POLITECNICO DI MILANO

lasar
laboratory of signal and risk analysis

MINES ParisTech | PSL

CENTRE DE RECHERCHE
SUR LES RISQUES
ET LES CRISES





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

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):**
  - Ahmed Ibrahim, Professor, Politecnico di Milano (Italy
  - \Maria Valentina Clavijo Mesa, Politecnico di Milano (Italy)
  - Zio Enrico, Professor, Politecnico di Milano (Italy) and Mines Paris – PSL University (France)
  - + Foreign Experts
- **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.

Maria Valentina CLAVIJO MESA
mariavalentina.clavijo@polimi.it
MSc: Naval and Oceanographic Engineering – University of Sao Paulo, Brazil
PhD Candidate (Cycle XXXVIII)
Laboratory of Analysis of Systems for the Assessment of Reliability, Risk and Resilience
Department of Energy, Politecnico di Milano
Research topic: Resilience of Critical Infrastructures exposed to Climate Change

Ibrahim AHMED
Ibrahim.ahmed@polimi.it
PhD Nuclear Engineering – Kyung Hee University, South Korea
Assistant Professor
Laboratory of Analysis of Systems for the Assessment of Reliability, Risk and Resilience
Department of Energy, Politecnico di Milano
Research topic: Risk monitoring of Nuclear Power Plants

Professor

Enrico Zio

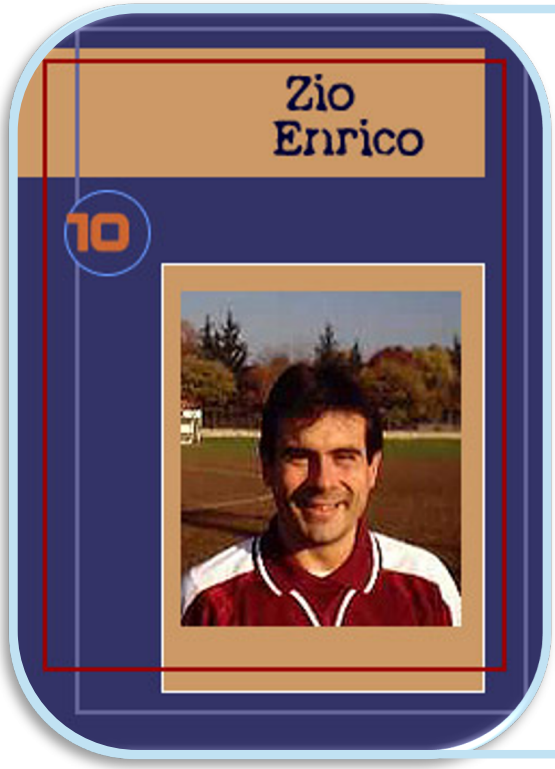
Enrico Zio

- Centre for research on Risks and Crises (CRC), Mines Paris PSL University
- Energy Department, Politecnico di Milano, Milan, Italy

- Fellow of the Italian Academy of Technology
- IEEE fellow
- Asia-Pacific Artificial Intelligence Association fellow
- Academy of the Artificial Intelligence Industry fellow
- Research Award of the Alexander von Humboldt Foundation
- Lifetime achievement award of the Society for Reliability and Safety
- Alan O. Plait 2024 Award
- System Safety Society (ISSS) Educator of the Year Award
- Ayyub-Wiechel Risk Analysis Award of the American Society of Mechanical Engineers, ASME (2025)

- H-index = 114
- Top 2% of the World scientists, according to Stanford ranking
- Top 1% of Highly Cited Researchers, according to Clarivate Analytics

Professor



Signed for Panthers: July 1998

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

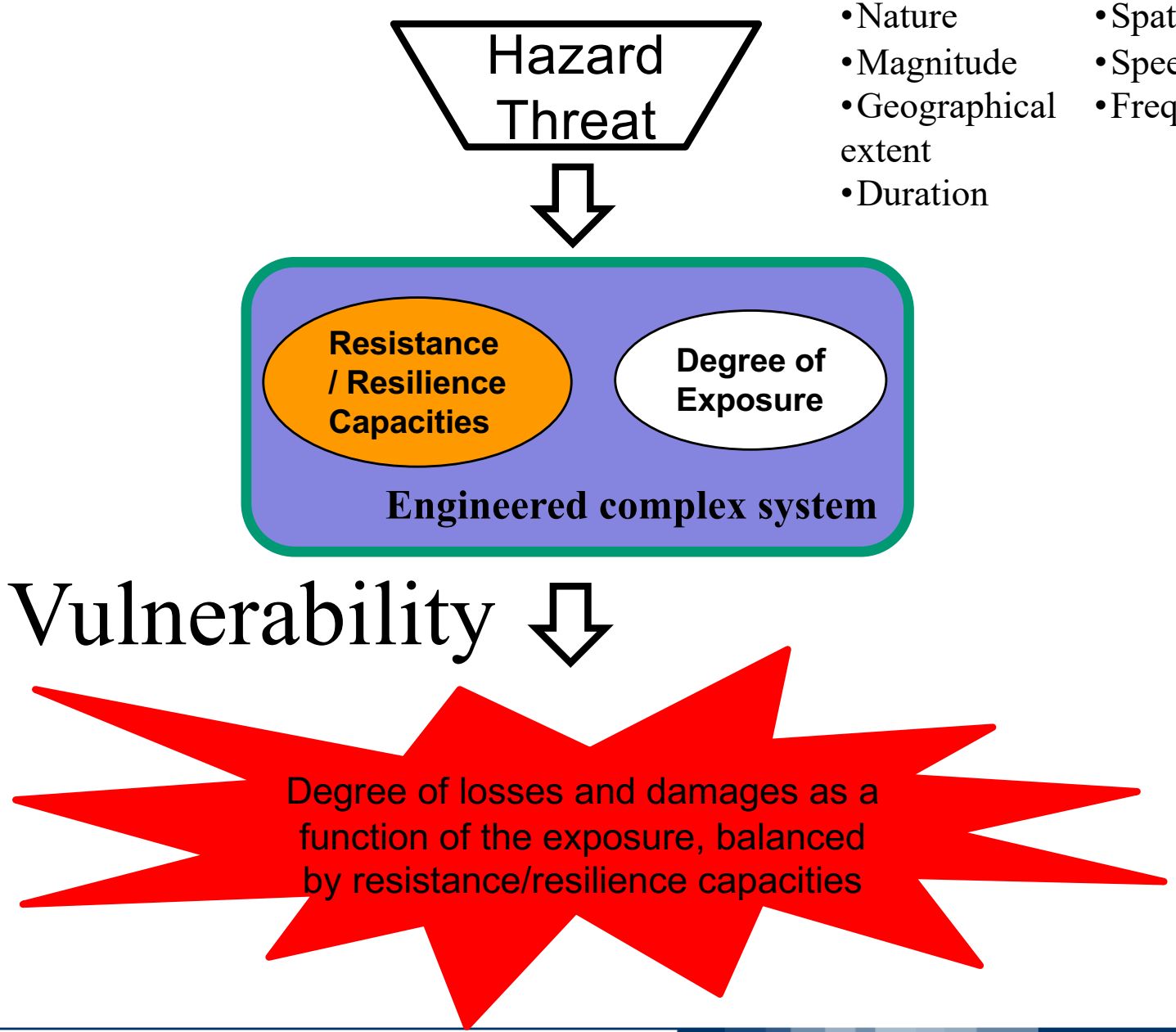
After the much talked retirement of the "*Divine Ponytail*" (Roberto Baggio), he stands as the last true and pure artist of the Italian soccer.

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.

Vulnerability

Vulnerability and failures

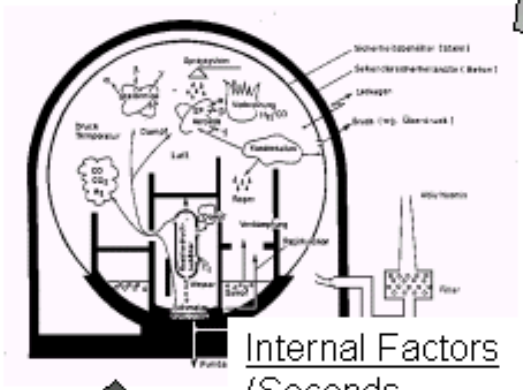


Vulnerability - Technical Example

External Threats

Short Distance Threat
(700 km/h)

Long Distance Threat
(10 m/s)



Internal Factors
(Seconds,
Minutes, Hours)

Earthquake

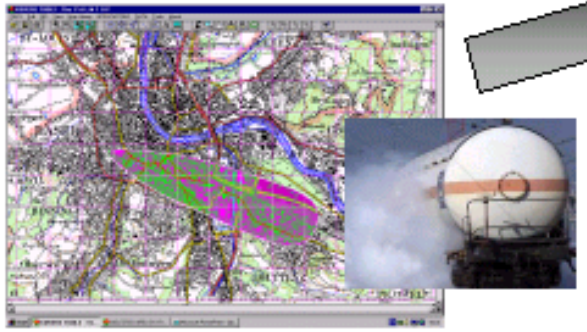
Short or Long Distance
Threat / Intentional
Software Attack
(Speed of Light)

- 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)

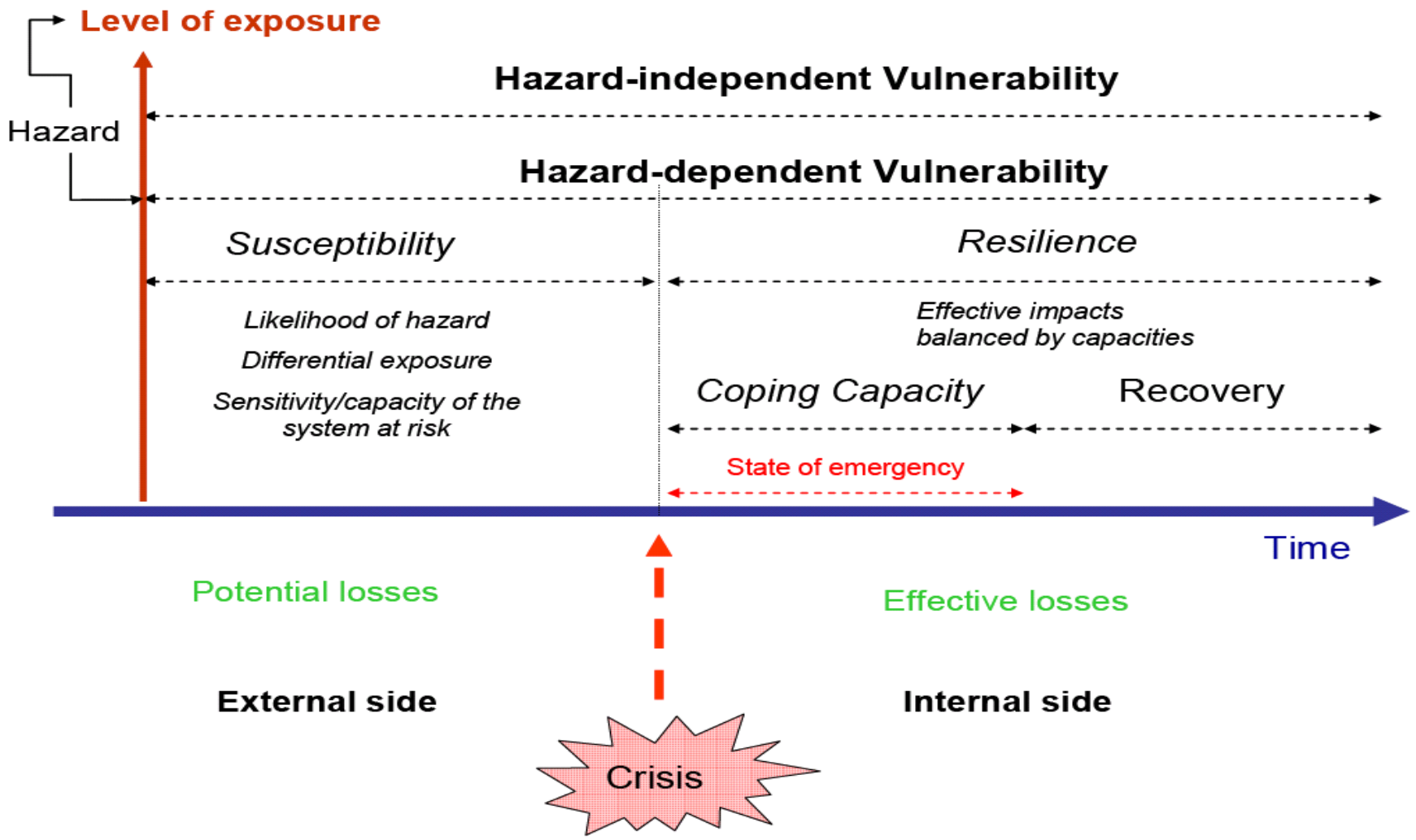
Congested
and/or crowded
areas

Internal Factors

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

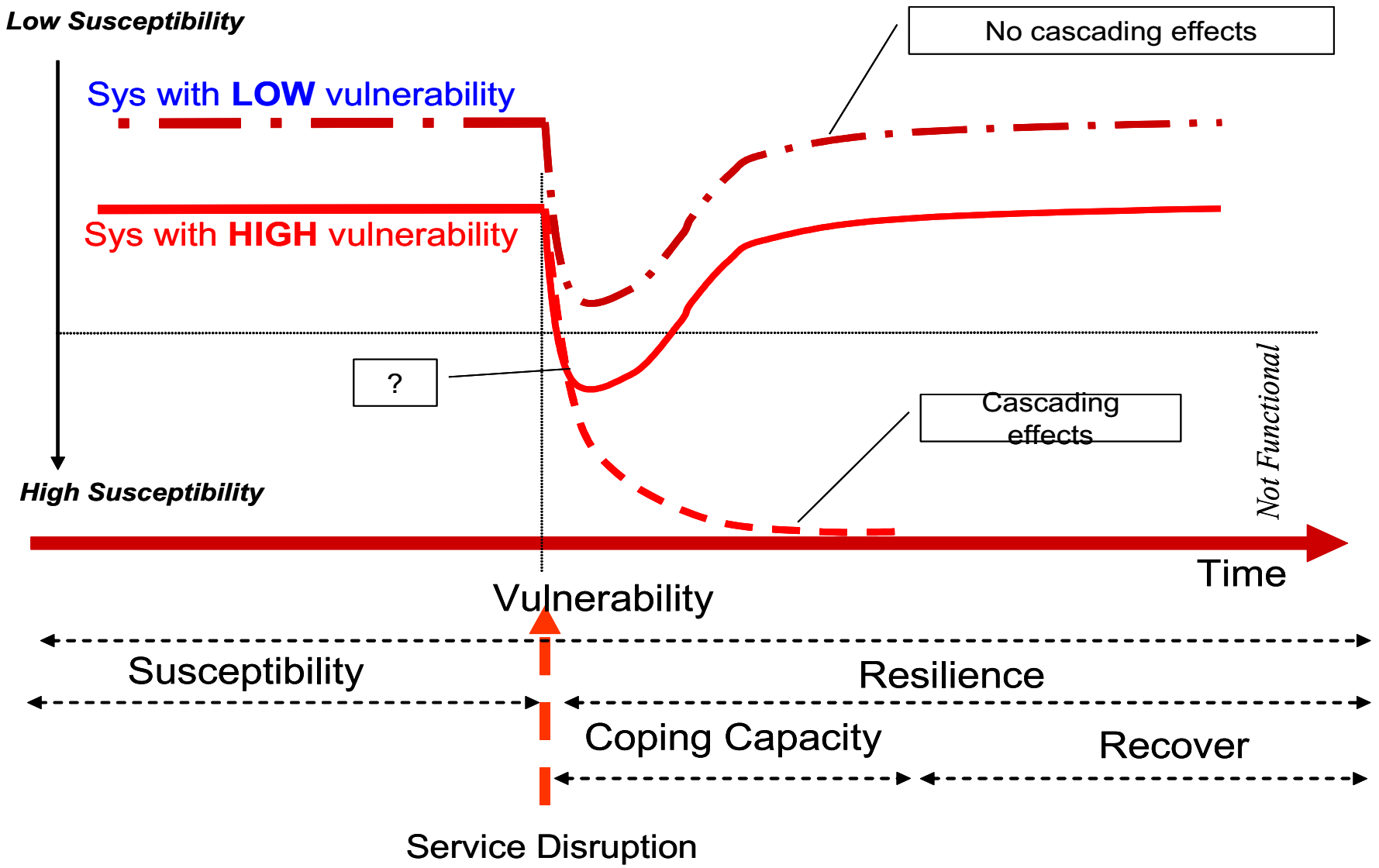
Vulnerability Assessment

Vulnerability Model



Source: S. Bouchon

Vulnerability Scenarios

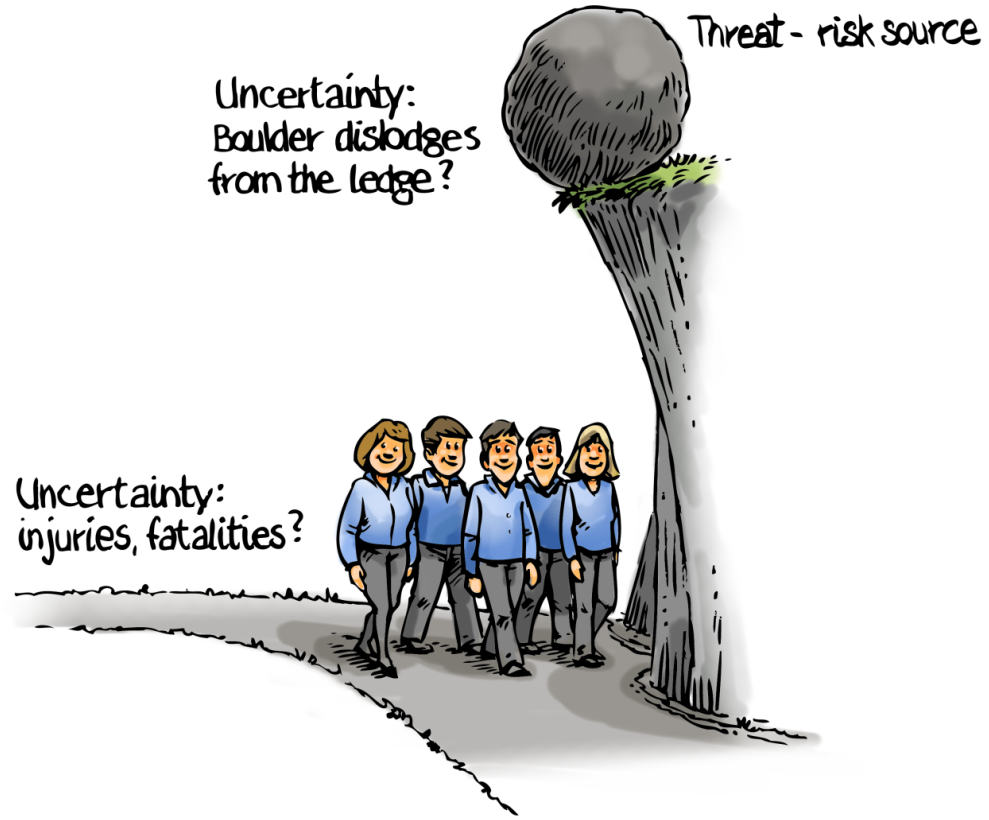


RISK

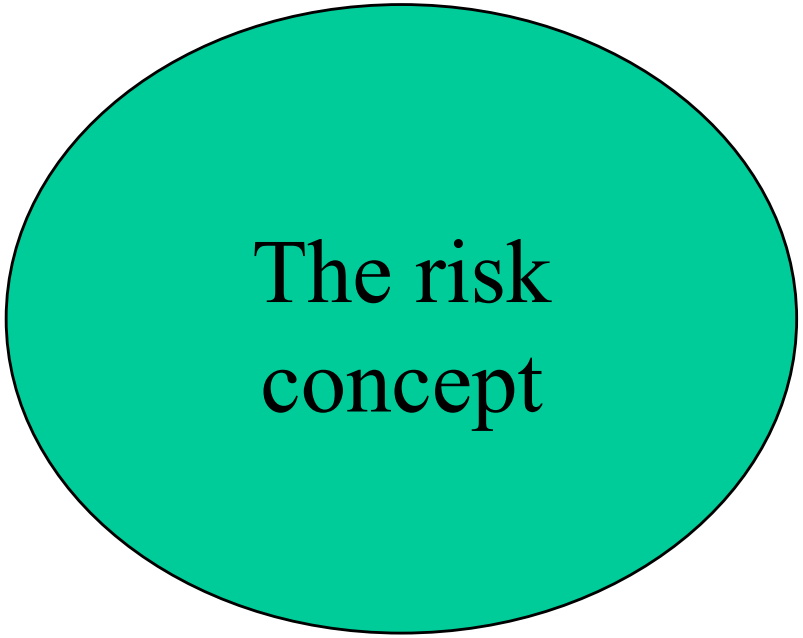
Consequences

Events with some effects

Some effects are undesirable



Uncertainty



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

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

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

RISK ASSESSMENT

RISK ASSESSMENT

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

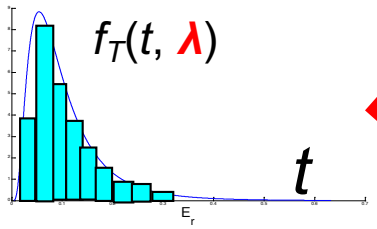
KNOWLEDGE K

valve 1

valve 2

...

