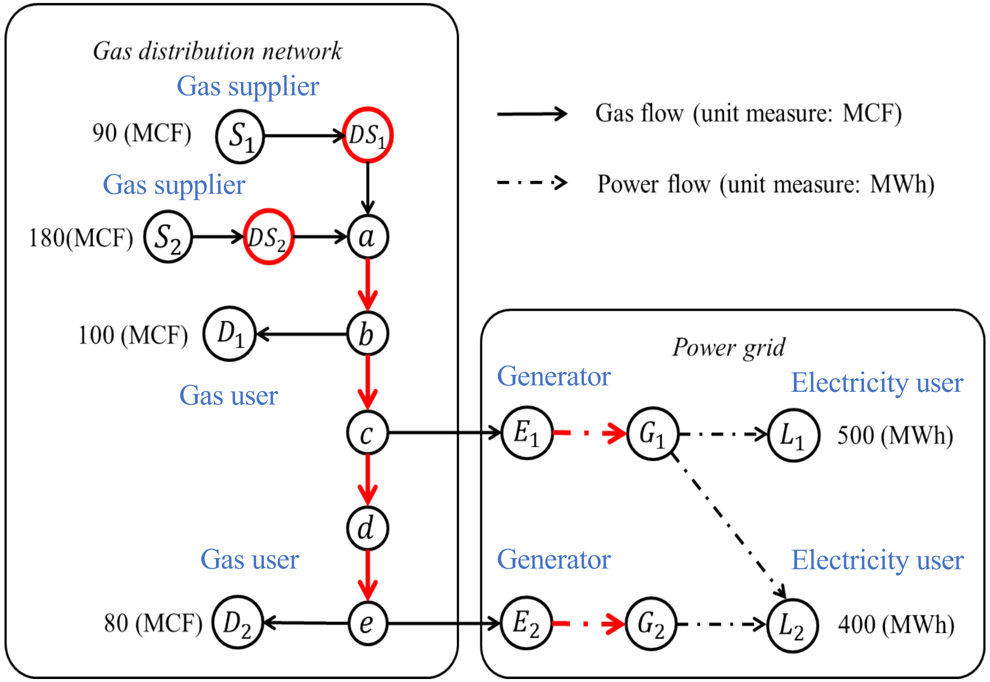


Resilience strategies

- To enhance resilience, **resilience strategies** include:
  - → Enhance the resilience awareness
  - → Share information
  - → Make integrated decision makings
  - → Train staff and managers
  - → Harden system components
  - → Adjust system topology
  - → Control system demand level
  - → Deploy backup systems (redundancy)
  - → Optimize repair sequence
- Resilience strategies are **system specific**
- Generally, in the time domain: **pre-event strategies** vs. **post-event strategies**, e.g., hardening vs. repair crew scheduling

Resilience-oriented decision making

Case study: Interconnected water supply and electric power systems



Most relevant system parameters obtained by *SADIM 1*

↓

1	Identify and predict potential hazards	F_3, F_7, F_2, F_4, H_r
2	Improve the efficiency of failure detection	H_r
3	Identify and improve maintenance of key elements	F_3, F_7, F_2, F_4
4	Design redundancy for link L_{a-b}	F_3
5	Design redundancy for link $L_{E_1-G_1}$	F_7
6	Design redundancy for buffer DS_2	F_2
7	Design redundancy for link L_{b-c}	F_4
8	Staff training	$F_3, F_7, F_2, F_4, H_r, \mu_3$
9	Establish efficient communication channels for operators	H_r, μ_3
10	Emergency education for users	H_h
11	Improve repair efficiency for link L_{a-b}	μ_3

Resilience-oriented decision making

Decision variables

The resilience enhancement activities i_v.

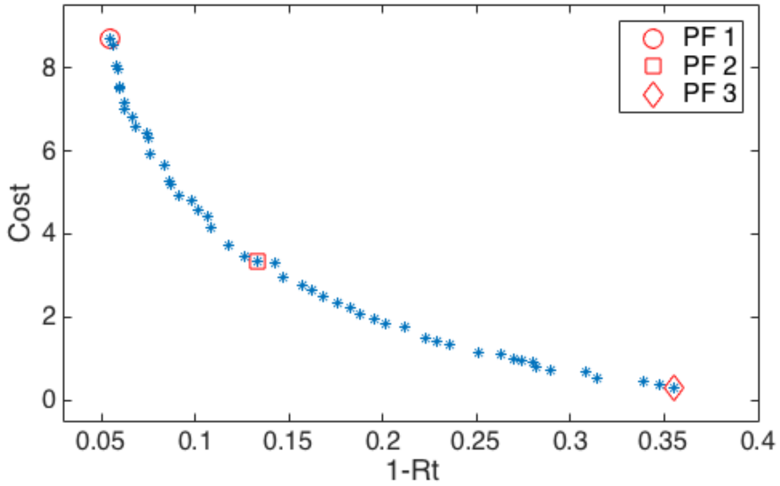
Objective functions

$$f_1 = 1 - R_t = 1 - \frac{\int_{t_f}^{t_h} \sum_{i_y}^{i_y = N_y} \omega_{i_y} y_{i_y}(t)\ dt}{\int_{t_f}^{t_h} \sum_{i_y}^{i_y = N_y} \omega_{i_y} D_{i_y}(t)\ dt}$$