valve *N*

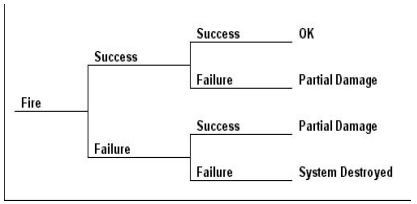


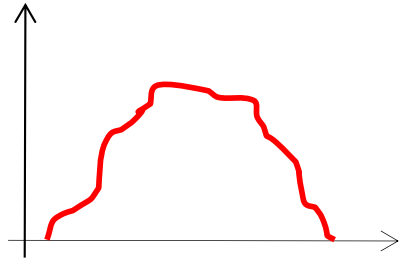
"λ is UNIFORM between 10^{-3} and 10^{-2} $[h^{-1}]$"

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

REPRESENTATION OF UNCERTAINTY (M)

SYSTEM RISK MODEL





(UNCERTAIN) RISK MEASURES (a,c,u,M,K)

UNCERTAINTY PROPAGATION

Probabilistic Risk Assessment

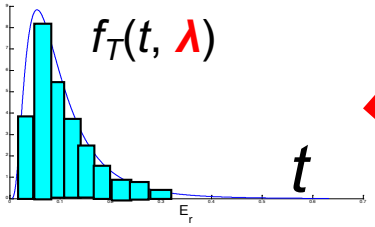
KNOWLEDGE K

valve 1

valve 2

...

valve *N*

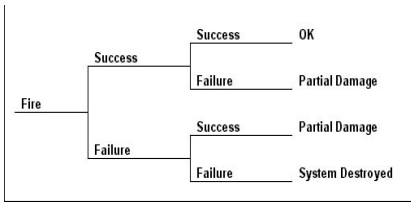


"λ is UNIFORM between 10^{-3} and 10^{-2} [h^{-1}]"

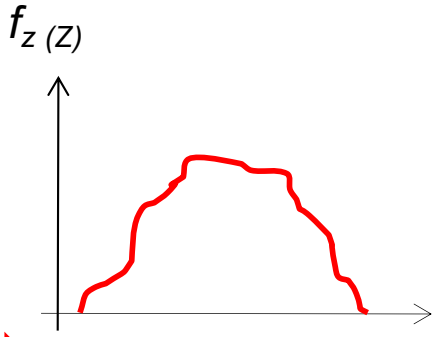
"λ is less than 10^{-2} [h^{-1}] with probability 0.9"

PROBABILISTIC REPRESENTATION OF UNCERTAINTY (M=P)

SYSTEM RISK MODEL

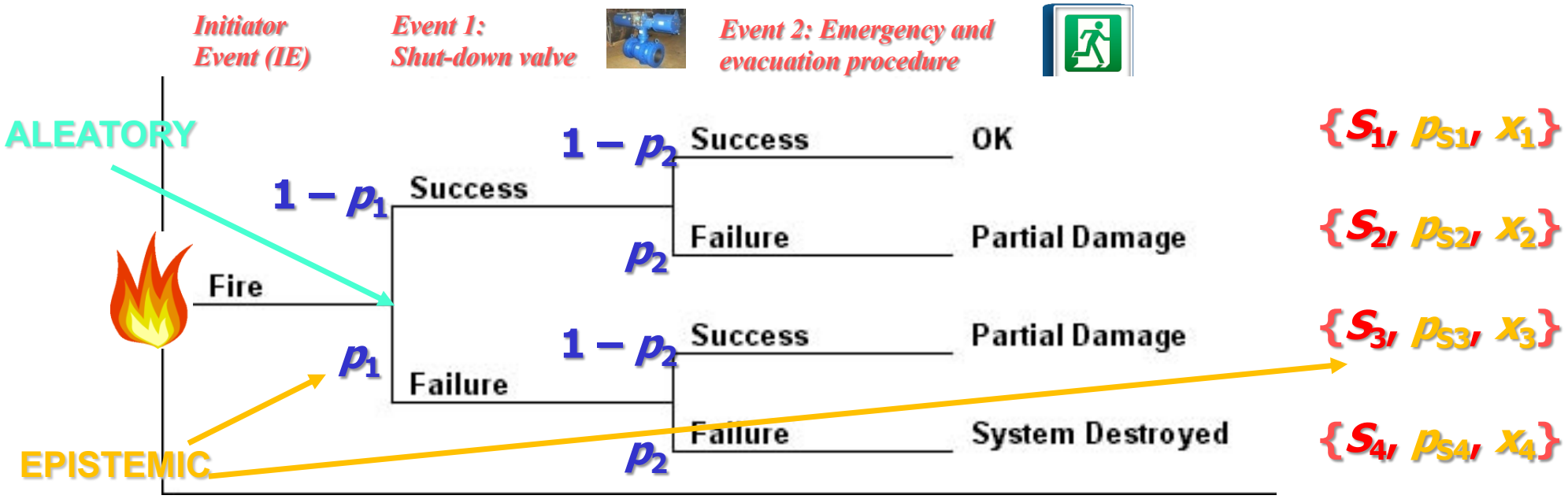


UNCERTAINTY PROPAGATION



(PROBABILISTIC) RISK MEASURES (a,c,u,P,K)

(aleatory and epistemic) Uncertainty



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

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

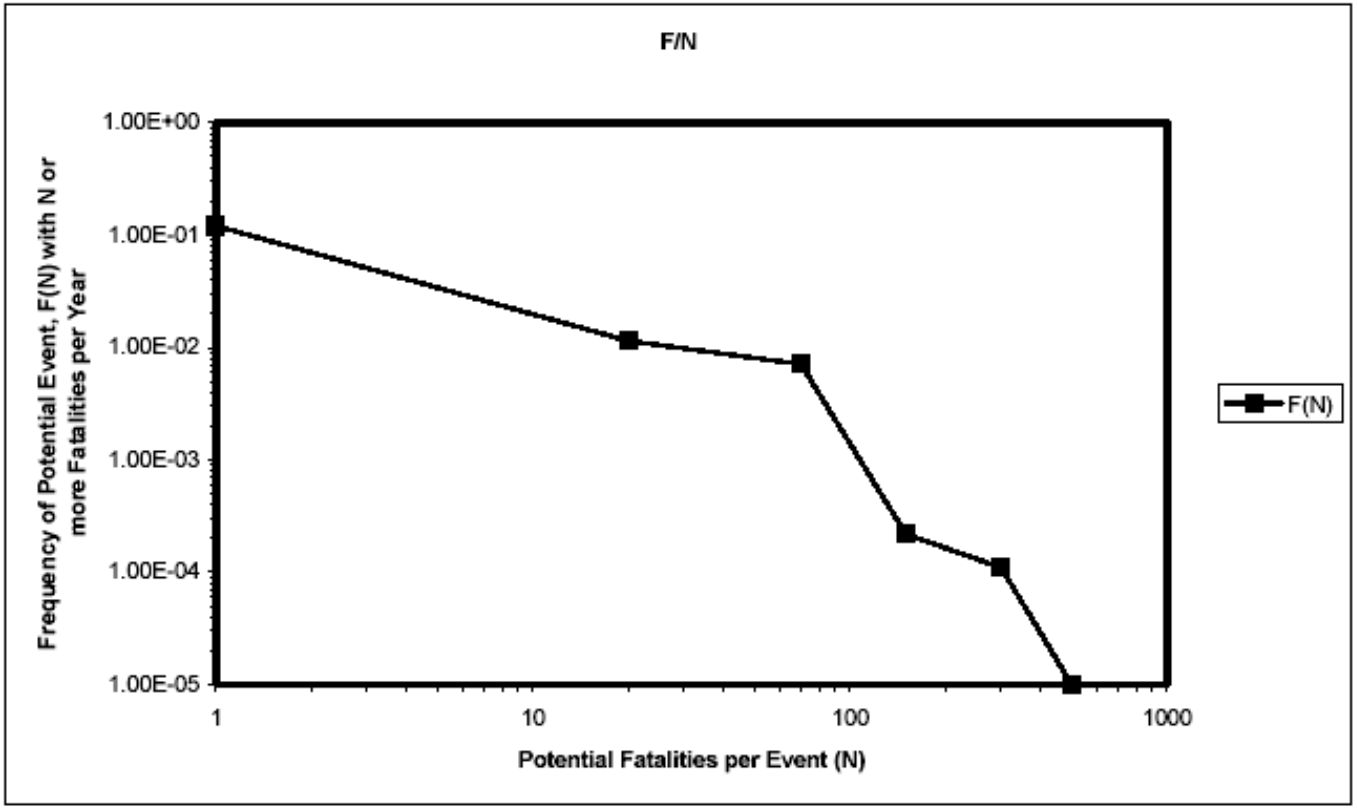
PRA results:

$\{S_i, p_i, x_i\}$

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.

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

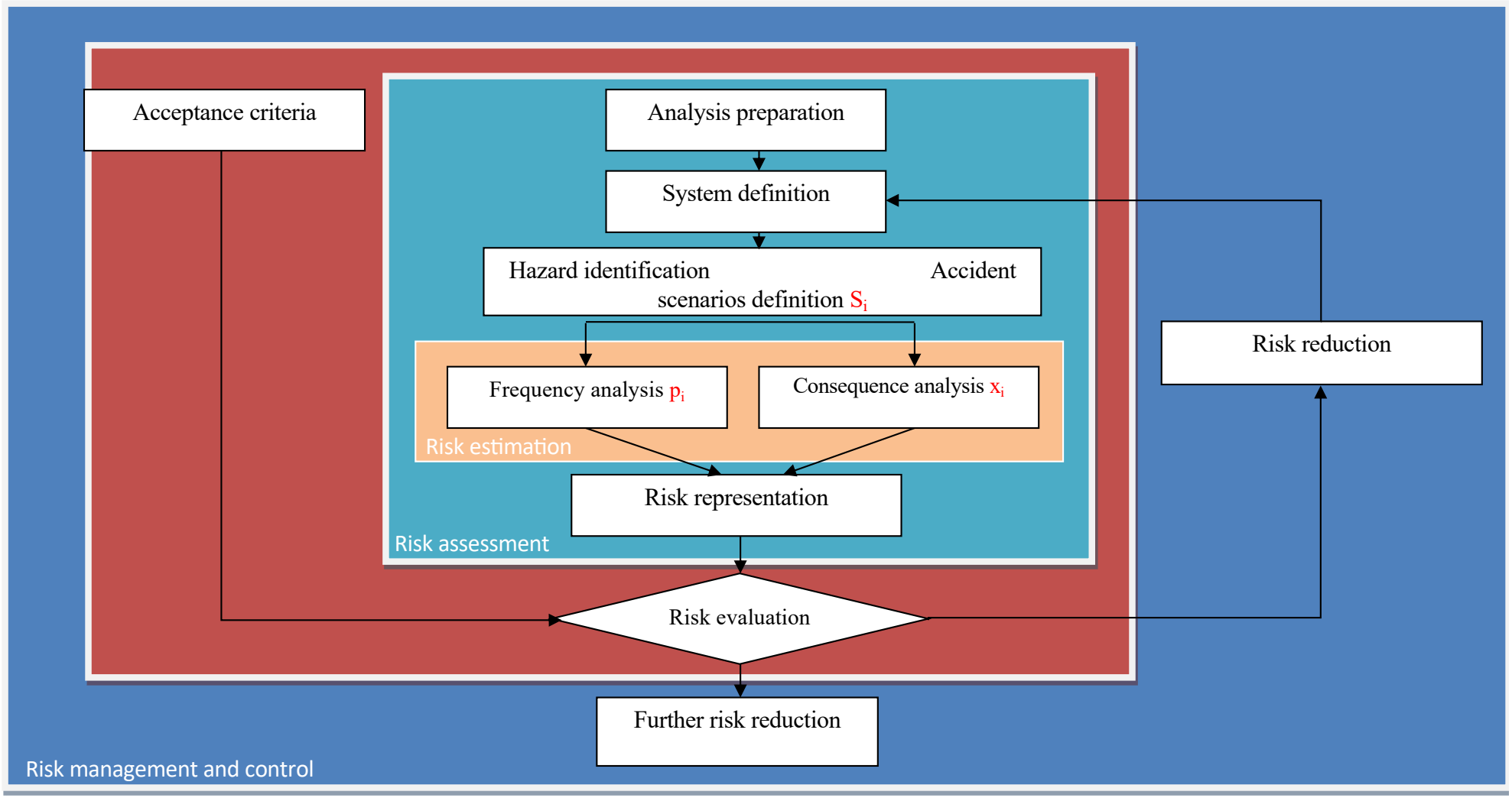
The level of risk is not acceptable and risk control measures are required to move the risk figure to the previous regions.

Consequence					Increasing Annual Frequency					
Severity	People	Environ.	Assets	Reputation	0	A	B	C	D	E
					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			Intolerable Risk			
4	PTD(*) or 1 fatality	Major effect	Major damage	National impact						
5	Multiple fatalities	Extensive effect	Extensive damage	International impact						

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

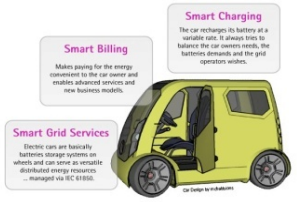
Risk acceptance criteria

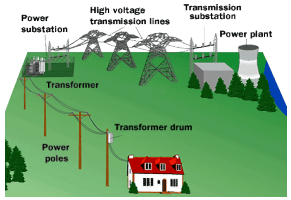
Complex Systems

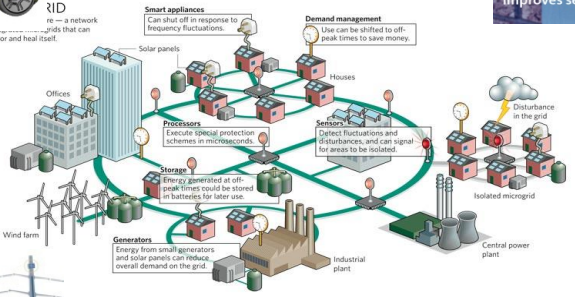
Enrico Zio

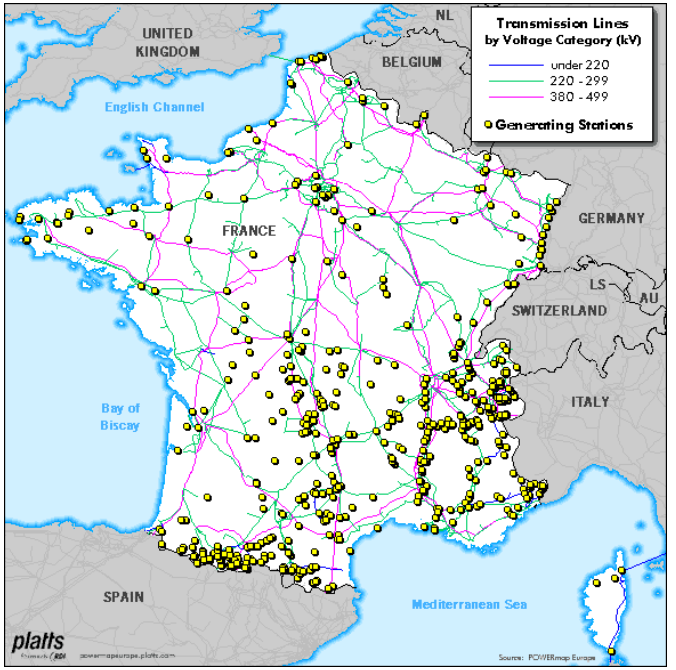
MINES ParisTech | PSL | POLITECNICO MILANO 1863

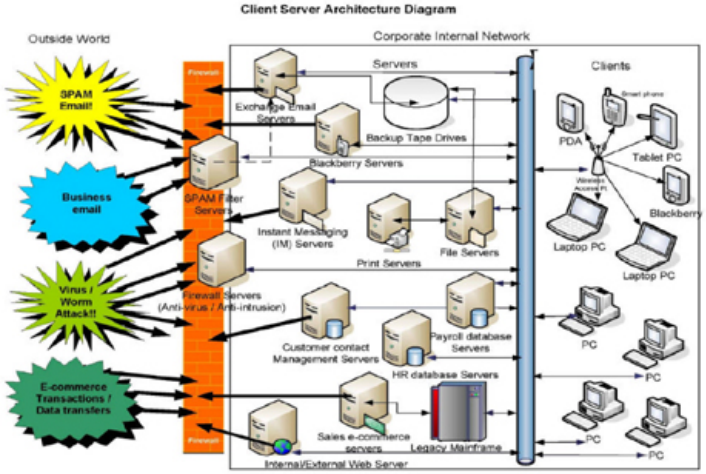
Complex (technical) systems



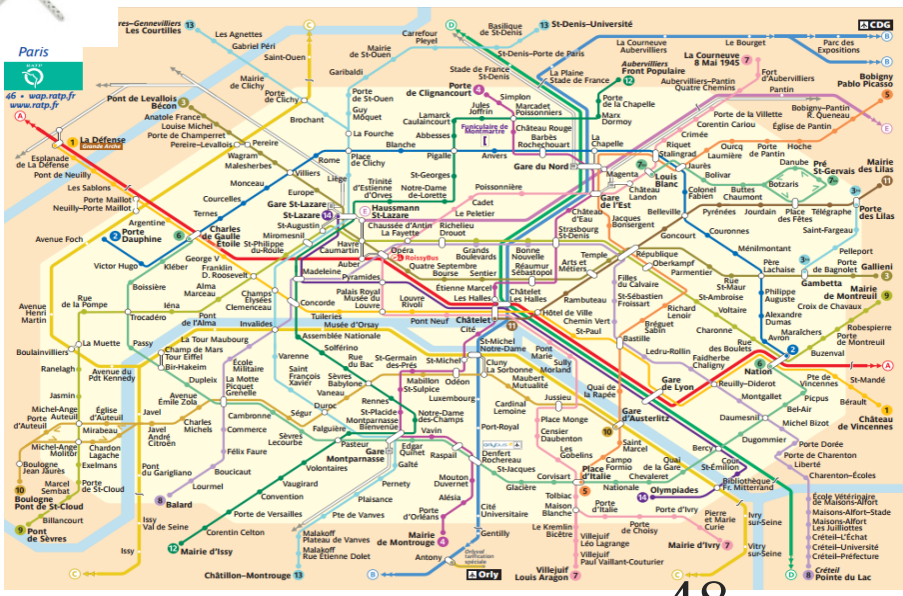






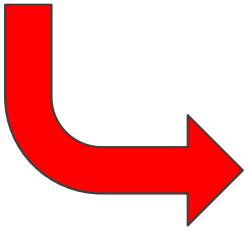


Microsoft submission to Federal Rules Committee



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)

Complicated vs. complex technical systems

Complicated Systems (mechanical watches, aircraft, power plants, etc.)

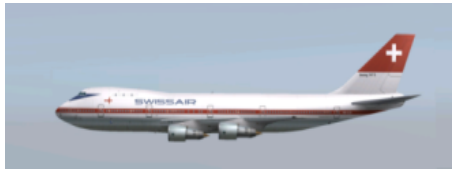
- Components have **well-defined roles** and are governed by prescribed interactions.
- **Structure remains stable** over the time. Low dynamics.
- **No adaptation**. One key defect may bring system to a halt.
- Limited range of responses to changes in their environment.
- **Decomposing** the system and analyzing sub-parts can give us an understanding of the behavior of the whole, i.e. the whole can be reassembled from its parts.
- Problems can be solved through analytical thinking and diligence work.

Complex Systems (stock market, www, power grid, etc.)

- **Rules of interaction** between the components may **change** over time and may not be well understood.
- **Connectivity of the components may be quite plastic** and roles may be fluid. Interactions are not always obvious.
- System responds to external conditions and **evolves**.
- Display organization without a central organizing principle (**self-organization/emergence**).
- Respond to and interact with their environment.
- Inadequate information about the state of the influencing variables, nonlinearities.
- Overall behavior cannot be simplified in terms of their building blocks. **The whole is much more than the sum of its parts.**

Examples of complicated and complex systems

Complicated Systems: Mechanical watches, Boeing 747, Power plants, …



Complex Systems: Stock market, Power grids, Highways, WWW, Natural ecosystems, ...

The nation's Power Grid is an example of a complex system that evolves continually

It must respond to the challenges such as:

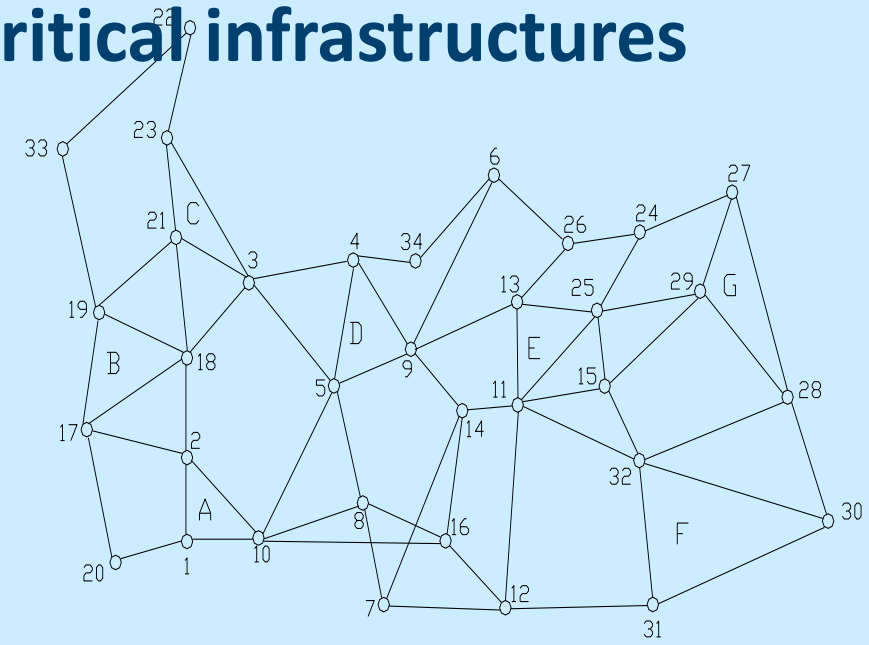
- incorporating **new, intermittent sources** at new locations such as wind and solar
- supporting a **market** in bulk electricity
- accommodating **new loads** such as electric cars
- exploiting the ongoing advances in **communications**, computer power, materials and devices.

Scrapping the Power Grid and redesigning it from scratch is not an option: **advances must build on and coexist** with components and technologies that are up to 50 years old.

Any redesign or upgrade affects how the engineering system is used and this, in turn, affects the requirements. This **interaction with and adaptation to the changing environment** makes the evolving system more complex.

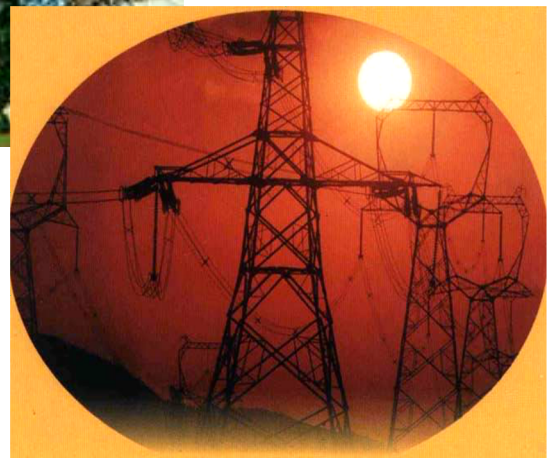
Critical Infrastructures

Critical infrastructures



Water supply Systems

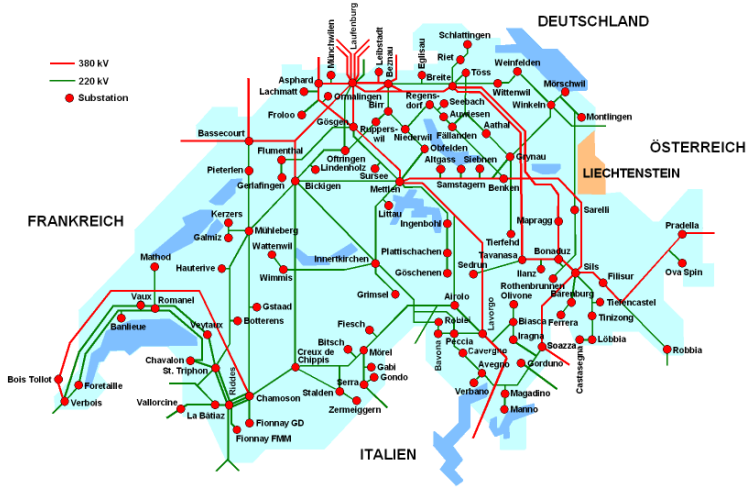
Electric Power Networks



Gas supply Systems

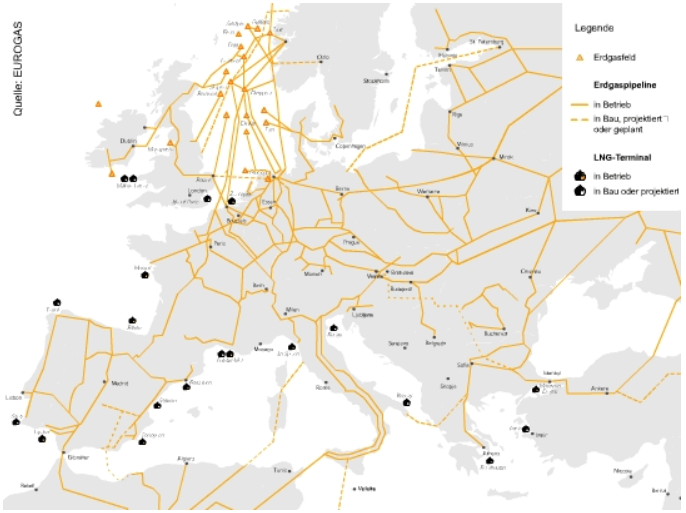
Critical Infrastructures

Swiss Power System



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

Natural Gas Pipelines

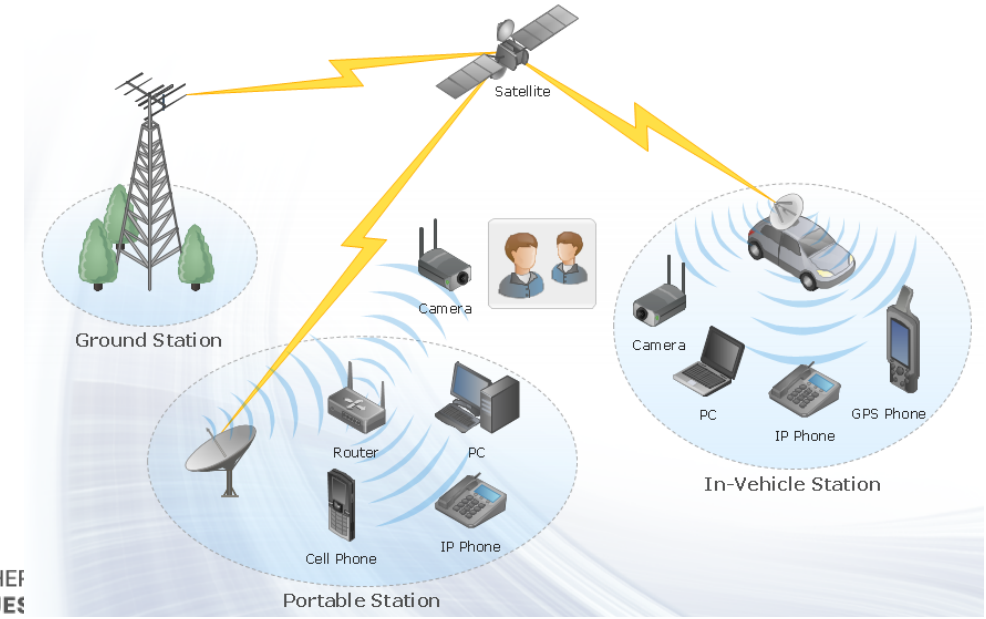


Critical Infrastructures: complexity

- Structural complexity
  - Heterogeneity
  - Scale and dimensionality
  - Dependences and interdependences
- Dynamic complexity
  - Emergent behavior
  - Adaptive learning
  - Evolution and growth mechanisms
  - Cascading

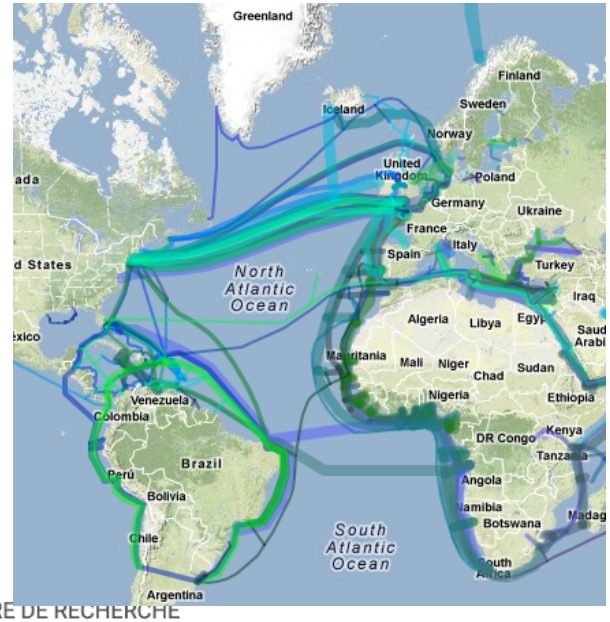
Critical Infrastructures: structural complexity

- ***Heterogeneity*** of components across different technological domains due to increased integration among systems.
  - ❖ Physical hard components (road, railways, pipelines, …)
  - ❖ Soft components (SCADA, information and telecommunication systems)
  - ❖ Human and organizational components



Critical Infrastructures: structural complexity

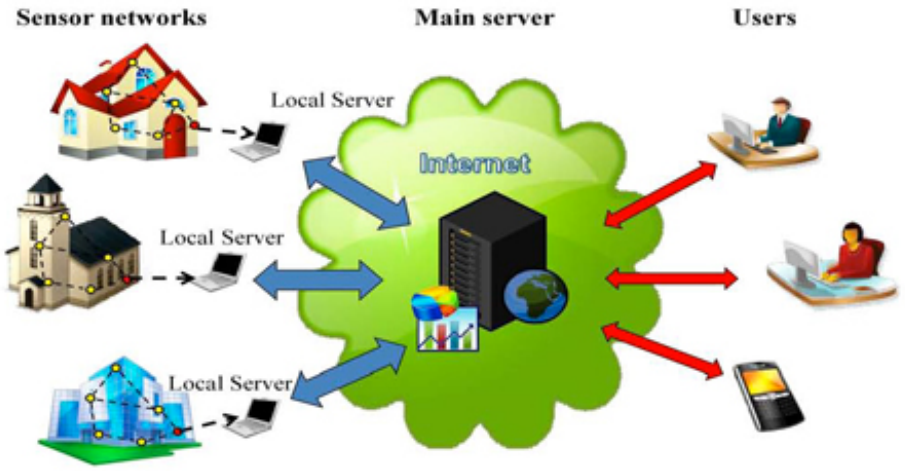
- ***Scale and dimensionality*** of connectivity through a large number of components highly interconnected by ***dependences and interdependences*** distributed over a large geographic extent.
- **Decomposability** of the system into subsystems and into further separate elementary elements.



Critical Infrastructures: structural complexity

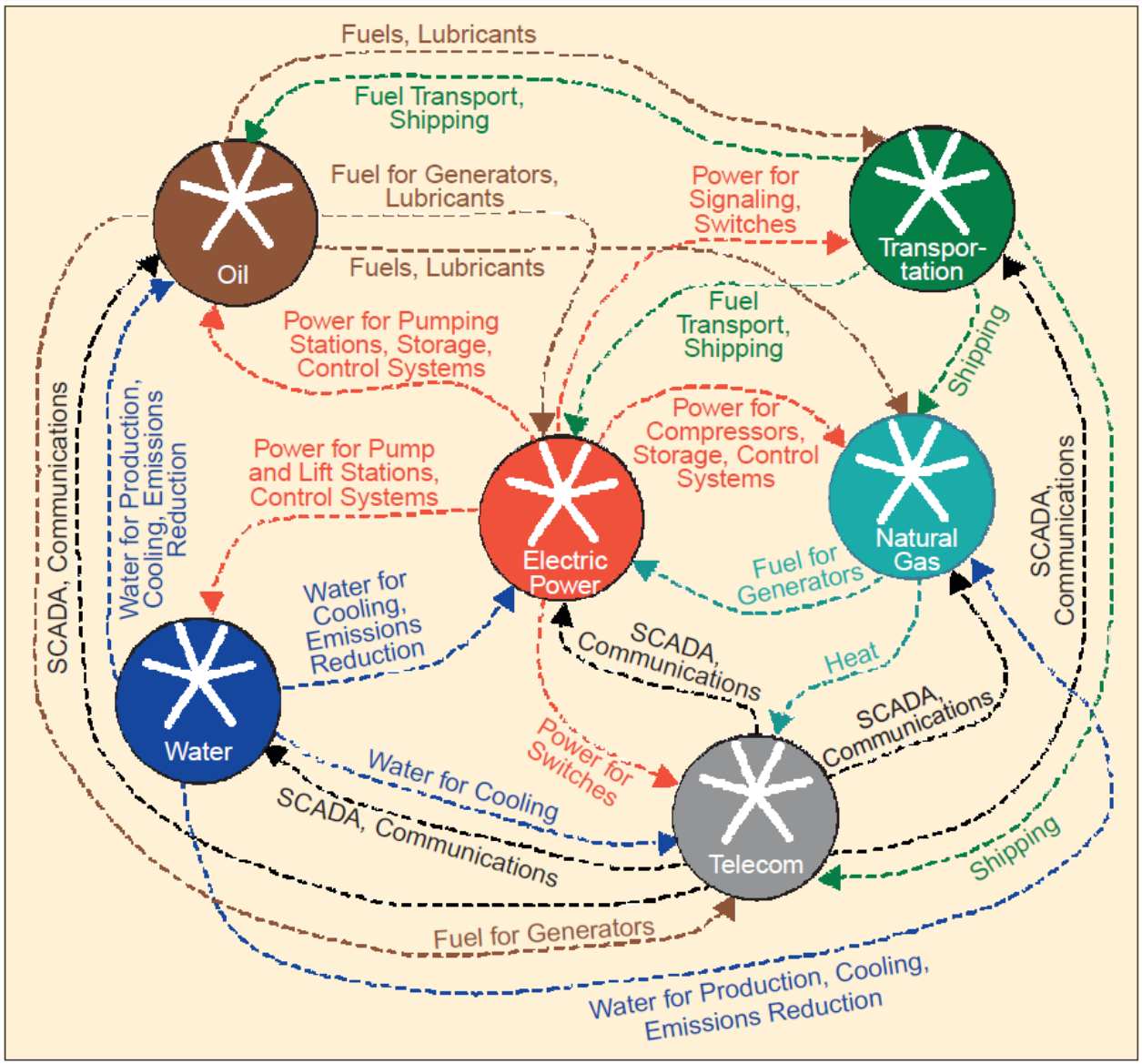
An example: the Internet

- It penetrates our offices, houses and public spaces
- It is a platform for commercial and social interactions
- It increases the efficiency of economic activities
- It is a backbone and enabler of convergence across multiple fields (engineering, social, economic, finance and policies)



Critical Infrastructures: structural complexity

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



Critical Infrastructures: dynamic complexity

Emergent behavior refers to actions of a system as a whole that are not simple combinations of the actions of the individual constituents of the system. It emerges in response to changes in the environmental and operational conditions of parts of the system.

Examples:

- *Internet*: social bookmarking leads to an emergent effect in which information resources are reorganized according to users priorities.
- *Electric power grids*: local failures can evolve into unexpected cascade failure patterns with transnational, cross-industry effects.
- *Smart grids*: large amount of information exchanged within technologies at a period of high electricity demand can lead to a vulnerable condition of the system.
- *Road transportation congestion*: slow movement of the traffic.

Critical Infrastructures: dynamic complexity

Emergent behavior on a **highway** during **rush hour.**

Global system property that emerges: **slow movement of the traffic**

It **arises from** the cumulative effects of the actions and interactions of all individual vehicles. The global effects depend on the general activities of sufficiently many of them, within the context of that highway.

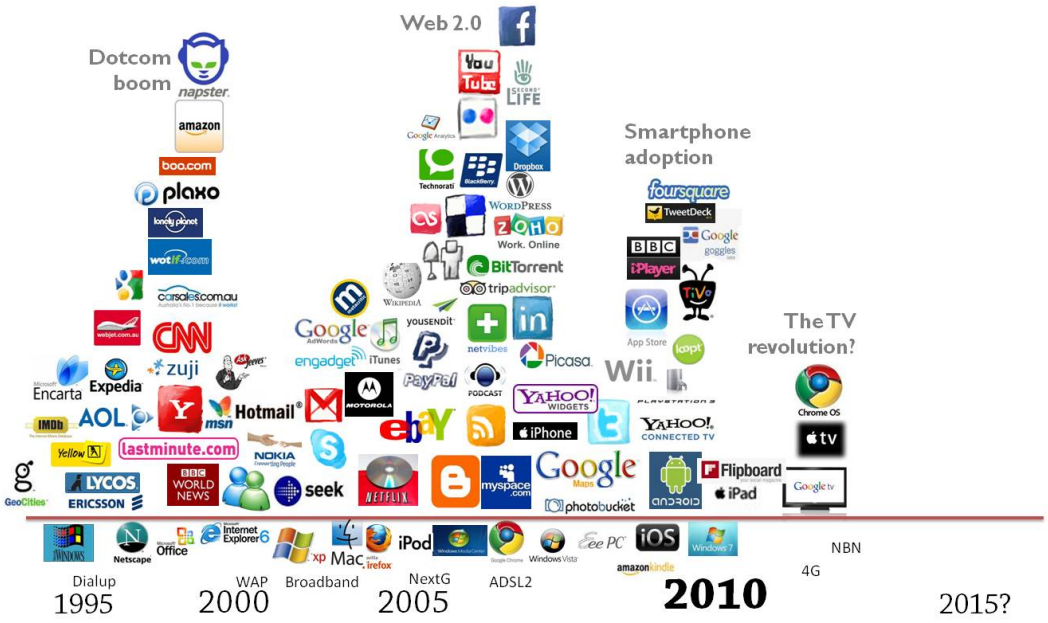
It is **not due to** specific actions of individual vehicles → no individual vehicle plays a critical role.
If some subset of the vehicles acted differently in their local actions (within certain boundaries), the global effect of slow-moving traffic would be unchanged.