$$f_2 = Cost = \sum_{v_i} c_{v_i}^{s}$$

Resilience-oriented decision making

Pareto Front



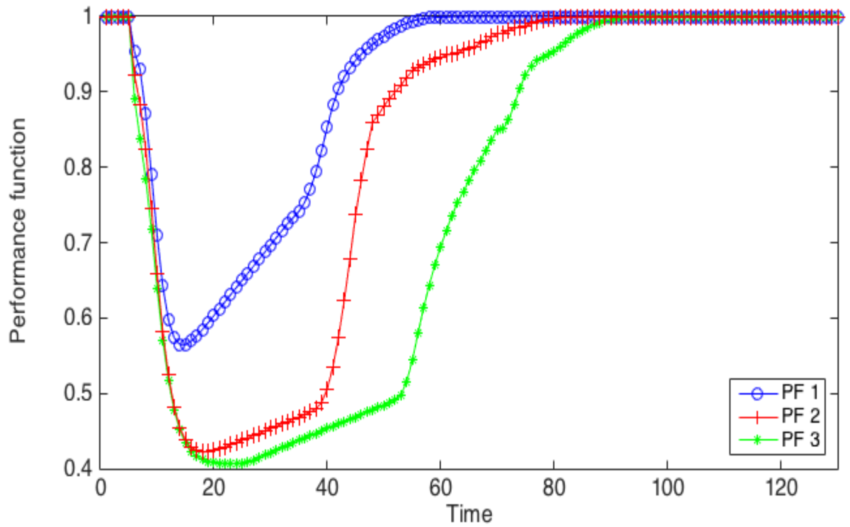
Three optimal values

- PF 1: minimum value of $f_1 = 1 - R_t$ and the maximum value of $f_2 = Cost$;
- PF 2: the best compromise solution obtained using the min-max approach to compromise between resilience and cost;
- PF 3: the maximum value of $f_1 = 1 - R_t$ the minimum value of $f_2 = Cost$.

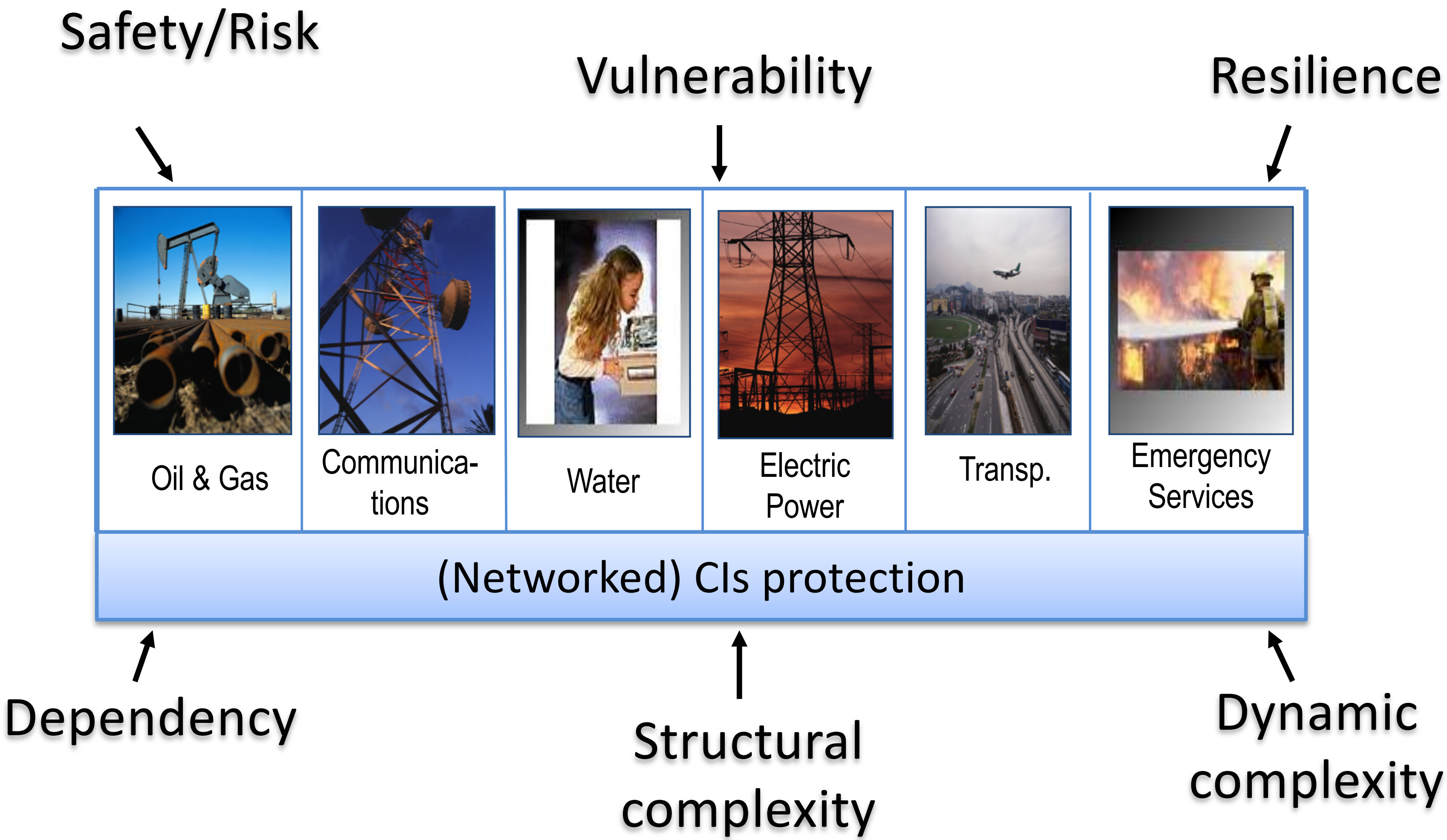
Resilience-oriented decision making

Optimal investment of RES activities

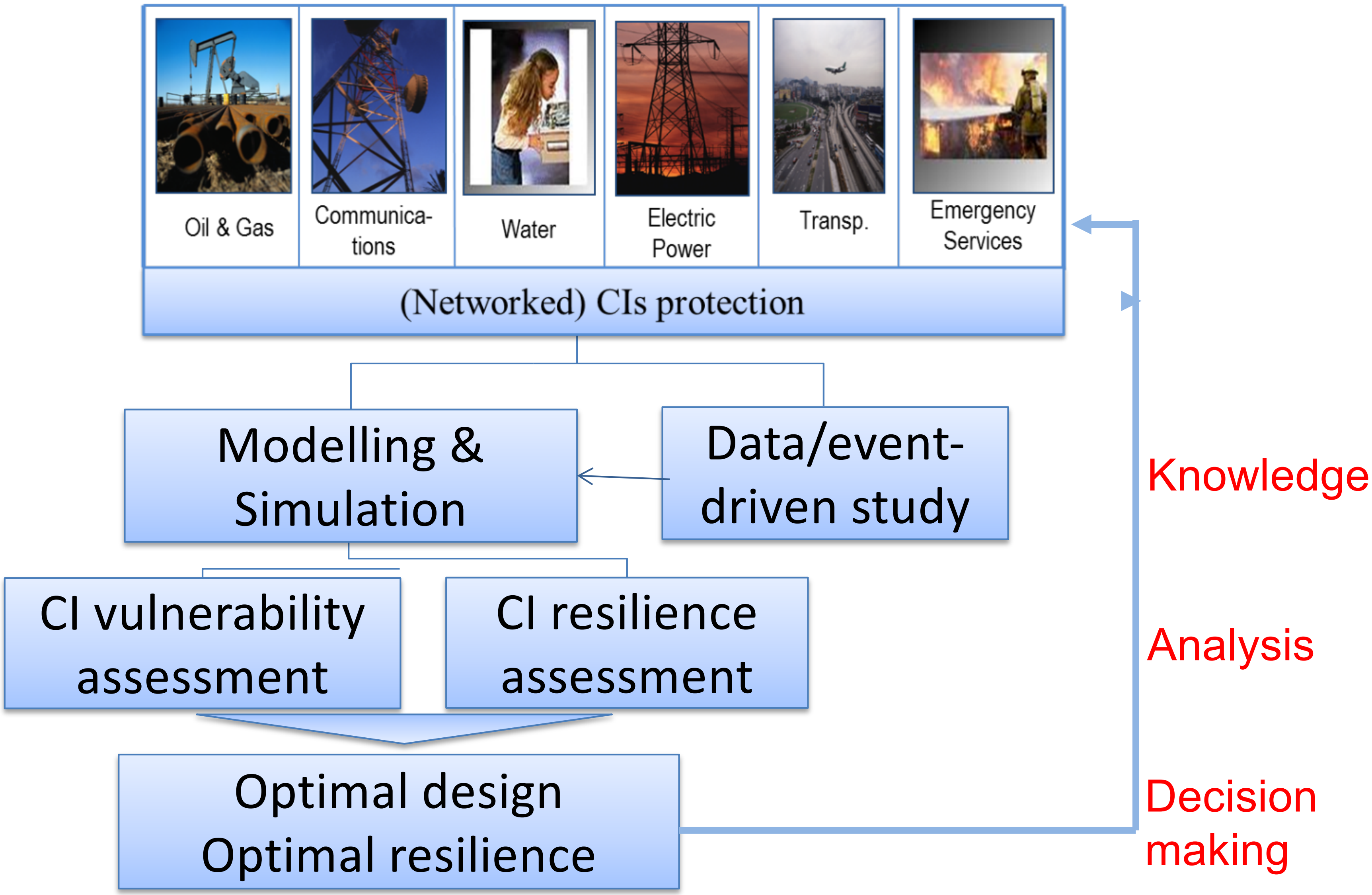
R_t	0.9454	0.8667	0.6447
$Cost$	8.7107	2.3275	0.7243



Conclusions


Safety/Risk
Vulnerability
Resilience
Oil & Gas
Communica-
tions
Water
Electric
Power
Transp.
Emergency
Services
(Networked) CIs protection
Dependency
Structural
complexity
Dynamic
complexity

Resilience of critical infrastructures



Advertising

SAPEA Webinar on Crisis Management

Join our panel of distinguished experts in our free webinar on resilience and information during crisis. April 17📢 💯

In this #webinar, we will discuss critical issues such as effective actions during crises, making sense of incoming information and data, and building trust in communities.
✋ Our esteemed panel includes: Chief Scientific Advisor Prof. Maarja Kruusmaa 🇺🇦, Prof. Virginia Murray, Prof. Enrico Zio, and Prof. Ortwin Renn. The webinar will be chaired by Prof. Nils-Eric Sahlin, MAE.

This is a unique opportunity to pose your questions and be part of the debate on this crucial topic. Don't miss this chance to learn from some of the best minds in the field. ❗ ❗ #Register now to secure your spot in the webinar.
https://lnkd.in/emHxMVMW

Reliability Engineering and System Safety 177 (2018) 176–190

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

The future of risk assessment

E. Zio[a,b]

[a] Chaire Systems Science and the Energy Challenge, Fondation Electricité de France (EDF), Laboratoire Genie Industriel, CentraleSupélec, Université Paris-Saclay, France
[b] Energy Department, Politecnico di Milano, Italy

ARTICLE INFO

Keyword:
Risk assessment
Simulation
Business continuity
Resilience
Condition monitoring-based risk assessment
Dynamic risk assessment
Cyber-physical systems
Safety and security assessment

ABSTRACT

Risk assessment must evolve for addressing the existing and future challenges, and considering the new systems and innovations that have already arrived in our lives and that are coming ahead. In this paper, I swing on the rapid changes and innovations that the World that we live in is experiencing, and analyze them with respect to the challenges that these pose to the field of risk assessment. Digitalization brings opportunities but with it comes also the complexity of cyber-physical systems. Climate change and extreme natural events are increasingly threatening our infrastructures; terrorist and malevolent threats are posing severe concerns for the security of our systems and lives. These sources of hazard are extremely uncertain and, thus, difficult to describe and model quantitatively.