Critical Infrastructures: dynamic complexity

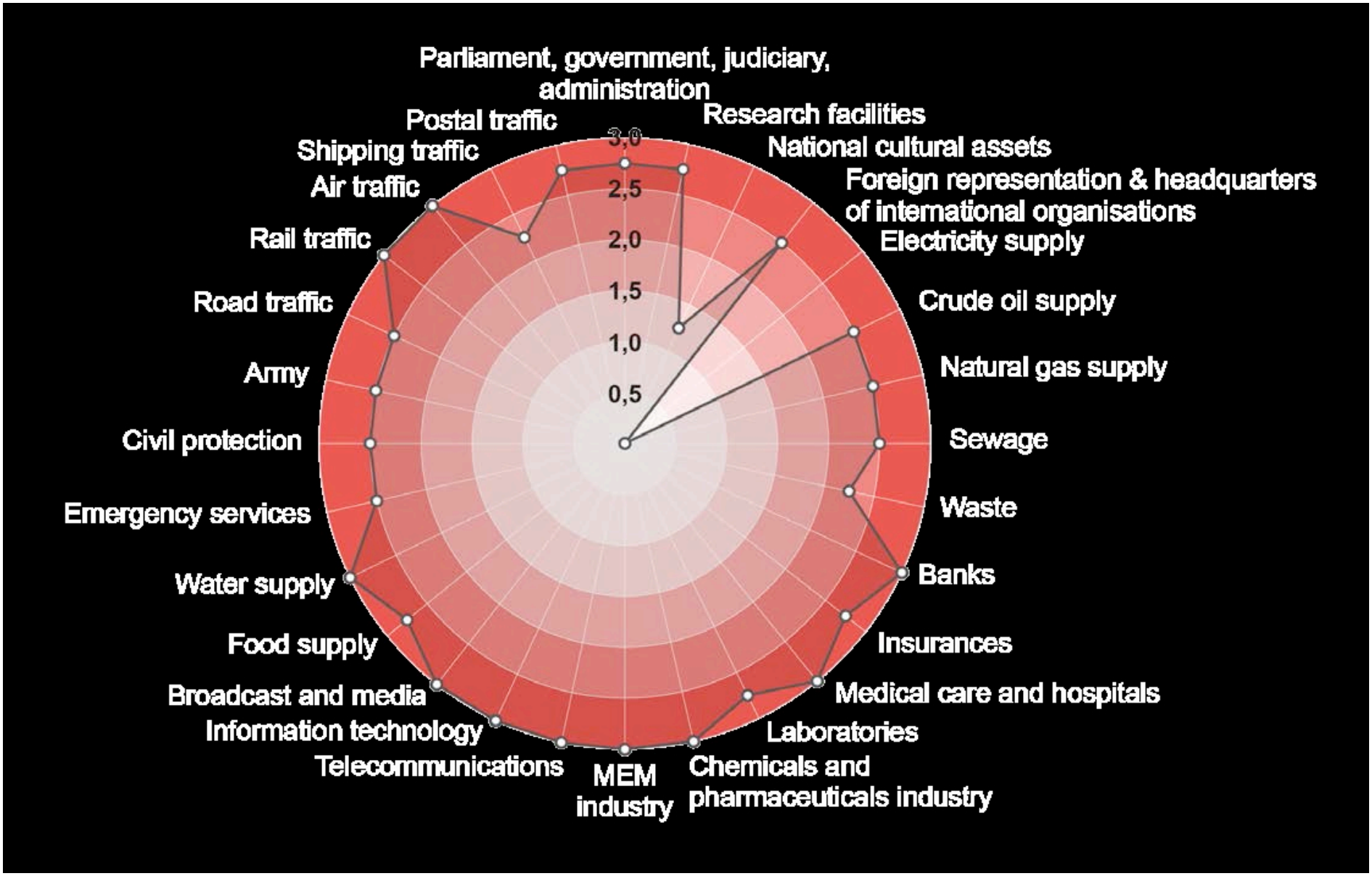
Evolution and growth mechanisms: the system is forced to evolve when the external pressures applied to it exceed “critical values” beyond which the adaptive learning mechanisms are inefficient. In the absence of a central authority governing system changes, the evolutionary process resembles natural selection in biological systems, resulting in the consequent disappearance of elements associated with low adaptive fitness. Unlike biological systems, complex engineered systems are exposed also to constant growth of user portfolios.

Examples:

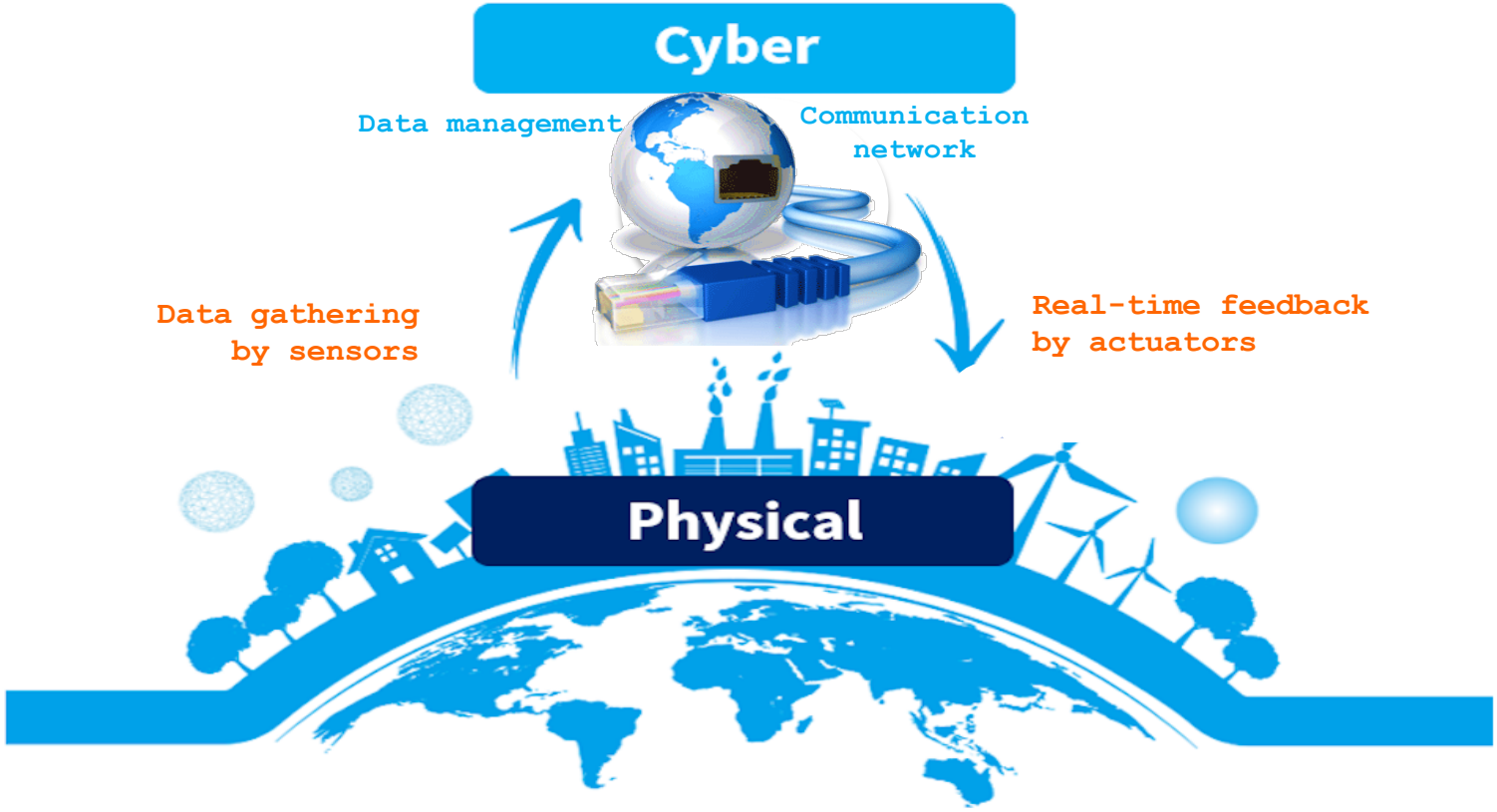
Internet: it is the product of the evolution of its constitutive software and hardware technologies, information and communication services and applications, and also it faces the creation of new ways of use, such as e-commerce.



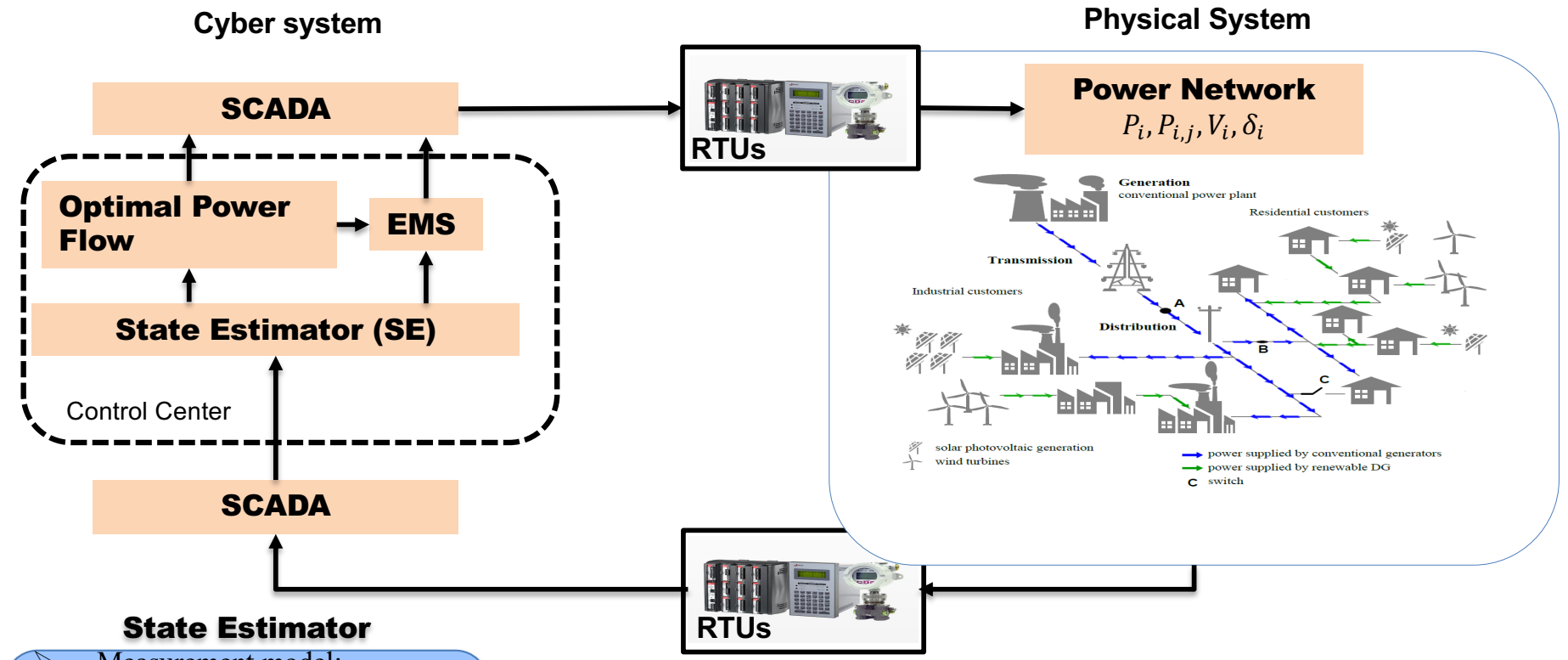
Critical Infrastructures and their interdependencies



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 :
  $\hat{x} = (H^T W H)^{-1} H^T W z$

Risk Assesssment and Management

Enrico Zio

MINES ParisTech | PSL | POLITECNICO MILANO 1863

Electric power supply systems: 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

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

Impact on Population - strong

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

Economic Losses - moderate

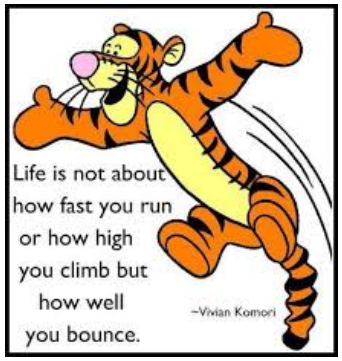
- About 120 million €
- Several hundred k € due to the interruption of continuously working industries.

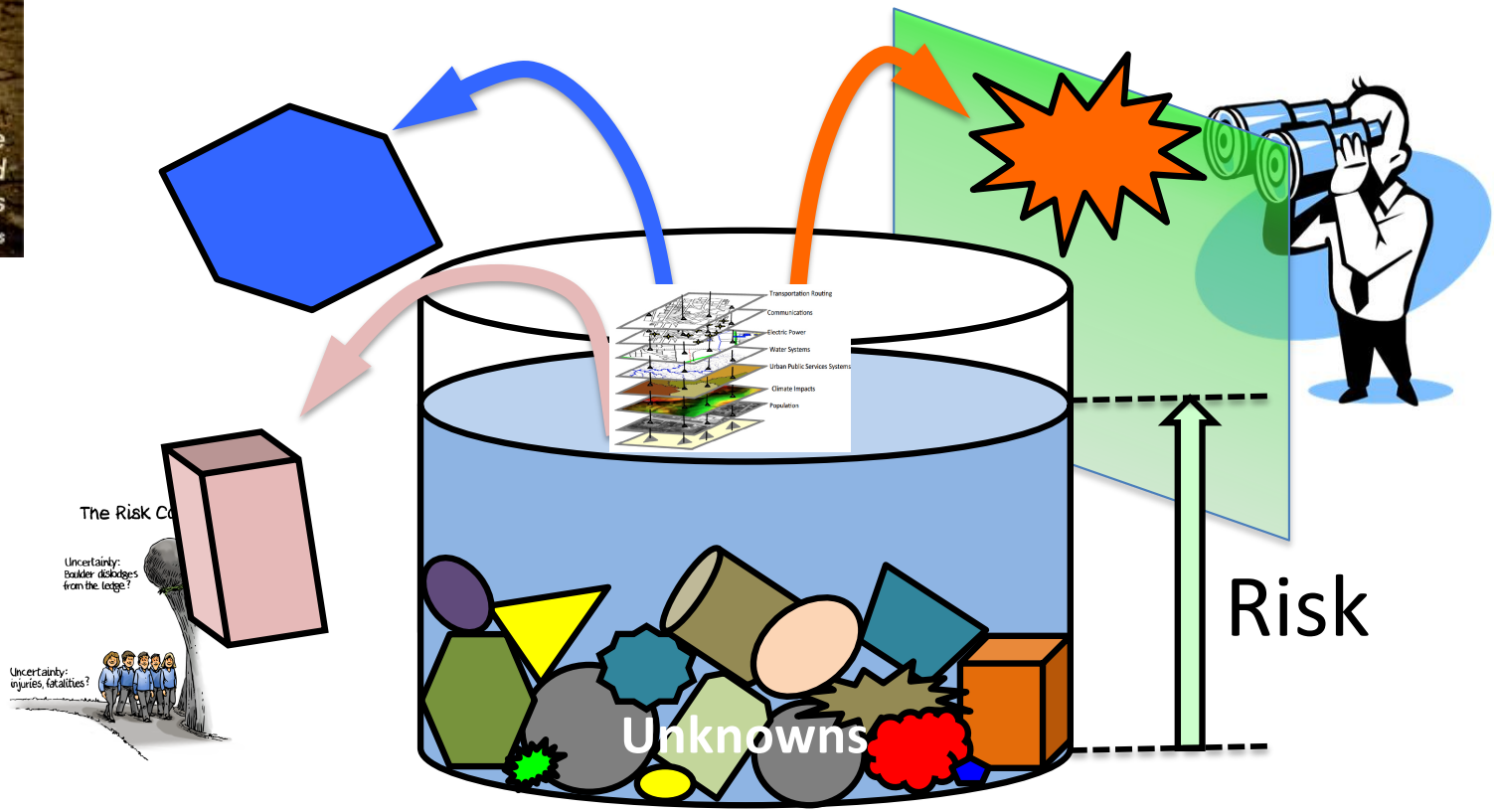
Impact on Dependent Critical Infrastructures - varying

- 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.