Some research and development directions that are emerging are presented and discussed, also considering the ever increasing computational capabilities and data availability. These include the use of simulation for accident scenario identification and exploration, the extension of risk assessment into the framework of resilience and business continuity, the reliance on data for dynamic and condition monitoring-based risk assessment, the safety and security assessment of cyber-physical systems.

The paper is not a research work and not exactly a review or a state of the art work, but rather it offers a lookout on risk assessment, open to consideration and discussion, as it cannot pretend to give an absolute point of view nor to be complete in the issues addressed (and the related literature referenced to).

1. Introduction

Safety is freedom, freedom from unaffordable harm, and, thus, a human right. Risk assessment has been the dominant paradigm for ensuring this right in the design and operation of industrial systems. Examples of areas of applications include the chemical process industry, the nuclear industry, the transportation sectors, the aerospace industry etc.

Risk assessment is a mature discipline. The structured performance of a risk assessment guides analysts to identify possible hazards/threats, analyze their causes and consequences, and describe risk, typically quantitatively and with a proper representation of uncertainties. In the assessment, the analysts make assumptions and simplifications, collect and analyze data, and develop and use models to represent the phenomena studied. For example, the failure modes of components due to a given earthquake, the heat fluxes on a structure due to a fire, the response of operators to an accident are all the results of conceptual models that attempt to mimic how a real accident would proceed, based on the knowledge available. The risk assessment of a system requires the consideration of a possibly very large number of scenarios with multiple failures of its components and, by so doing, provides an in-depth understanding and knowledge of the system failure modes with consequent increase of the awareness on risk and the attention to safety, which typically leads to an overall improvement of the safety of the system.

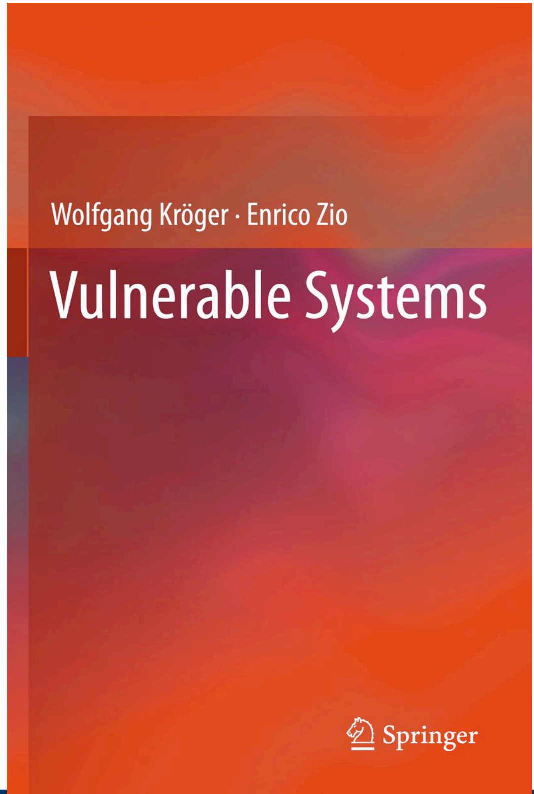
The World we live in is rapidly changing in many ways. Digitalization is bringing new opportunities of connectivity, monitoring and awareness, and is changing the way we communicate and socially behave. Mobility and social pressure are changing the landscape in which we live and operate. Continuous advancements in technical knowledge and technology are improving our production processes, products and services, as well as our environments, while changing the business and work/job scenarios. As the digital, physical and human worlds continue to integrate, we experience a deep transformation in industry, which far-reaches into our lives. The 4th industrial revolution, the internet of things and big data, the industrial internet, are changing the way we design, manufacture, supply products and services, the way we move and live in our environment. This is creating a complex network of things and people that are seamlessly connected and communicating. It is providing opportunities to make production systems and services more efficient and faster, and more flexible and resilient the complex supply chains and distribution networks that tie the global economy.

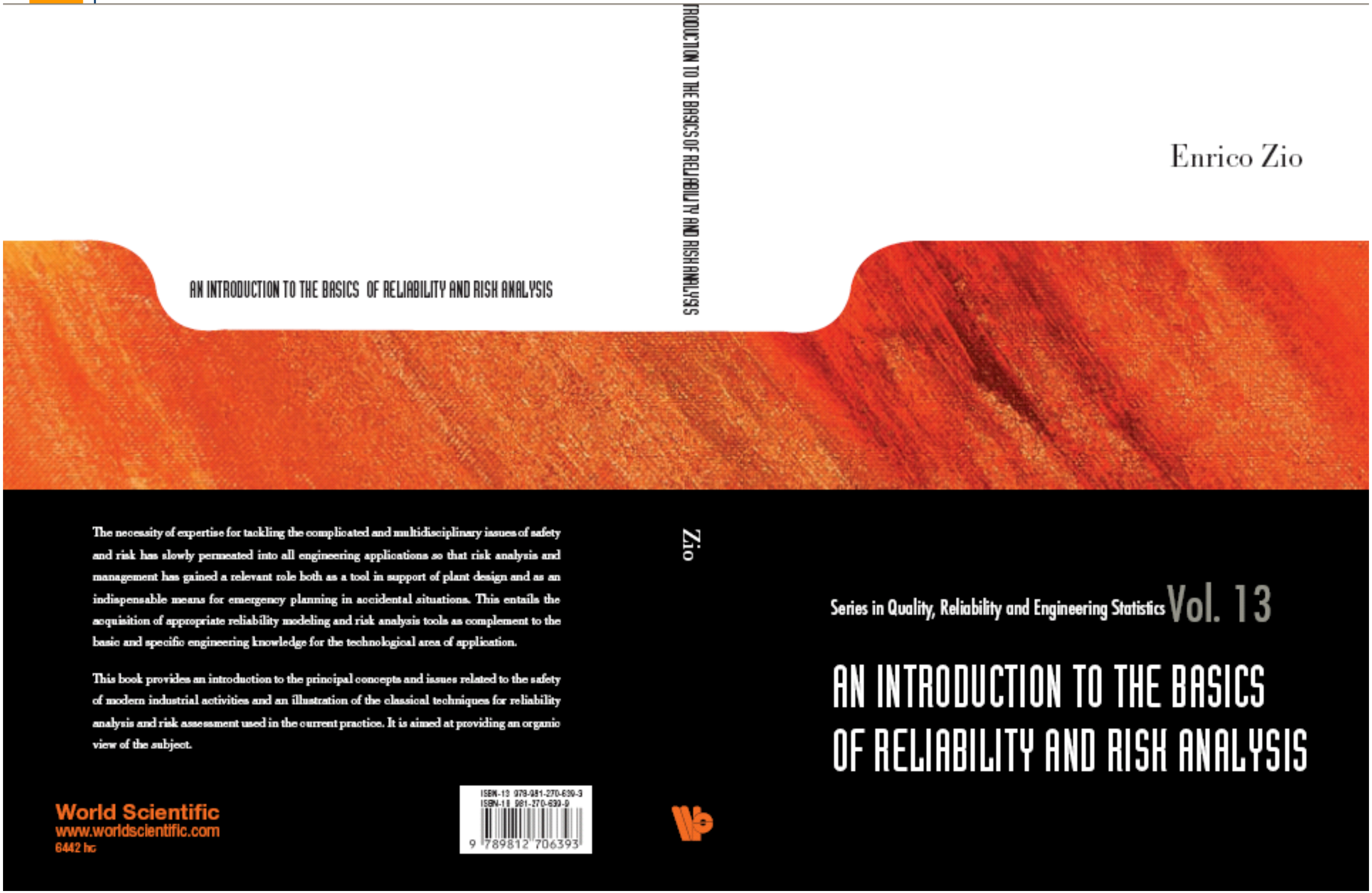
E-mail addresses: enrico.zio@polimi.it, enrico.zio@centralesupelec.fr.

https://doi.org/10.1016/j.ress.2018.04.020
Received 1 June 2017; Received in revised form 20 March 2018; Accepted 24 April 2018
Available online 25 April 2018

Learning material

- Copies of transparencies.
- Selection of articles available for download.
- Books




AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS
Enrico Zio
Zio
The necessity of expertise for tackling the complicated and multidisciplinary issues of safety and risk has slowly permeated into all engineering applications so that risk analysis and management has gained a relevant role both as a tool in support of plant design and as an indispensable means for emergency planning in accidental situations. This entails the acquisition of appropriate reliability modeling and risk analysis tools as complement to the basic and specific engineering knowledge for the technological area of application.
This book provides an introduction to the principal concepts and issues related to the safety of modern industrial activities and an illustration of the classical techniques for reliability analysis and risk assessment used in the current practice. It is aimed at providing an organic view of the subject.
Series in Quality, Reliability and Engineering Statistics Vol. 13
AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS
World Scientific
www.worldscientific.com
6442 hc
ISBN-13 978-981-270-639-3
ISBN-10 981-270-639-9
9 789812 706393

Connecting Great Minds

Series on Quality, Reliability and Engineering Statistics – Vol. 14

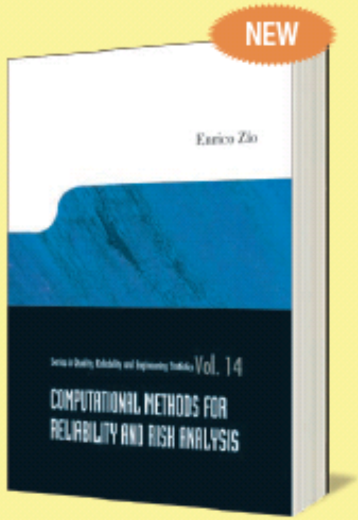
COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS

Enrico Zio

Department of Energy, Polytechnic of Milan, Italy

This book illustrates a number of modelling and computational techniques for addressing relevant issues in reliability and risk analysis. In particular, it provides: i) a basic illustration of some methods used in reliability and risk analysis for modelling the stochastic behaviour of systems, e.g. the Markov and Monte Carlo simulation methods; ii) an introduction to Genetic Algorithms, tailored to their application for RAMS (Reliability, Availability, Maintainability and Safety) optimization; iii) an introduction to key issues of system reliability and risk analysis, like dependent failures and importance measures; iv) a presentation of the issue of uncertainty and of the techniques of sensitivity and uncertainty analysis used in support to reliability and risk analysis.

The book provides a technical basis for senior undergraduate or graduate courses and a reference for researchers and practitioners in the field of reliability and risk analysis. Several practical examples are provided to demonstrate the application of the concepts and techniques in practice.