Italian Blackout, September 28, 2003

Risk Assessment and Management

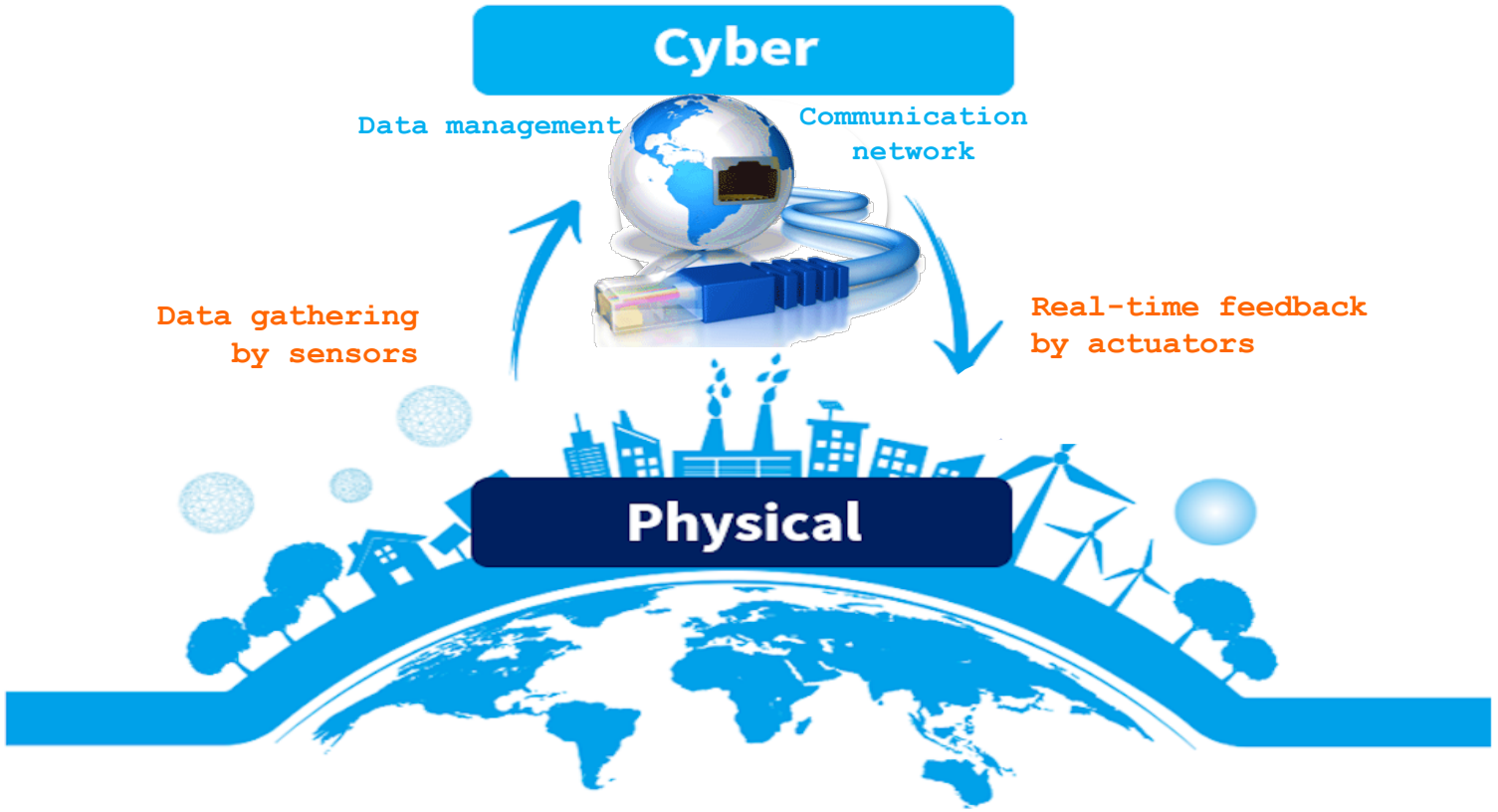




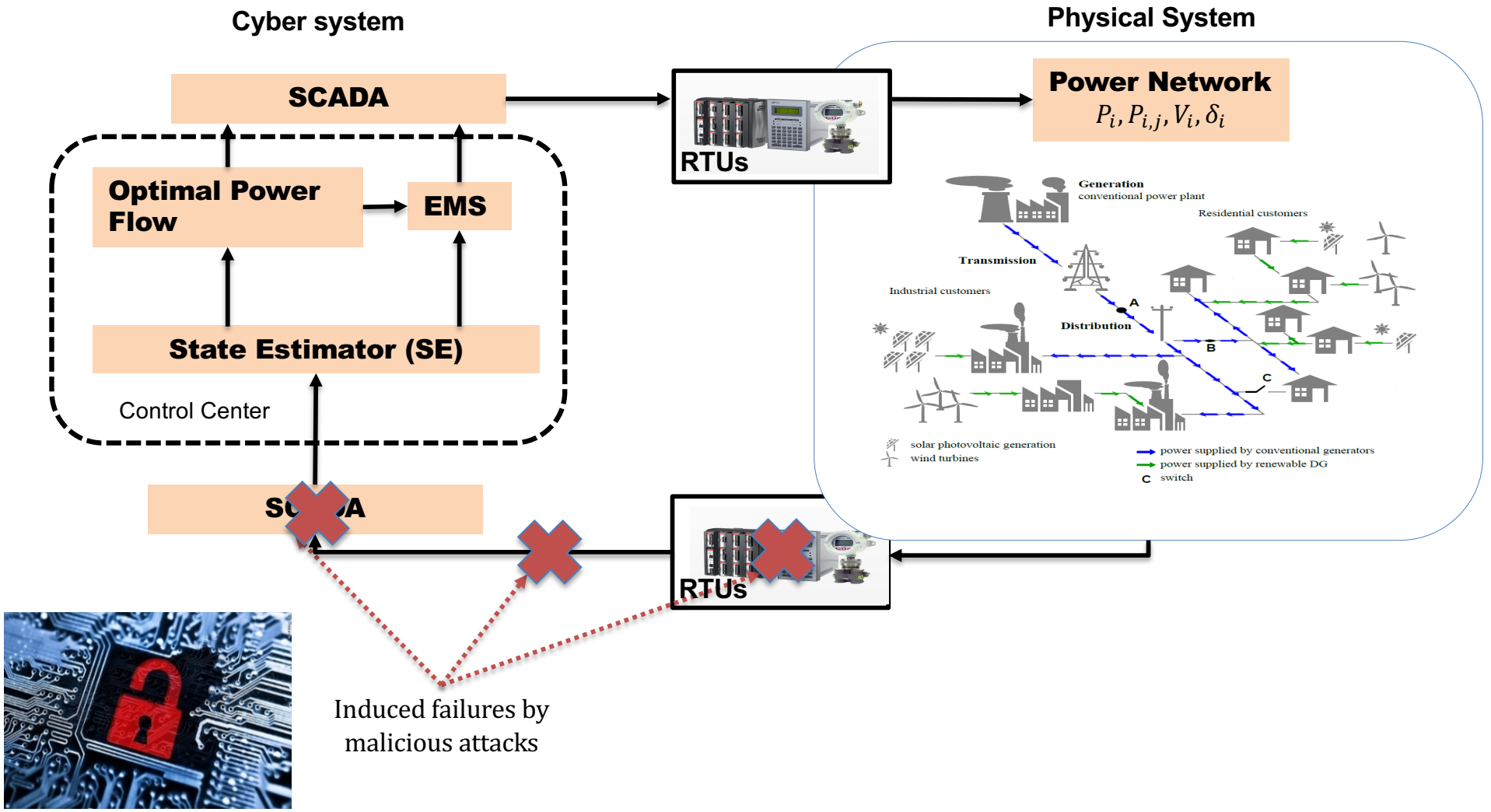
A. Yamaguchi, PSAM 12, 2016

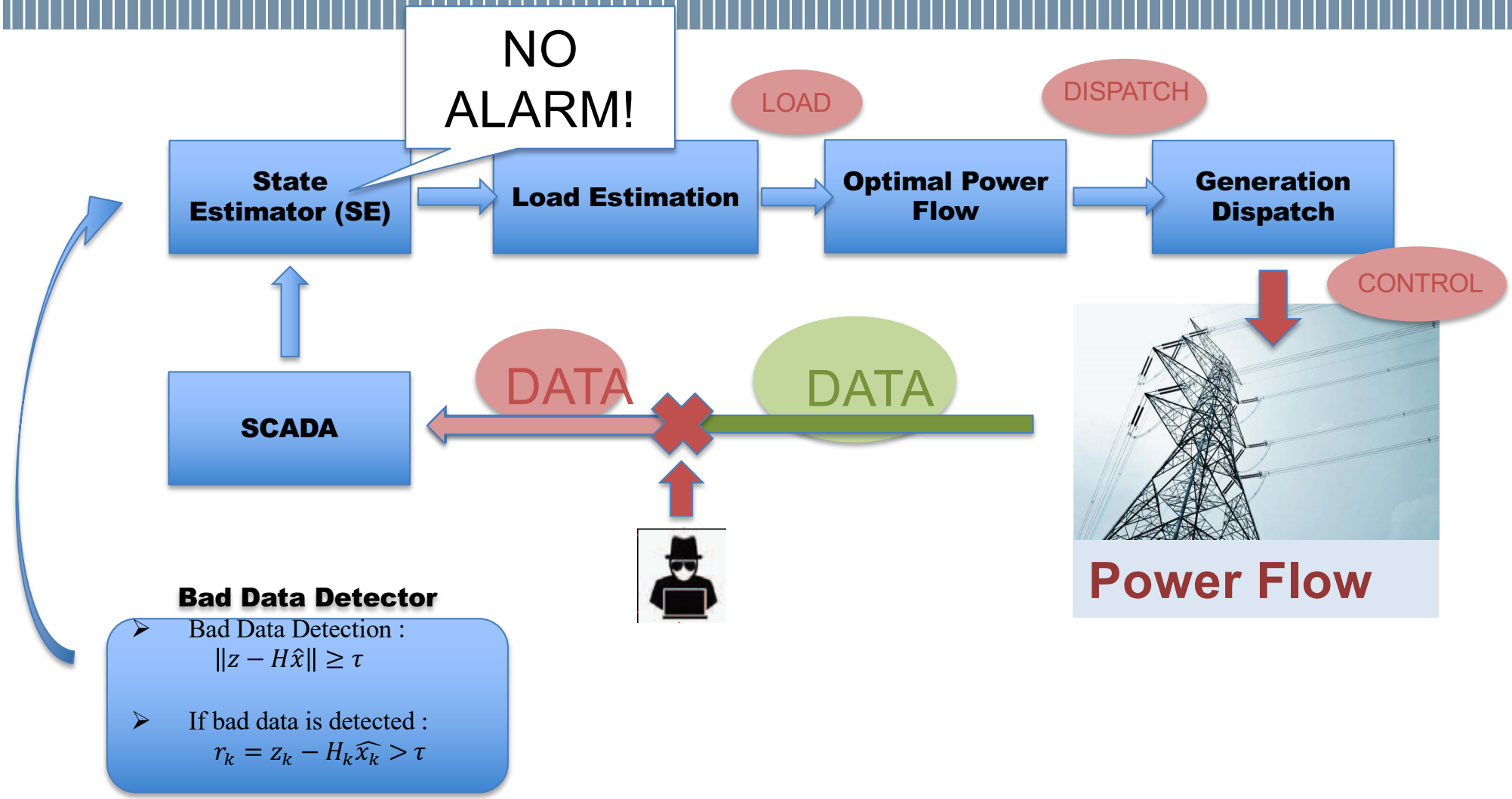
T. Aven and E. Zio, Foundational Issues in Risk Assessment and Risk Management, Risk Analysis, Vol. 34(7), 2014

World Risk Society: Risk Assessment of CPSs



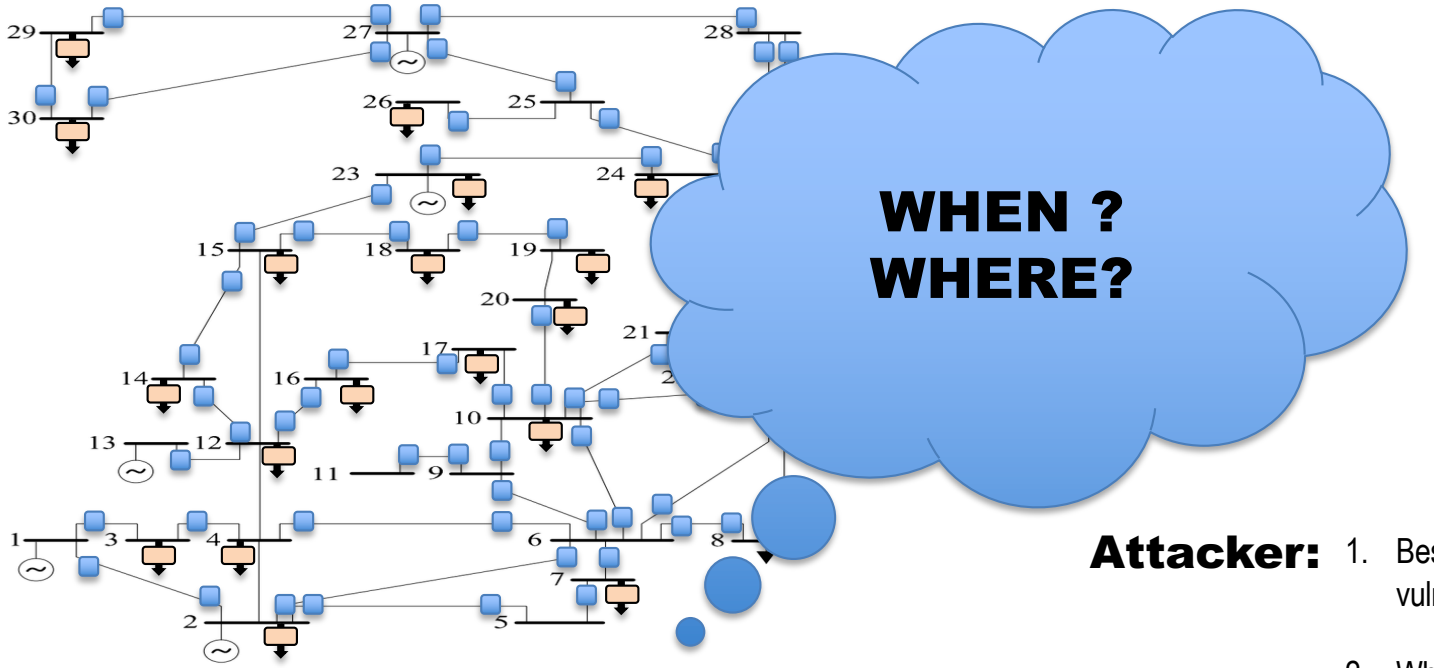
Risk Assessment of CPSs





✓ **DC approximation**: linearized equations model...

Risk Assessment of CPSs



WHEN ?
WHERE?

Attacker:

1. Best attack timing? When the grid is more vulnerable?
2. Which are the most vulnerable sensors ?

CPS for renewables energy application :

1. Grid condition favorable to cyber-attack.
2. Most vulnerable portion of the grid.
3. Renewables energy resources availability

Risk Assessment of CPSs

CYBER ATTACKS

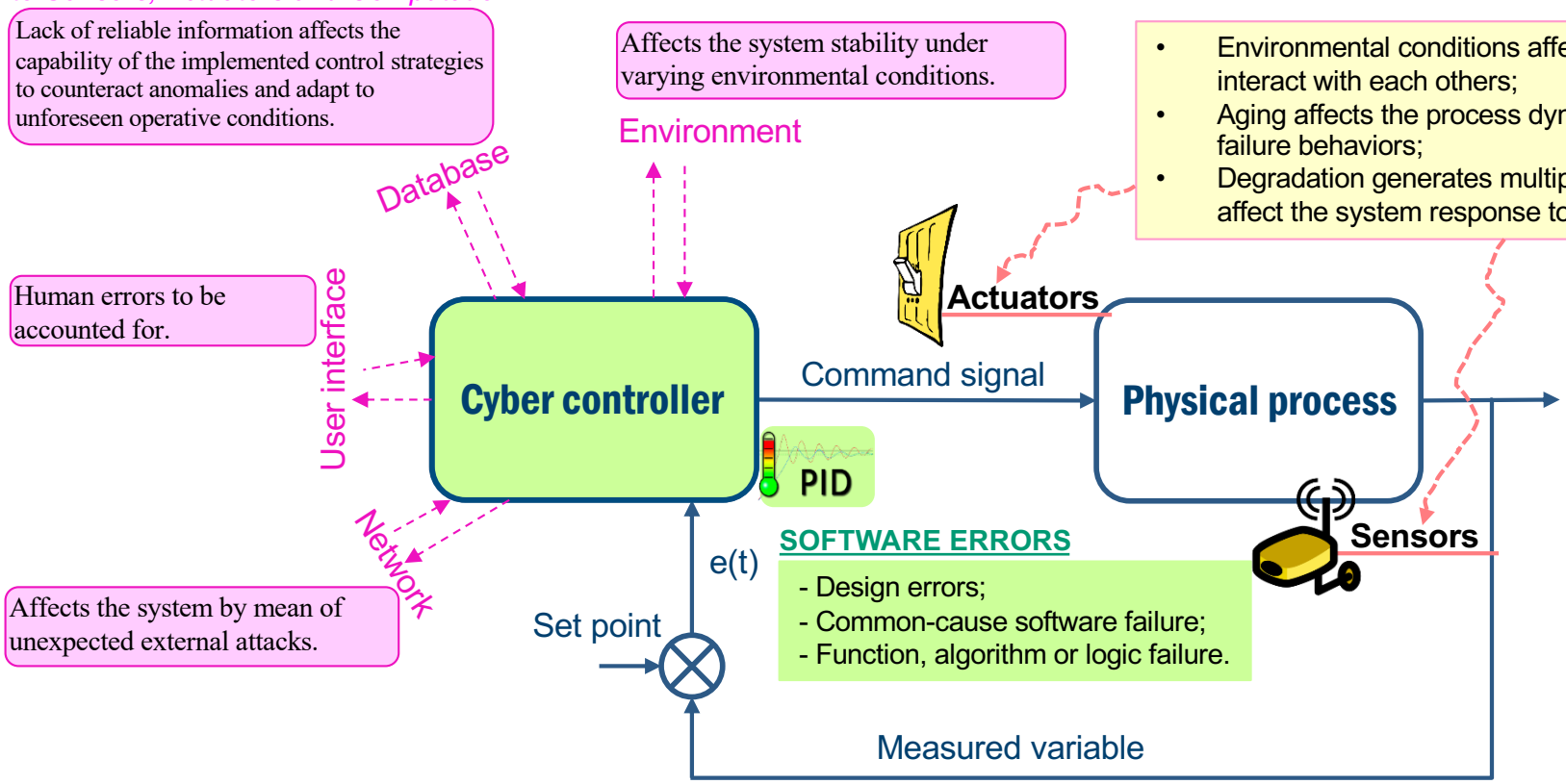
to Sensors, Actuators and Computation

Lack of reliable information affects the capability of the implemented control strategies to counteract anomalies and adapt to unforeseen operative conditions.

Affects the system stability under varying environmental conditions.

COMPONENT FAILURES

- Environmental conditions affect the way components interact with each others;
- Aging affects the process dynamics of the hardware failure behaviors;
- Degradation generates multiple failure modes which affect the system response to different stimuli.



UNCERTAINTIES IN SAFETY ANALYSIS: How to build confidence in safety decisions?

Risk assessment of CPSs

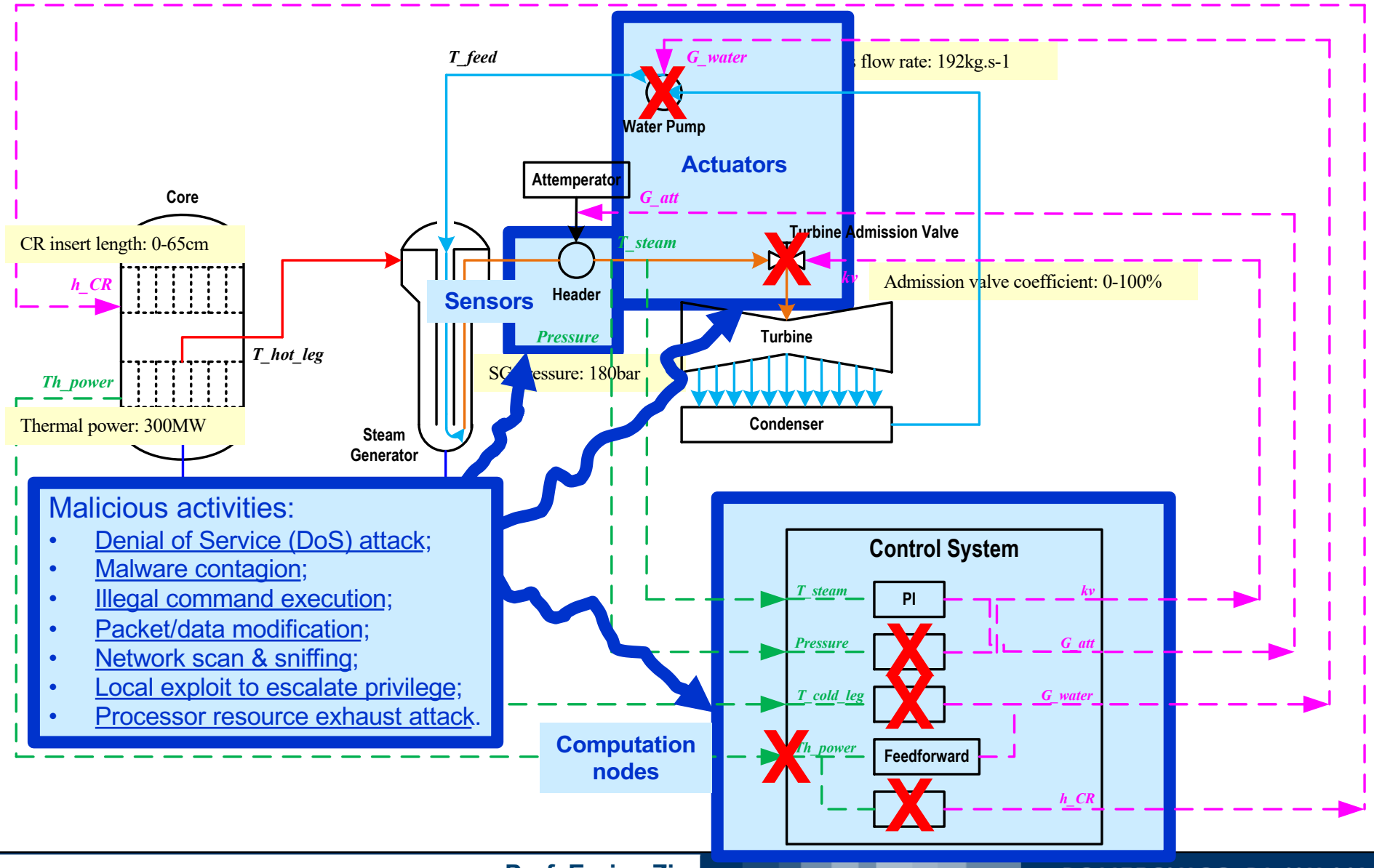
Cyber attack ⟷ Component failure & software error

Digital I&C Systems in NPPs

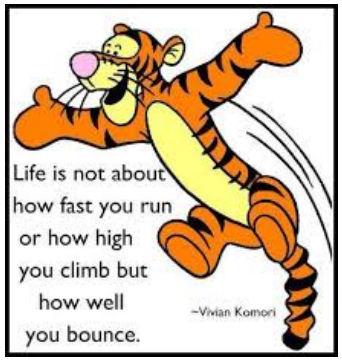
VULNERABILITIES IN SECURITY ANALYSIS: How to build confidence in security solutions?