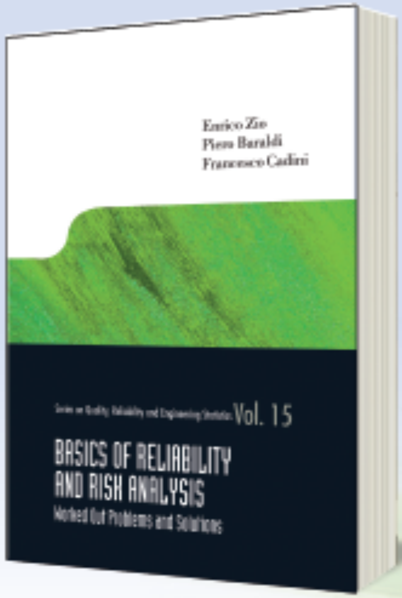
250pp (approx.) Feb 2009
978-981-283-901-5 US$51 £28
981-283-901-1

World Scientific www.worldscientific.com

ICP Imperial College Press www.icpress.co.uk

Preferred Publisher of Leading Thinkers

Connecting Great Minds



Series on Quality, Reliability and Engineering Statistics - Vol. 15

BASICS OF RELIABILITY AND RISK ANALYSIS

Worked Out Problems and Solutions

by **Enrico Zio** *(École Centrale Paris et Supelec, France & Politecnico di Milano, Italy)*, **Piero Baraldi** *(Politecnico di Milano, Italy)*, & **Francesco Cadini** *(Politecnico di Milano, Italy)*

Reliability and safety are fundamental attributes of any modern technological system. To achieve this, diverse types of protection barriers are placed as safeguards from the hazard posed by the operation of the system, within a multiple-barrier design concept. These barriers are intended to protect the system from failures of any of its elements, hardware and software, human and organizational.

Correspondingly, the quantification of the probability of failure of the system and its protective barriers, through reliability and risk analyses, becomes a primary task in both the system design and operation phases.

This exercise book serves as a complementary tool supporting the methodology concepts introduced in the books "An introduction to the basics of reliability and risk analysis" and "Computational methods for reliability and risk analysis" by Enrico Zio, in that it gives an opportunity to familiarize with the applications of classical and advanced techniques of reliability and risk analysis.

This book is also available as a set with *Computational Methods for Reliability and Risk Analysis* and *An Introduction to the Basics of Reliability and Risk Analysis*.

220pp	June 2011	
978-981-4355-03-2	US$68	£44
Set		
978-981-4360-68-5	US$199	£129

World Scientific
Connecting Great Minds

Series on Quality Reliability and Engineering Statistics - Vol. 14

COMPUTATIONAL METHODS FOR RELIABILITY AND RISK ANALYSIS

by **Enrico Zio** *(Polytechnic of Milan, Italy)*

This book illustrates a number of modelling and computational techniques for addressing relevant issues in reliability and risk analysis. In particular, it provides: i) a basic illustration of some methods used in reliability and risk analysis for modelling the stochastic failure and repair behaviour of systems, e.g. the Markov and Monte Carlo simulation methods; ii) an introduction to Genetic Algorithms, tailored to their application for RAMS (Reliability, Availability, Maintainability and Safety) optimization; iii) an introduction to key issues of system reliability and risk analysis, like dependent failures and importance measures; and iv) a presentation of the issue of uncertainty and of the techniques of sensitivity and uncertainty analysis used in support of reliability and risk analysis.

The book provides a technical basis for senior undergraduate or graduate courses and a reference for researchers and practitioners in the field of reliability and risk analysis. Several practical examples are included to demonstrate the application of the concepts and techniques in practice.

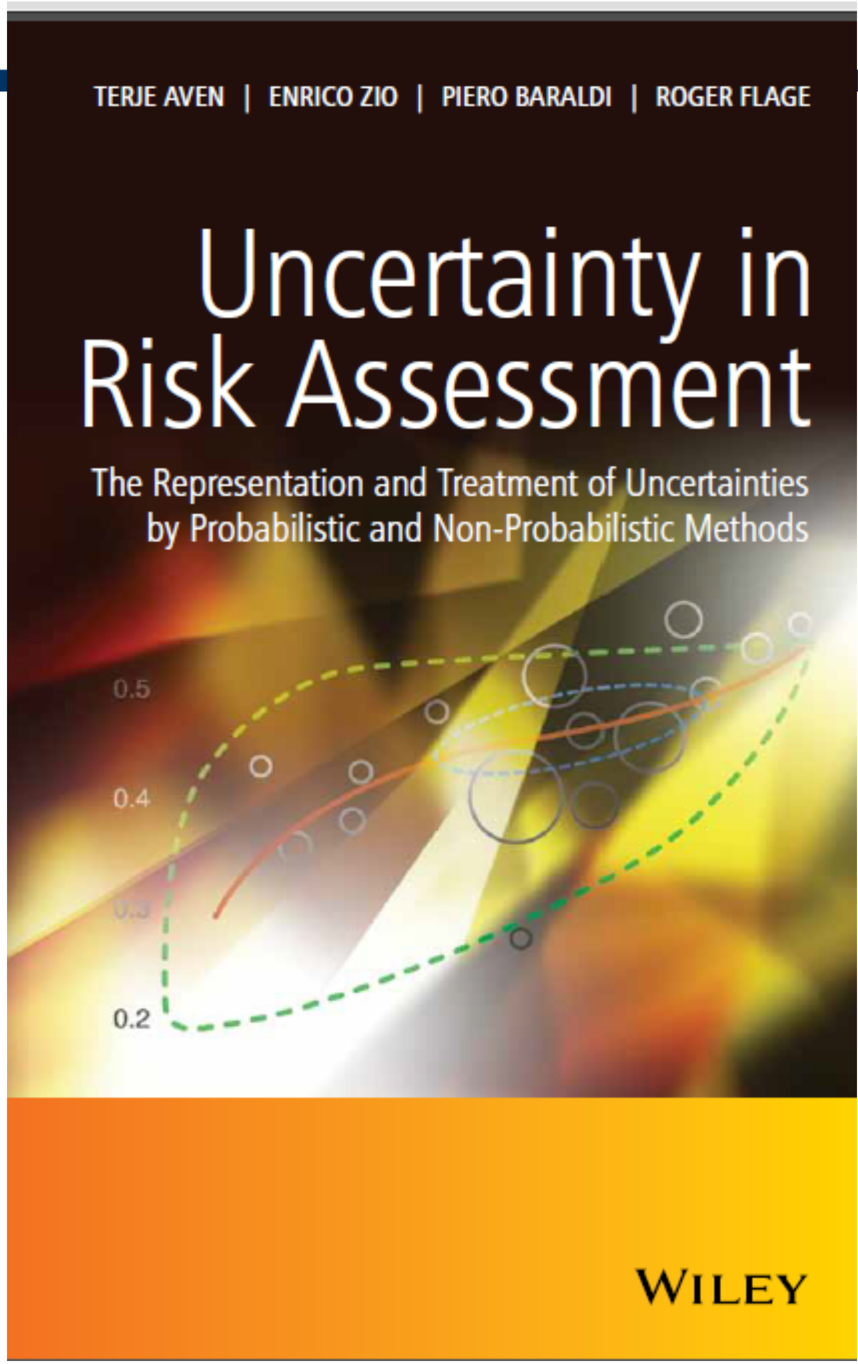
This book is also available as a set with *Basics of Reliability and Risk Analysis* and *An Introduction to the Basics of Reliability and Risk Analysis*.

Readership: Undergraduates, graduates, academics and professionals in the fields of systems engineering and safety and risk analysis.

264pp	January 2009	
978-981-283-901-5	£57	$92
Set		
978-981-4360-68-5	£129	$225

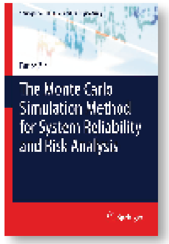
Imperial College Press
www.icpress.co.uk

Preferred Publisher for Leading Thinkers


TERJE AVEN | ENRICO ZIO | PIERO BARALDI | ROGER FLAGE
Uncertainty in Risk Assessment
The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods
0.5
0.4
0.2
WILEY

Springer

springer.com



2013, 2013, XIV, 198 p. 69 illus., 24 in color.

Printed book

Hardcover
- ▸ 129,95 € | £117.00 | $179.00
- ▸ *139,05 € (D) | 142,94 € (A) | CHF 173.00

eBook

For individual purchases buy at a lower price on springer.com. A free preview is available. Also available from libraries offering Springer's eBook Collection.
- ▸ springer.com/ebooks

MyCopy

Printed eBook exclusively available to patrons whose library offers Springer's eBook Collection.***
- ▸ € | $ 24.95
- ▸ springer.com/mycopy

E. Zio, Ecole Centrale Paris, Chatenay-Malabry, France

The Monte Carlo Simulation Method for System Reliability and Risk Analysis

Series: Springer Series in Reliability Engineering

- ▸ Illustrates the Monte Carlo simulation method and its application to reliability and system engineering to give the readers the sound fundamentals of Monte Carlo sampling and simulation
- ▸ Explains the merits of pursuing the application of Monte Carlo sampling and simulation methods when realistic modeling is required so that readers may exploit these in their own applications
- ▸ Includes a range of simple academic examples in support to the explanation of the theoretical foundations as well as case studies provide the practical value of the most advanced techniques so that the techniques are accessible

Monte Carlo simulation is one of the best tools for performing realistic analysis of complex systems as it allows most of the limiting assumptions on system behavior to be relaxed. The Monte Carlo Simulation Method for System Reliability and Risk Analysis comprehensively illustrates the Monte Carlo simulation method and its application to reliability and system engineering. Readers are given a sound understanding of the fundamentals of Monte Carlo sampling and simulation and its application for realistic system modeling.

Whilst many of the topics rely on a high-level understanding of calculus, probability and statistics, simple academic examples will be provided in support to the explanation of the theoretical foundations to facilitate comprehension of the subject matter. Case studies will be introduced to provide the practical value of the most advanced techniques.

This detailed approach makes The Monte Carlo Simulation Method for System Reliability and Risk Analysis a key reference for senior undergraduate and graduate students as well as researchers and practitioners. It provides a powerful tool for all those involved in system analysis for reliability, maintenance and risk evaluations.

Organizational and administrative details of the course

Course overview

- **Title:** Resilience of critical infrastructures
- **Coordinators:**
  - Nasi Greta, Associate Professor, Bocconi University
  - Zio Enrico, Professor, Politecnico di Milano (Italy) and Mines Paris PSL University (France)
- **Teaching team (Polimi):**
  - Zio Enrico, Professor, Politecnico di Milano (Italy) and Mines Paristech (France)
  - Di Maio Francesco, Professor, Politecnico di Milano (Italy)
  - Naseh Moghanlou Lida, PhD student, Politecnico di Milano (Italy)
- **Audience:** Master students
- **Language:** English

Greta Nasi

greta.nasi@unibocconi.it

ITALY

Associate Professor, Department of Social and Political Sciences, Università Bocconi

Director of the Master of Science in Cyber Risk Strategy and Governance at Università Bocconi and Politecnico di Milano