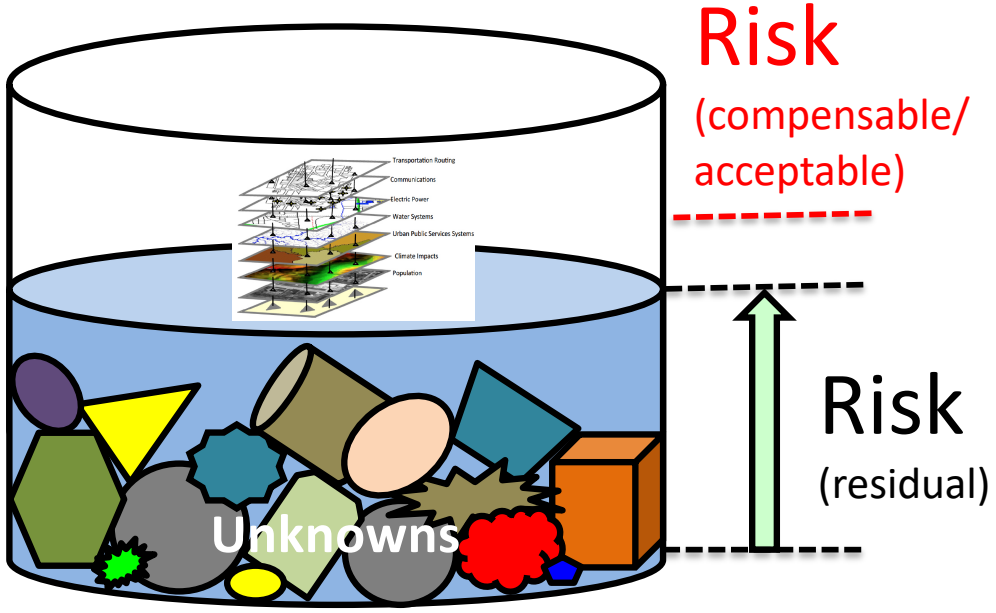
Risk Assessment of CPSs

Modeling and simulation of cyber threats



Risk Assessment and Management

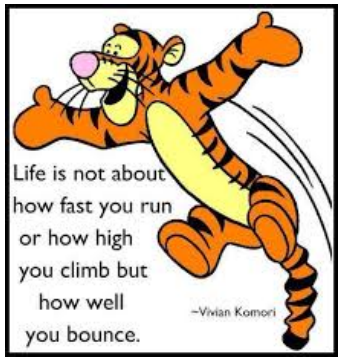




A. Yamaguchi, PSAM 12, 2016

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

From risk prevention/mitigation to resilience



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!!!

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***)

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.

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)

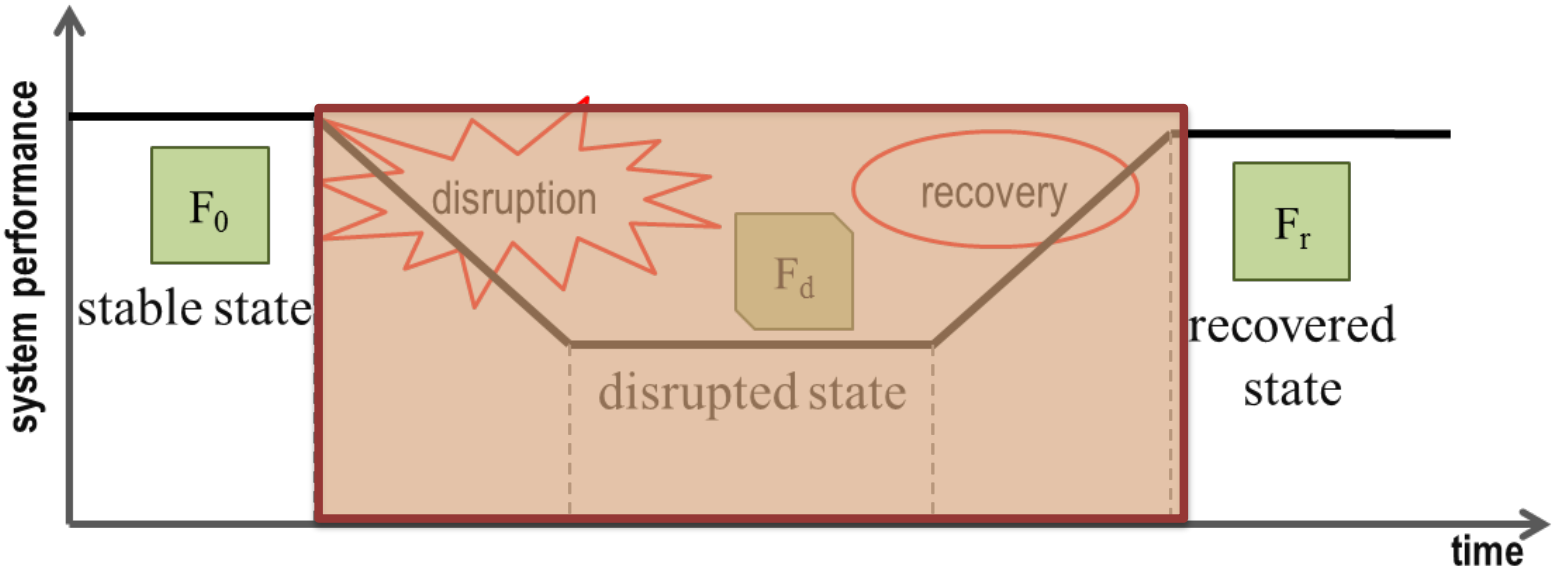
"The ability of a system to **sustain** external and internal **disruptions** without discontinuity of performing the system's function or, if the function is disconnected, to fully **recover** the function rapidly" (US ASME 2009)

"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)

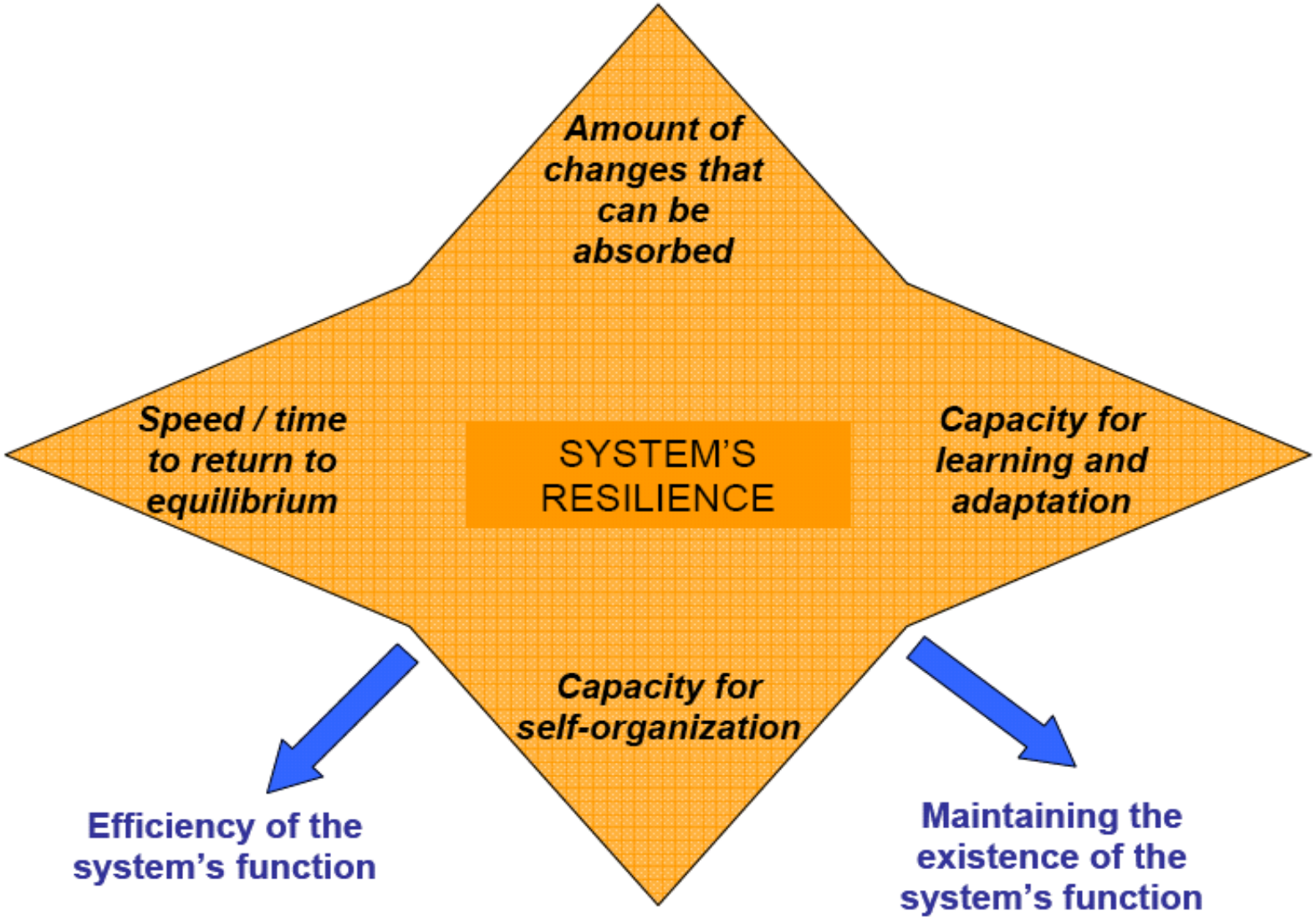
…

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



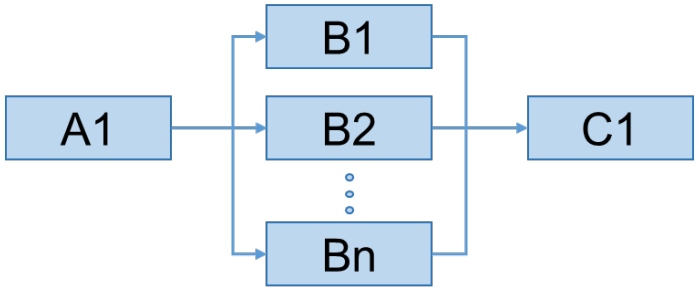
Features of system's resilience

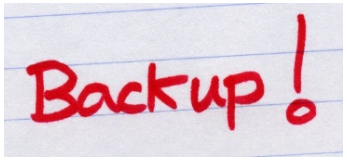
4R framework

Robustness, **R**apidity

Redundancy

- Physical
- Operational





Resourcefulness

- Technical
- Organizational

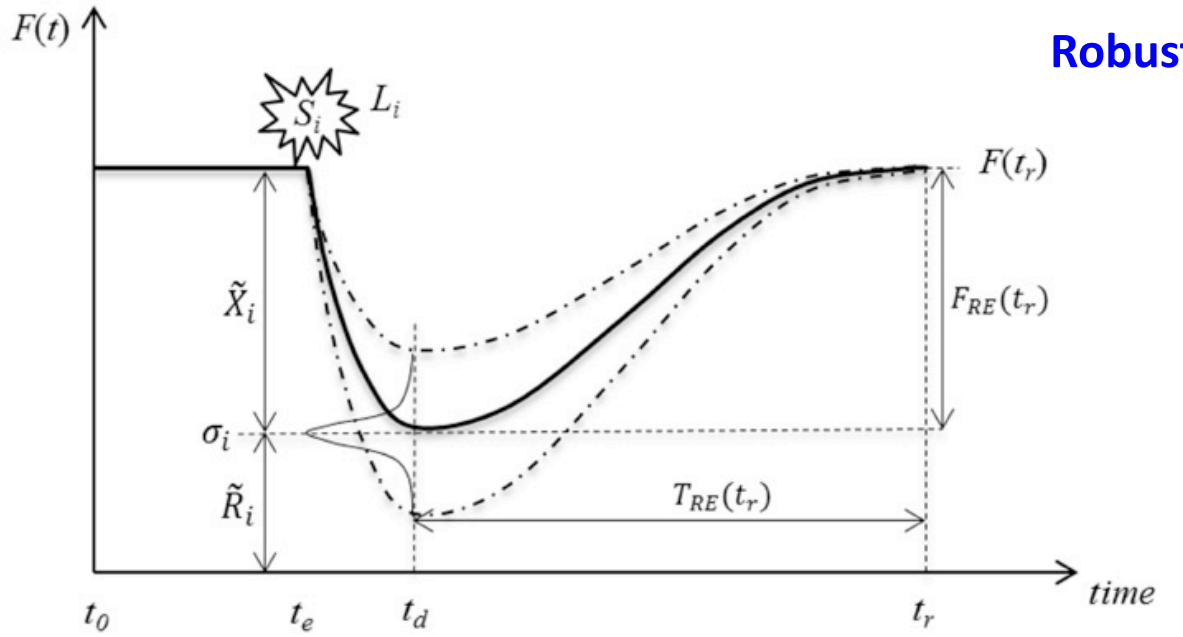
What is system resilience?

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

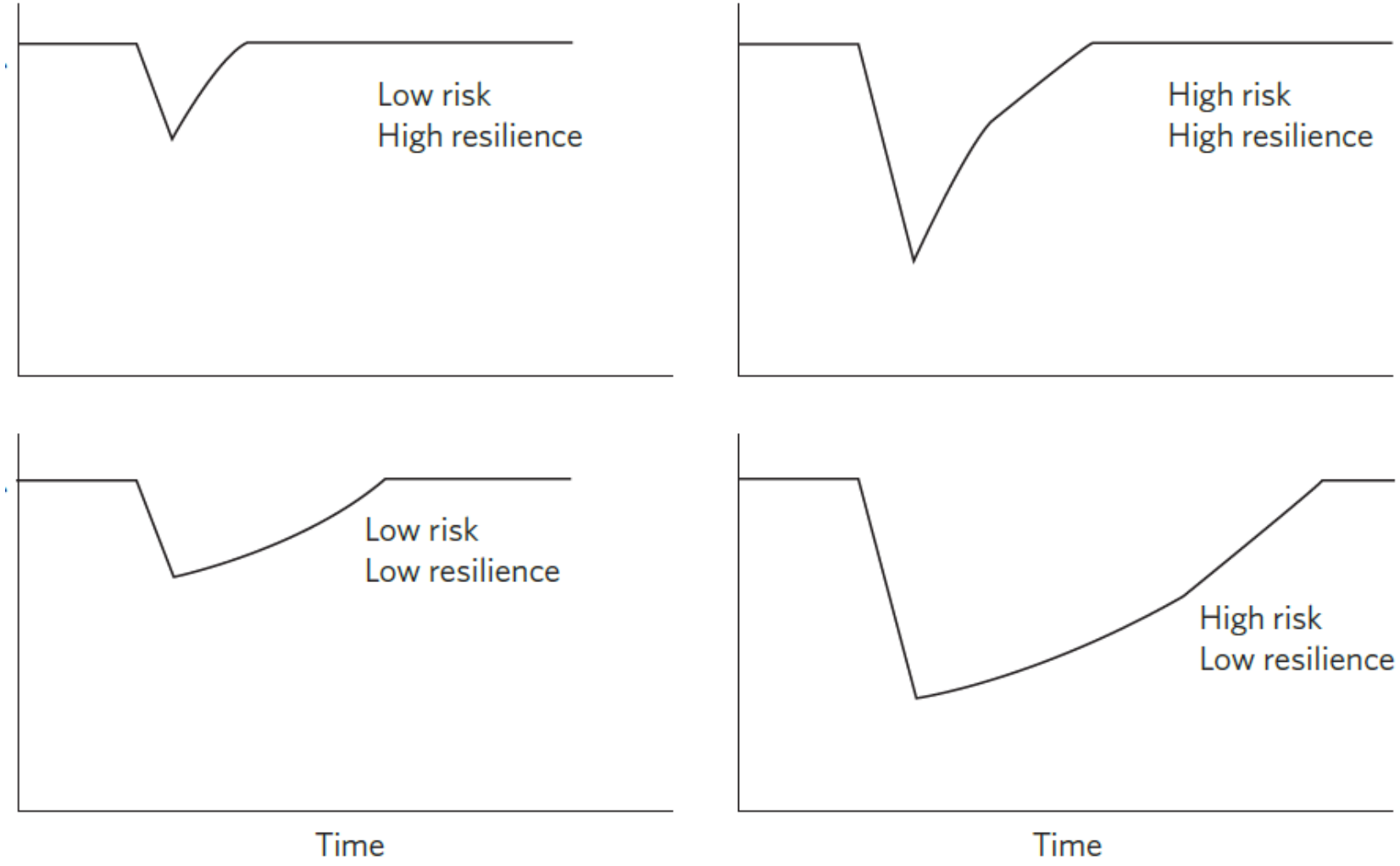
Robustness = $\left\{\left\langle \tilde{R}_i\right\rangle\right\} = \left\{\left\langle F(t_0) - \tilde{X}_i(\sigma_i)\right\rangle\right\}$