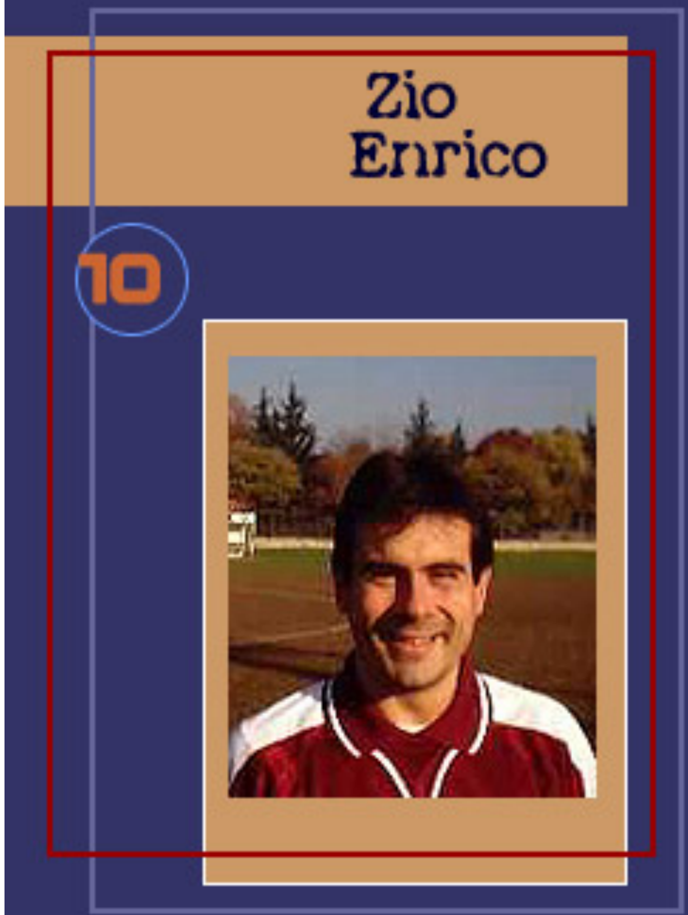
Director of Research for Government, SDA Bocconi School of Management

Director of the Executive Master in Management of International Organizations, SDA Bocconi School of Management

Honorary Fellow, Business School of the University of Edinburgh

Greta Nasi is an Associate Professor at the Department of Policy Analysis and Public Management at Università Bocconi and Director of the Master of Science in Cyber Risk Stategy and Governance at Università Bocconi and Politecnico di Milano
At SDA Bocconi, she is currently the Director of Research for Government (Government, Health and Not for Profit Division) and the Director of the Executive Master in Management of International Organizations. She was the Director of the Public Management and Policy Department from 2012-2016. She has conducted numerous research, education and consulting projects with some of the leading institutions at national and international level.
Her research activities focus on the following topics: innovation and change management in the public sector, digital transformation in public services and in the healthcare sector, service and city management and competitiveness.
Since 2016, she has been an Honorary Fellow at the Business School of the University of Edinburgh. She is the author of numerous books and articles on her topics of interest. Her works have been published in Public Administration, Public Management Review and the International Journal of Public Administration, the Journal of Medical Internet Research, among others. She is a member of the editorial board of many journals including Public Management Review, the Journal of Comparative Policy Analysis: Research and Practice (2005-2019) and Review of Public Administration. She has served on the board of many public administrations such as the International Research Society of Public Management and she is an institutional representative at the Association for Public Policy Analysis and Management. She has been invited to lecture in many international universities such as Seul National University, Lee Kwan Yew School of Public Policy, ESADE, Erasmus University, among others.
Greta was a Fulbright Scholar at the Maxwell School of Public Affairs and Citizenship, where she earned her MPA. She also has a Ph.D. in Public Management from the Università di Parma and a B.Sc. in Public Administration and International Organizations from Università Bocconi.

Speaker



signed for Panthers: July 1998

Better known "***Little knee***" for his ease in running.

After the much talked retirement of the "*Divine Ponytail*" (Roberto Baggio), he stands as the last true and pure artist of the Italian soccer. He remains a patrimony to be safeguarded, in spite of the " *tactical problem*" he represents for the Panthers team.

Fancy on the field and even brilliant off the field: meeting him disguised as Santa Claus at weddings or as deejay in popular Milano's bars, one would never realize that he is an internationally renowned luminary.

Francesco Di Maio

francesco.dimaio@polimi.it

ITALY

Associate Professor

Laboratory of Signal Analysis and Risk Analysis

Department of Energy, Politecnico di Milano

Lida Naseh Moghanlou

lida.naseh@polimi.it

IRAN

MSc: Mechanical Engineering- Applied design

PhD Candidate (cycle XXXV)

Laboratory of Signal Analysis and Risk Analysis

Department of Energy, Politecnico di Milano

Research Topic: Resilience of the system of systems made up of electric power grid, the charging infrastructure and the system of Electric Vehicles (EVs)

1	14/04/2023	14:15-18:15	Course introduction: definition of critical infrastructure, safety, vulnerability, risk, resilience
2	21/04/2023	14:15-18:15	Logic Methods: Fault Trees + Exercises
3	28/04/2023	14:15-18:15	Logic Methods: Event Trees + Exercises
4	05/05/2023	14:15-18:15	Logic Methods: GTST-MLD (with application to CPS)
			Homework assignment (project)
5	12/05/2023	14:15-18:15	Complexity theory and centrality measures
6	19/05/2023	14:15-18:15	Decision analysis for resilience (Game theory, Adversarial Risk Analysis, …)
			Homework assignment (project)
7	26/05/2023	14:15-18:15	Seminar (TBD)

Thanks…

…for your attention…
…and for being resilient