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

Robustness Recovery Rapidity



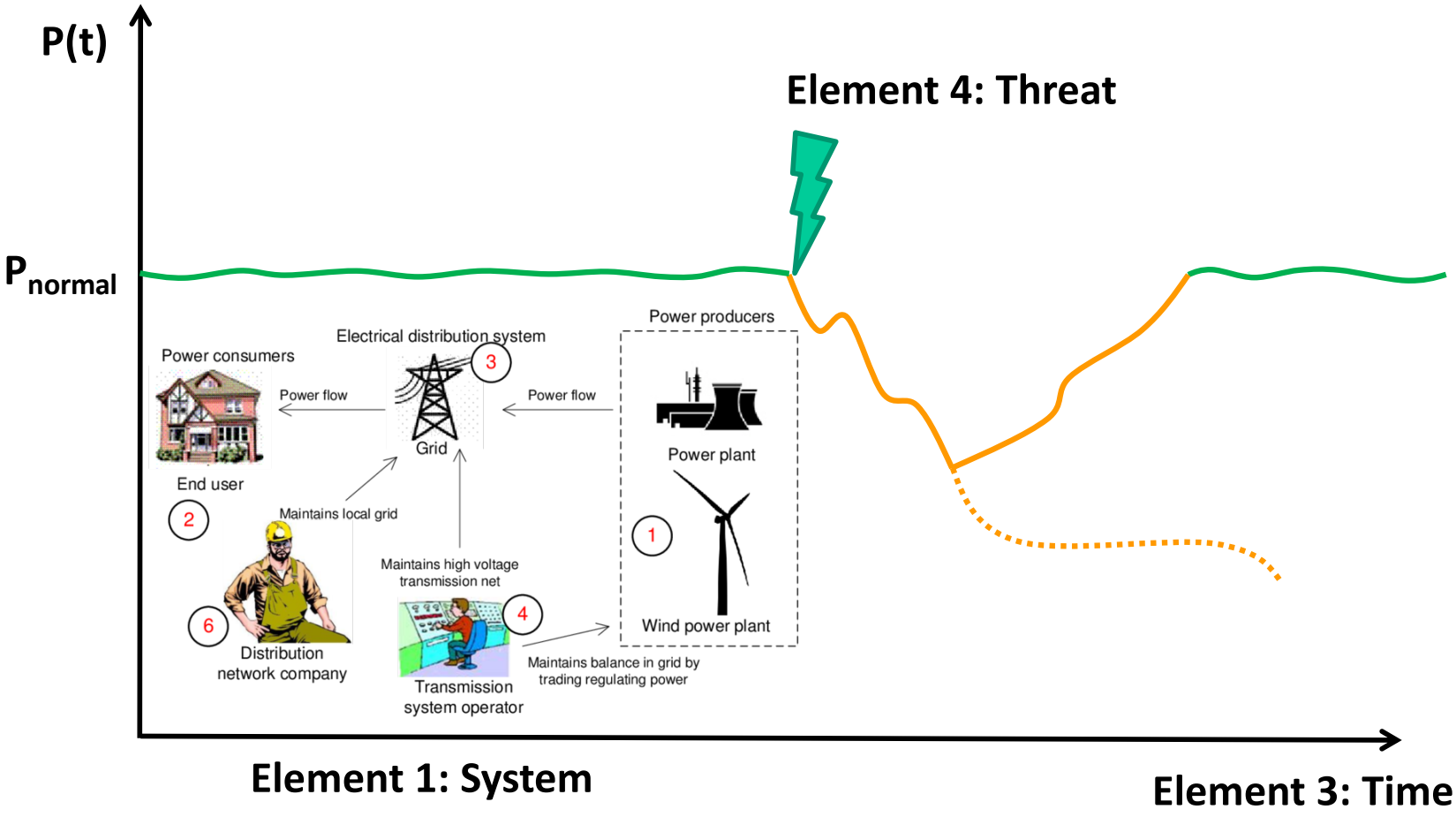
Resilience vs. risk



CI resilience quantification and assessment

Basic elements

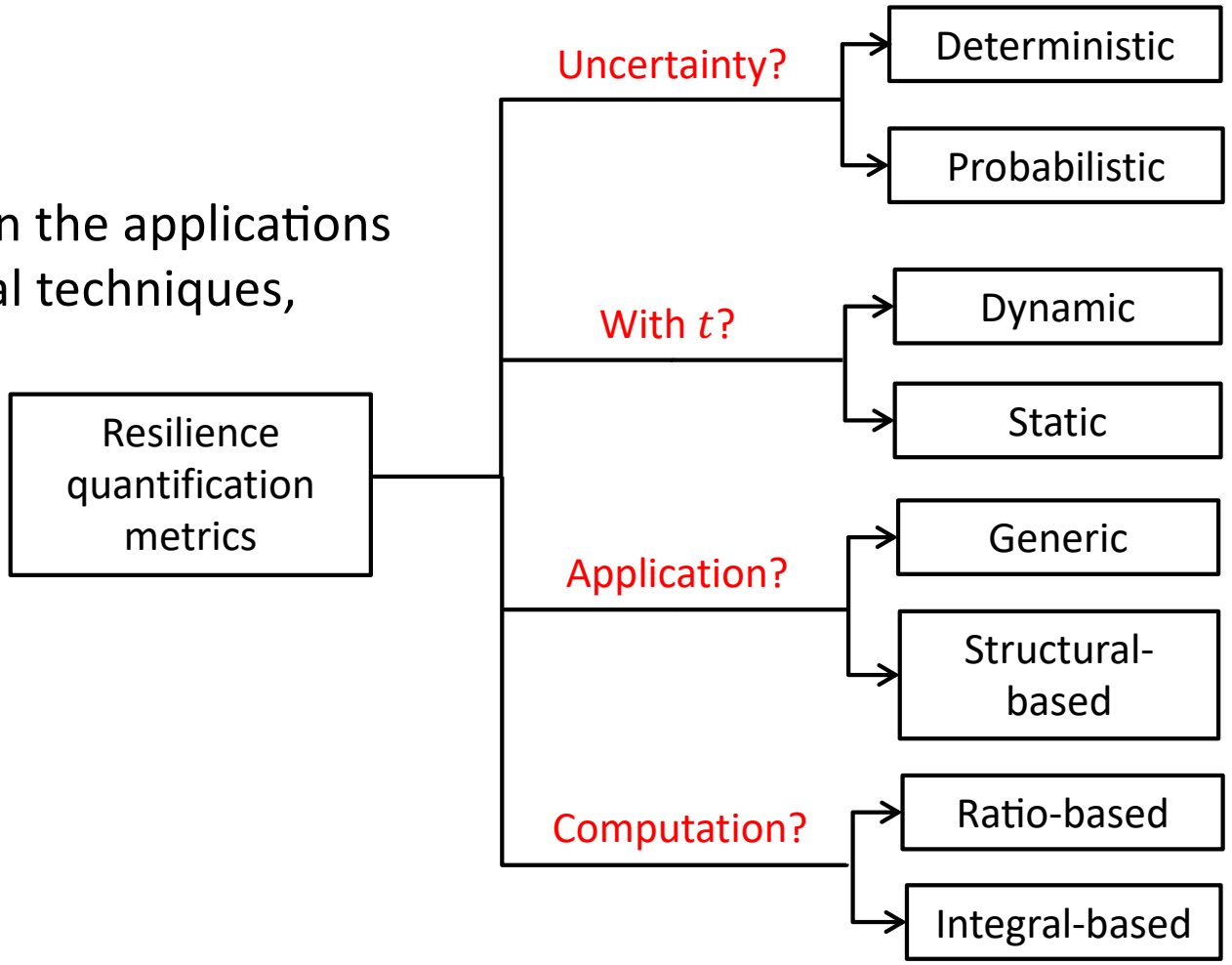
Element 2: Quality of Performance



CI resilience quantification and assessment

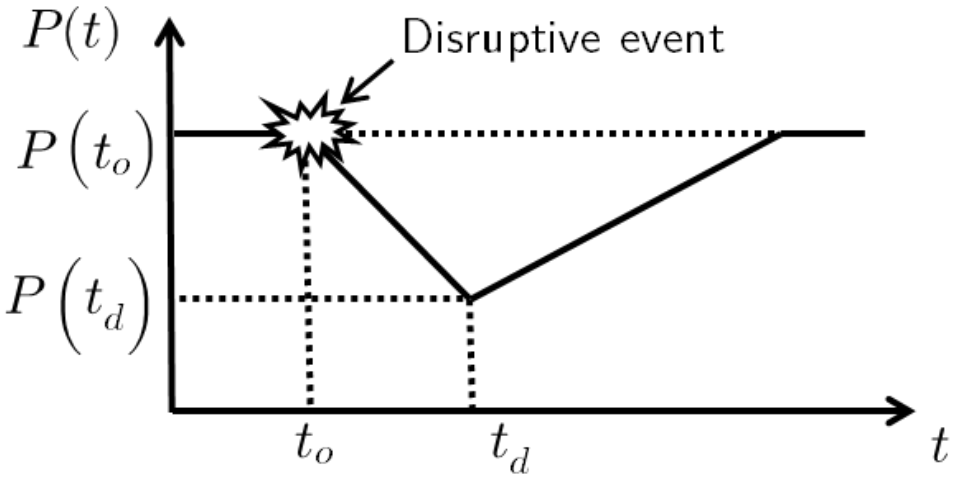
Resilience metrics

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



Resilience metric 1 (Henry and Ramirez-Marquez 2012)

$$\boldsymbol{R}(t) = \frac{P(t) - P\left(t_d\right)}{P\left(t_o\right) - P\left(t_d\right)}, \quad t \geq t_d$$



→ $\boldsymbol{R}(t)$: system resilience at time t under a disruptive event

→ $P(t)$ system performance function

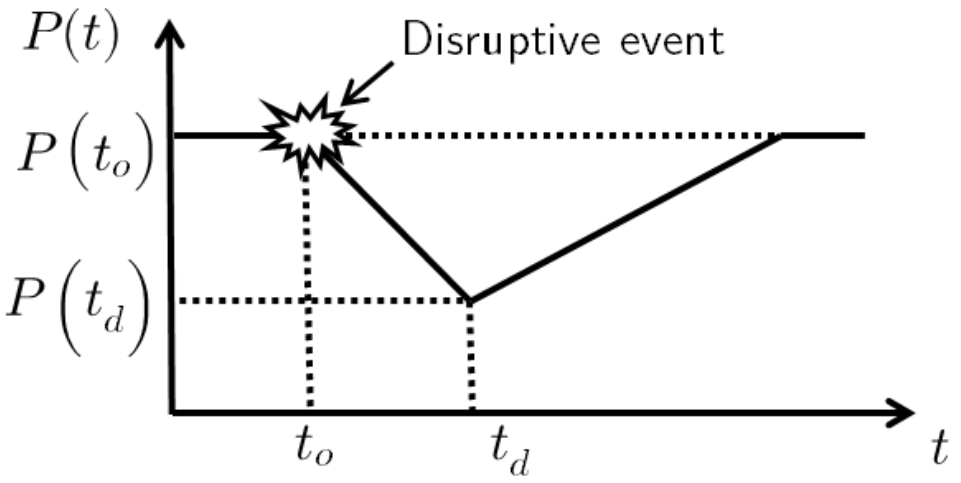
→ t_o: the time when the external disruptive event occurs

→ t_d: the time when system performance reaches its lowest level

Ratio of the recovered performance up to time t to the total loss of system performance due to a certain disruptive event.

Resilience metric 1 (Henry and Ramirez-Marquez 2012)

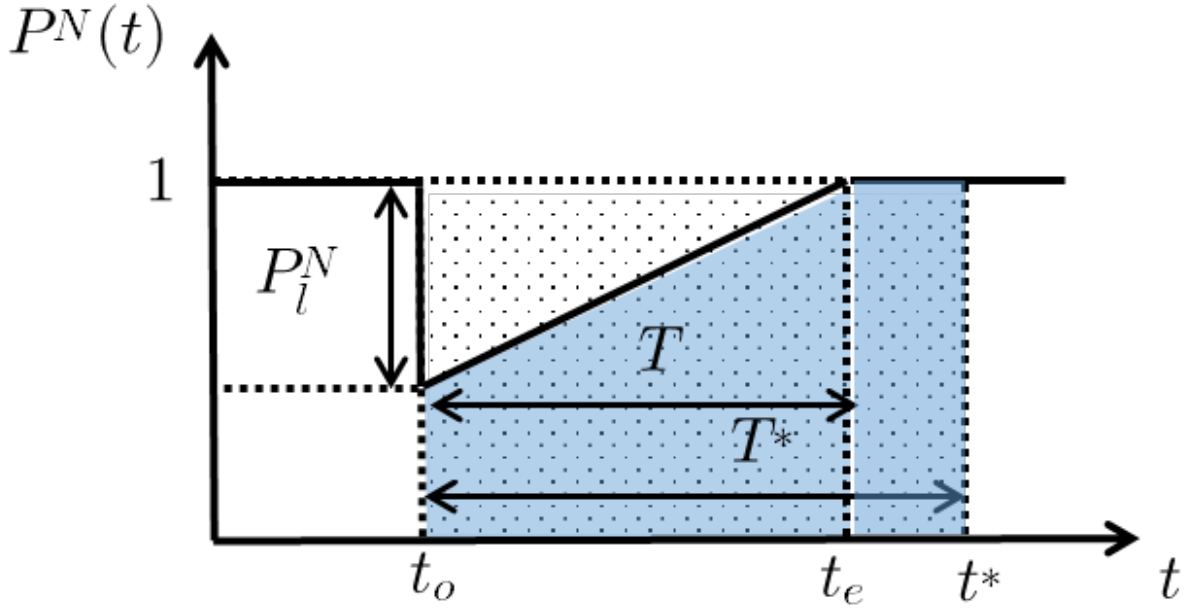
$$\boldsymbol{R}(t) = \frac{P(t) - P\left(t_d\right)}{P\left(t_o\right) - P\left(t_d\right)}, t \geq t_d$$



- Deterministic, dynamic, ratio-based
- $P(t)$ could be higher than $P(t_o)$, therefore $\boldsymbol{R}(t)$ could be >1

Resilience metric 2 (Zobel 2011)

$$\boldsymbol{R} = \frac{T^* - P_l^N \cdot T/2}{T^*} = 1 - \frac{P_l^N T}{2T^*}$$



→ $P^N(t)$: normalized system performance function

→ P_l^N: loss of normalized system performance after a disruption

→ t_o: the instant when the external disruptive event occurs

→ t_e: the instant when the system performance returns to original level

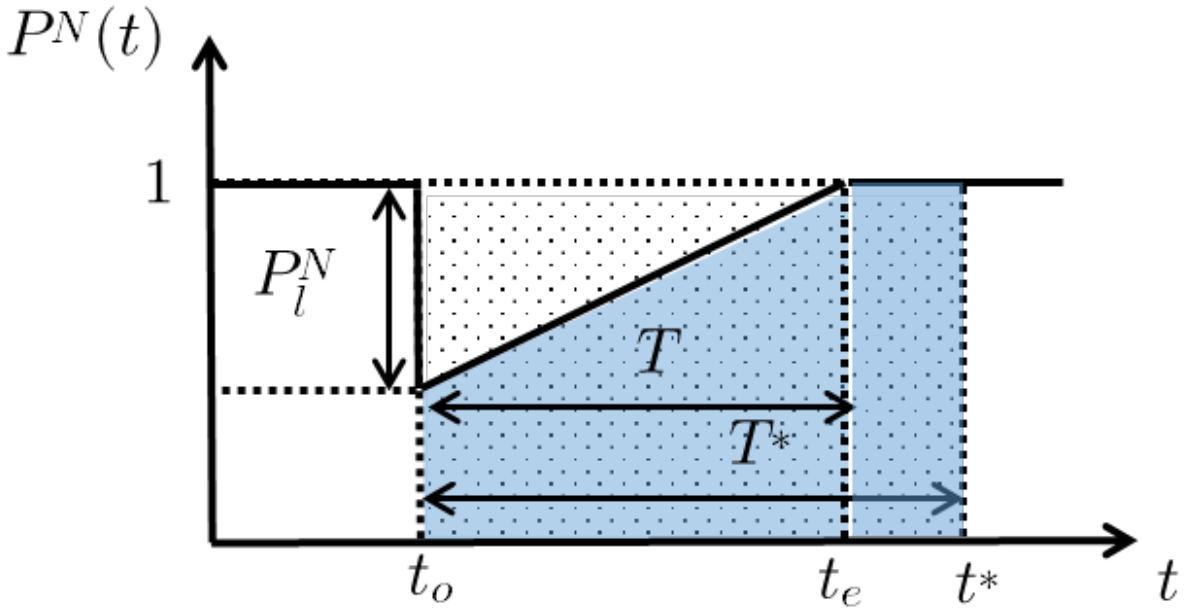
→ t^*: a strict upper bound for restoration time t

→ $T = t_e - t_o$ and $T^* = t^* - t_o$.

Resilience metric 2 (Zobel 2011)

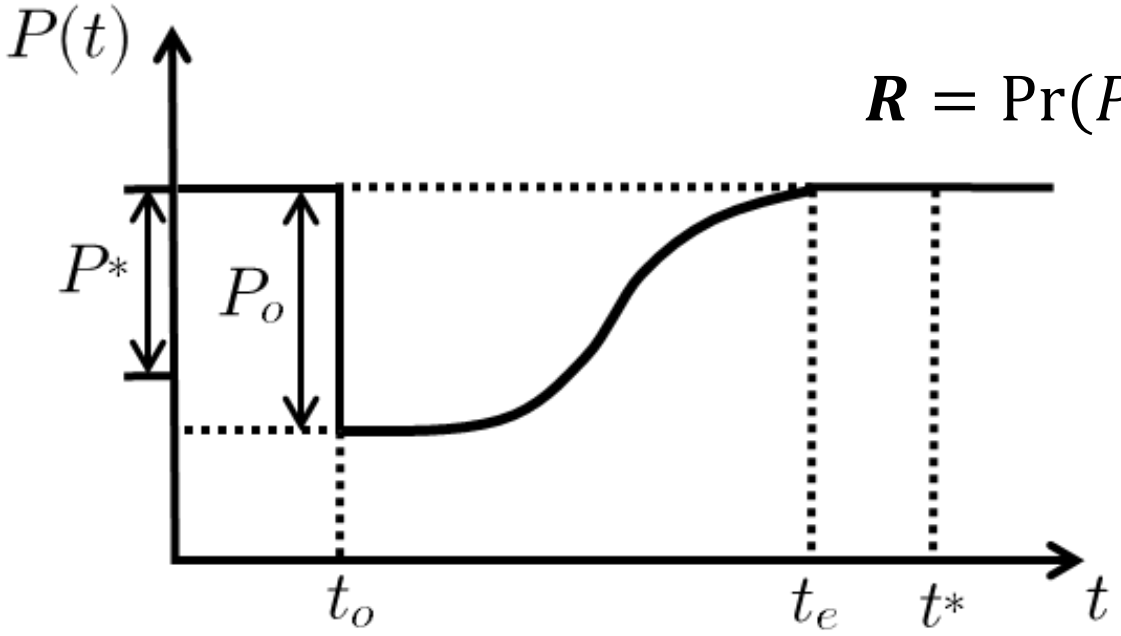
$$\boldsymbol{R} = \frac{T^* - P_l^N \cdot T/2}{T^*}$$

$$= 1 - \frac{P_l^N T}{2T^*}$$



- Ratio of the area between the system performance curve and the time axis and the area between the desired performance (=1) and the time axis
- Deterministic, static, ratio-based
- Considers both the loss of performance and the length of recovery

Resilience metric 3 (Chang & Shinozuka 2004)



$$\boldsymbol{R} = \Pr(P_o > P^* \text{ and } t_e < t^*)$$

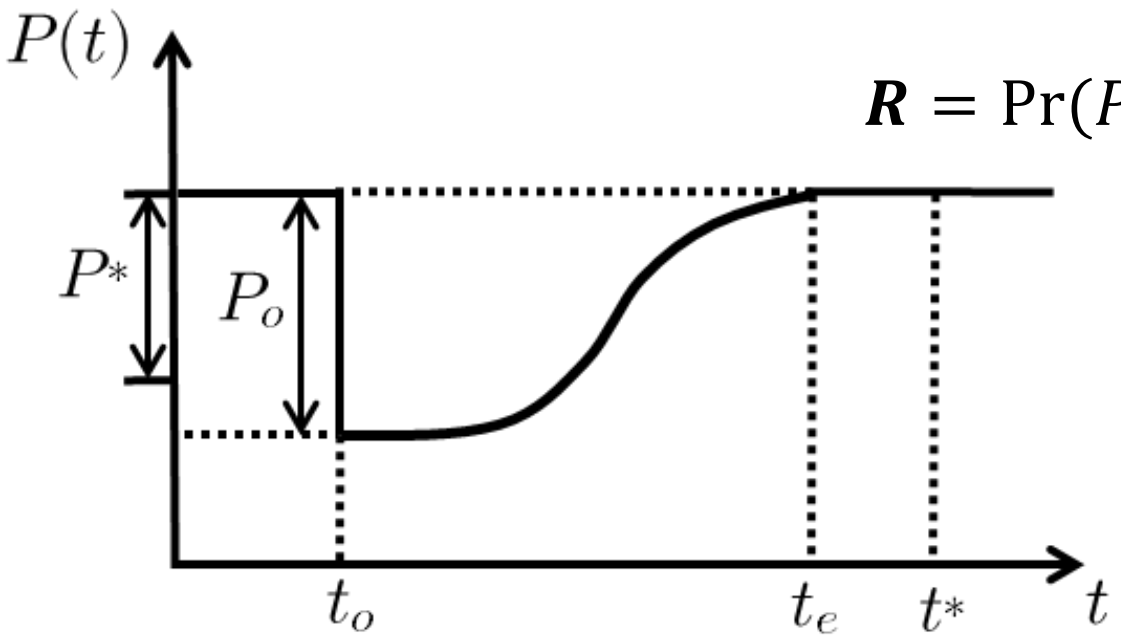
→ P_o: the initial system performance loss after a disruption, i.e., the largest loss during the disruptive event

→ P^*: the maximum acceptable loss of system performance

→ t_e: the time when the system performance returns to its original level

→ t^*: the maximum acceptable system recovery instant

Resilience metric 3 (Chang & Shinozuka 2004)

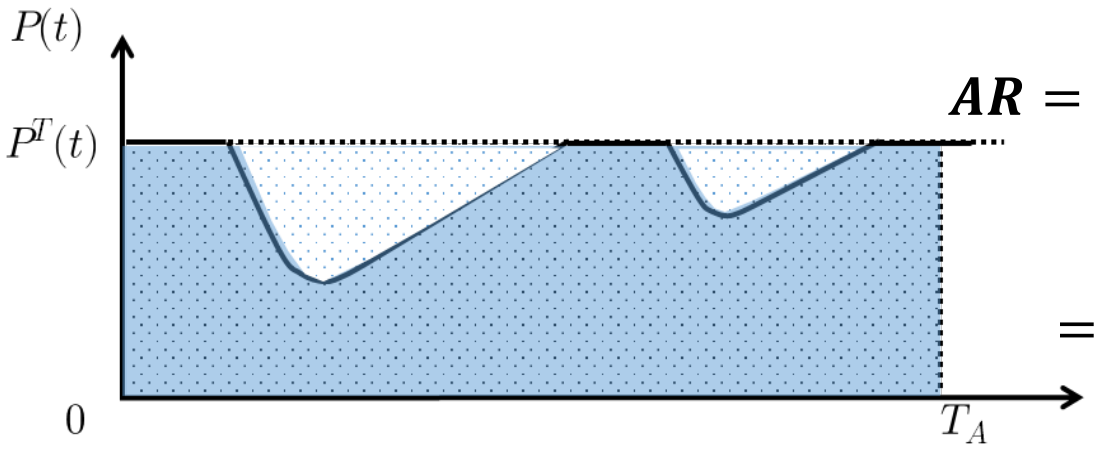


$$\boldsymbol{R} = \Pr(P_o > P^* \text{ and } t_e < t^*)$$

- Probabilistic metric (considers uncertainty of the process)
- Taking into account both the loss of performance and the length of recovery

Resilience metric

Resilience metric 4 (Ouyang 2014)



$$\boldsymbol{AR} = E\left[\frac{\int_0^{T_A} P(t)dt}{\int_0^{T_A} P^T(t)dt}\right]$$

$$= E\left[\frac{\int_0^{T_A} P^T(t)dt - \sum_{n=1}^{N(T_A)} AIA_n(t_n)}{\int_0^{T_A} P^T(t)dt}\right]$$

- Annual system resilience
- Measuring the **mean** ratio of the area between the system performance curve and the time axis to the area between the target performance curve and the time axis during a year
- Probabilistic, integration-based and ratio-based
- Taking into account multiple disruptive events

Resilience metric

	Value	Data required in system performance (SP) dimension	Data required in time dimension	Feature/advantage in the application
Metric 1 $\boldsymbol{R}(t) = \frac{P(t) - P(t_d)}{P(t_o) - P(t_d)}$	Function of time	$P(t)$: SP function	t_o and t_d	It is actually a normalized SP function
Metric 2 $\boldsymbol{R} = 1 - \frac{P_l^N T}{2T^*}$	Single value $\in [0,1]$	The lowest value of the normalized SP.	t_o, t_e, and t^*	Provide a rough estimation based on relatively less information
Metric 3 $\boldsymbol{R} = \int_{t_0}^{t_e} \frac{P^N(t)}{T_{RE}} dt$	Single value $\in [0,1]$	$P^N(t)$: the normalized SP function of time	t_o and t_e	Including more information of SP
Metric 4 $\boldsymbol{R} = \Pr(P_o < P^* \cap t_e < t^*)$	Single value Probability	SP value at a critical time instant	t_e and t^*	Taking into account the uncertainty of the event or system

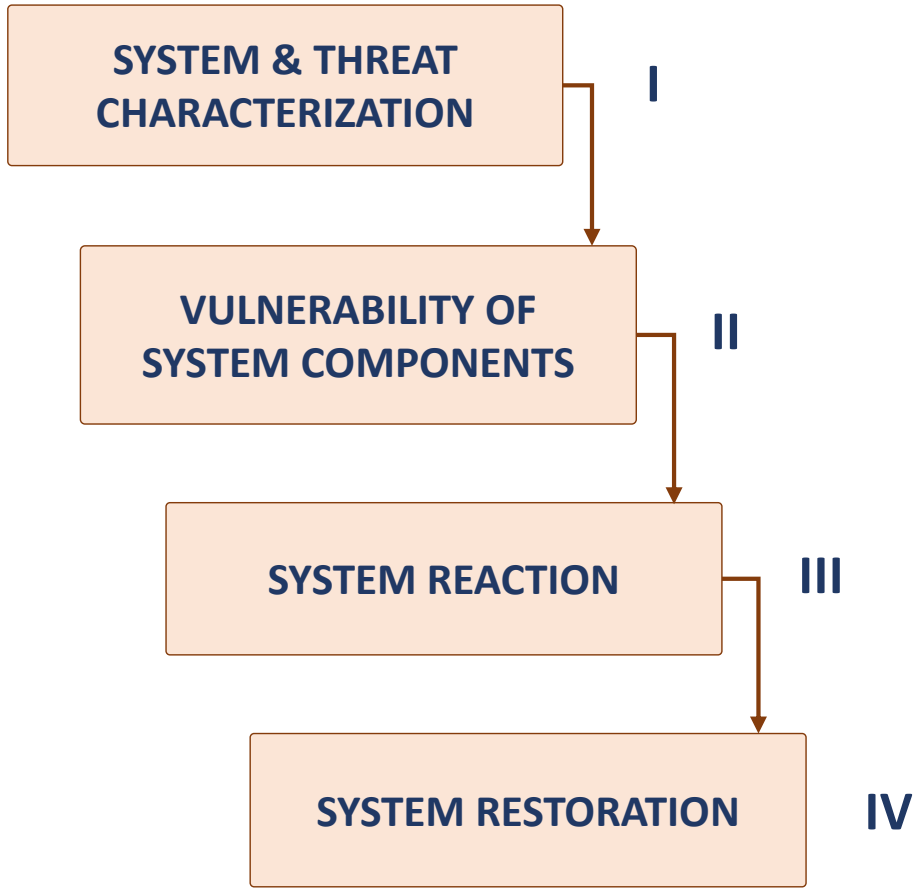
- Their uses depend on the applications and available data

Resilience assessment framework

Resilience assessment

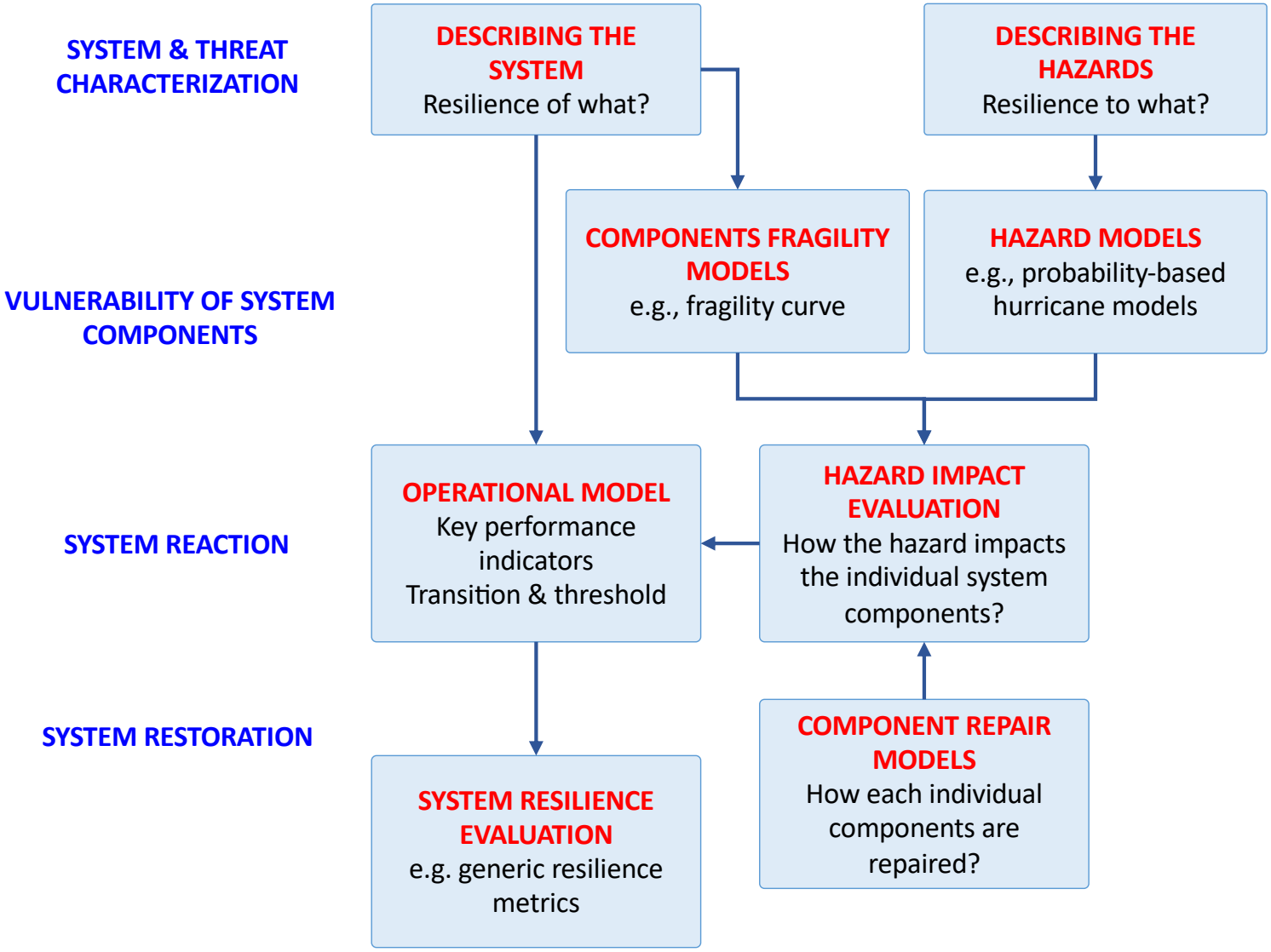
Simulation-based resilience assessment framework

- **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

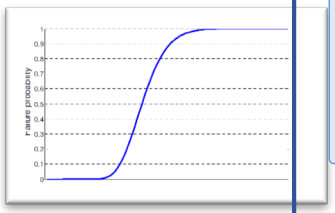


Resilience assessment

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

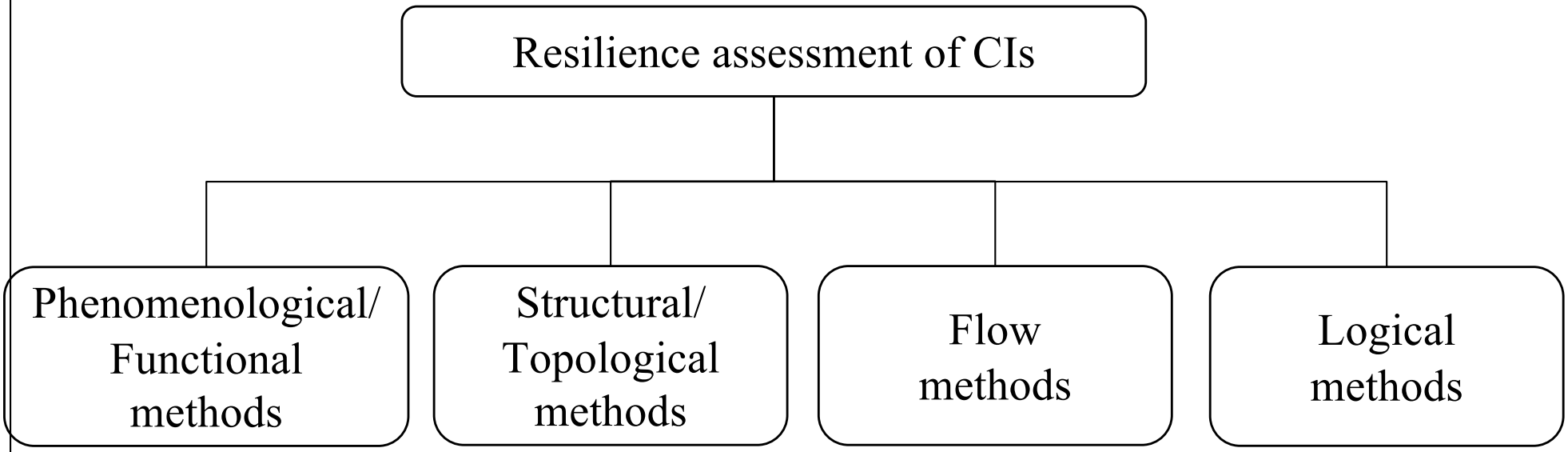
SYSTEM RESILEINCE EVALUTION
e.g. generic resilience metrics

COMPONENT REPAIR MODELS
How each individual components are repaired?

- Probability distribution of the restoration time

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

Methods



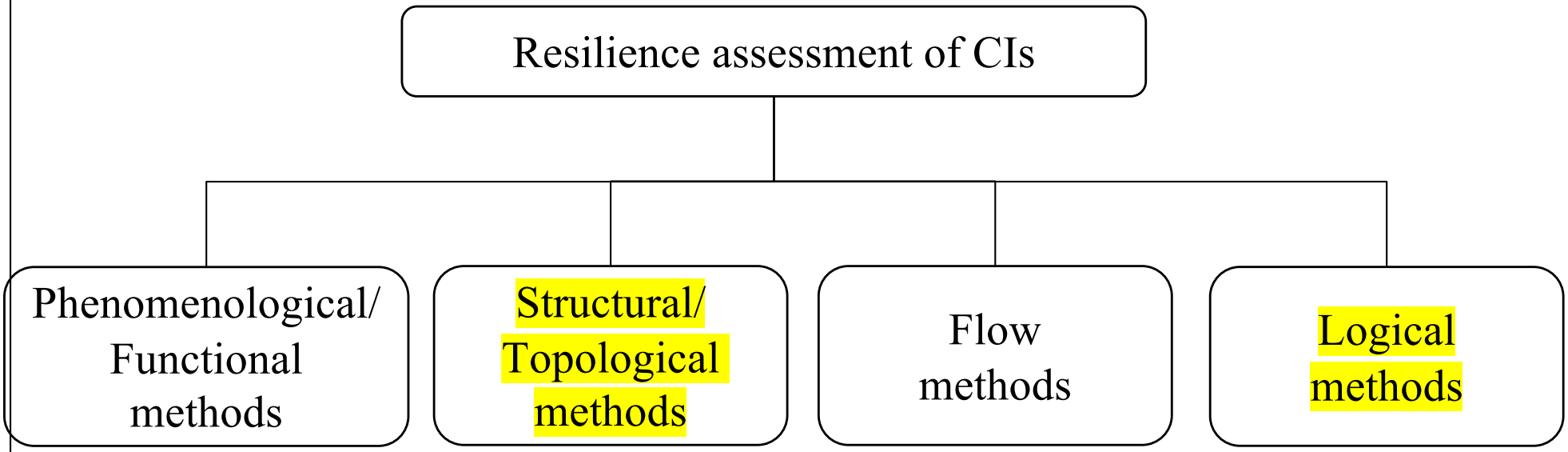
e.g., Agent Based Modeling and Simulation, System Dynamic Model, Economic-Based Approaches, …

e.g., Topology-based approaches

e.g., Flow-based approaches (maximum flow model, …)

e.g., Risk Analysis (fault/event trees, …), Probabilistic Modeling (Markov Chains, Bayesian network, …)

Methods



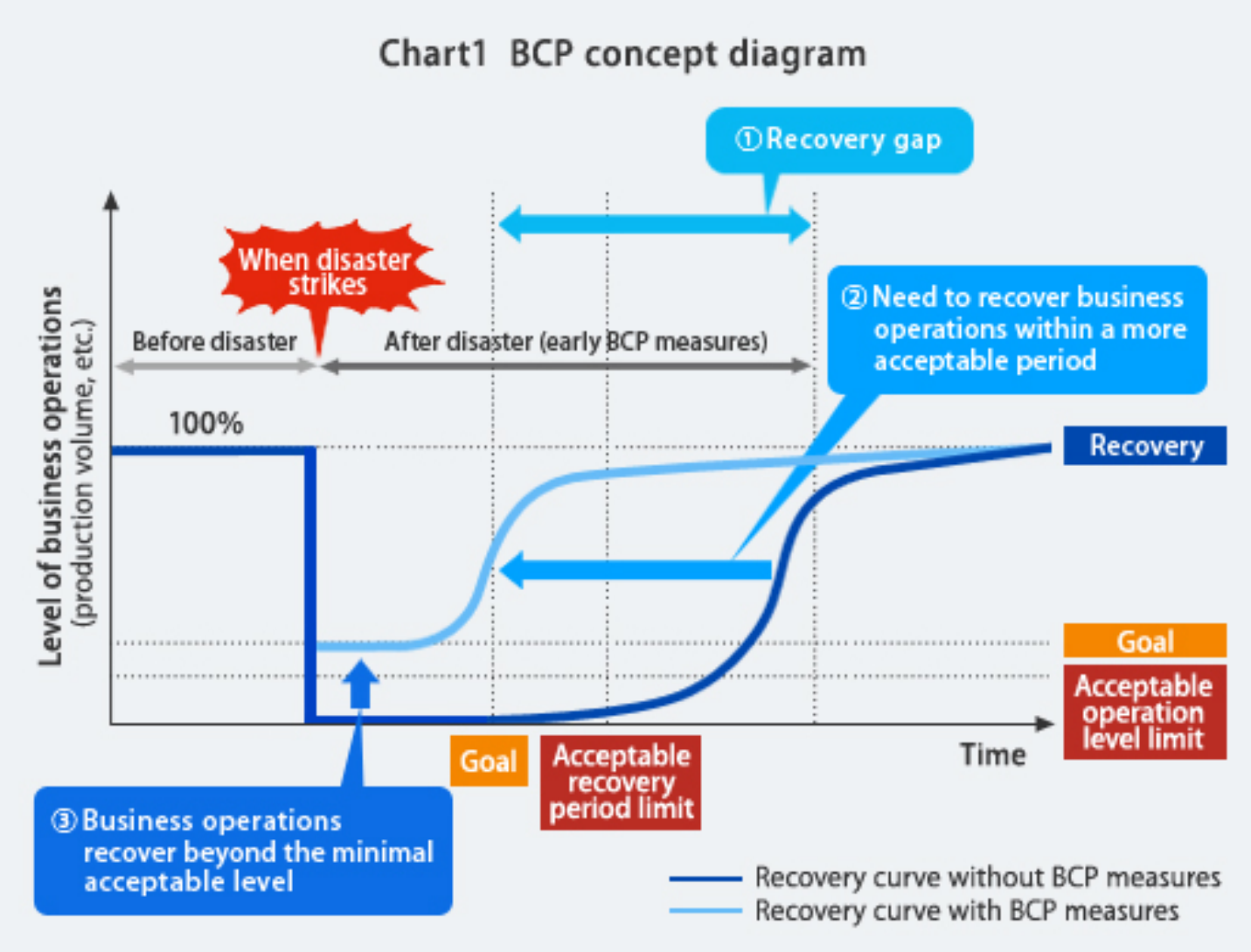
e.g., Agent Based Modeling and Simulation, System Dynamic Model, Economic-Based Approaches, …

e.g., Topology-based approaches

e.g., Flow-based approaches (maximum flow model, …)

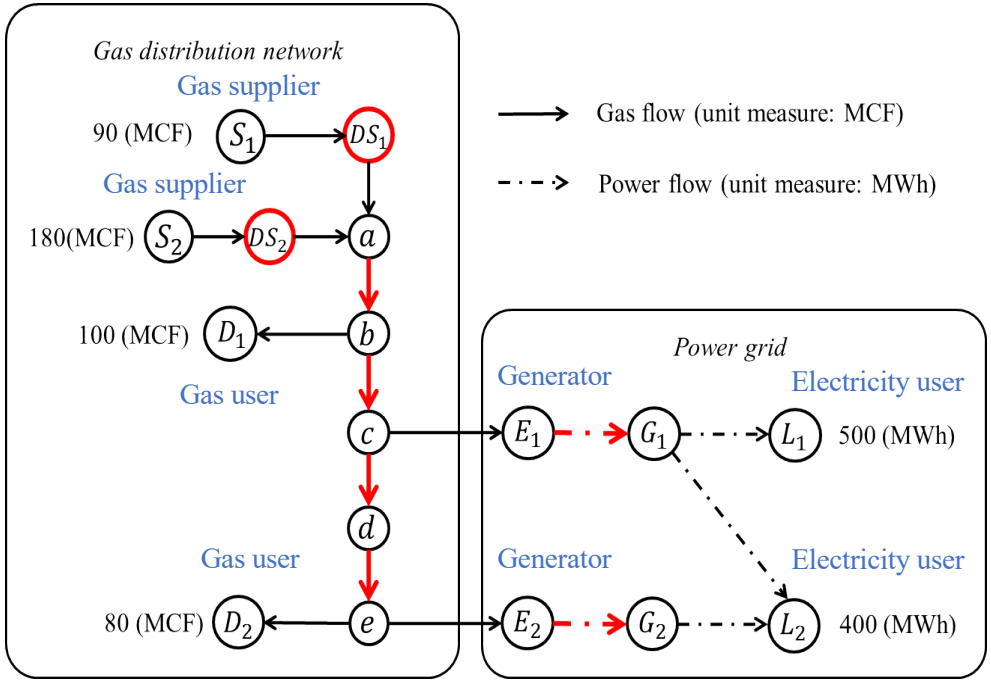
e.g., Risk Analysis (fault/event trees, …), Probabilistic Modeling (Markov Chains, Bayesian network, …)

Resilience improvement



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

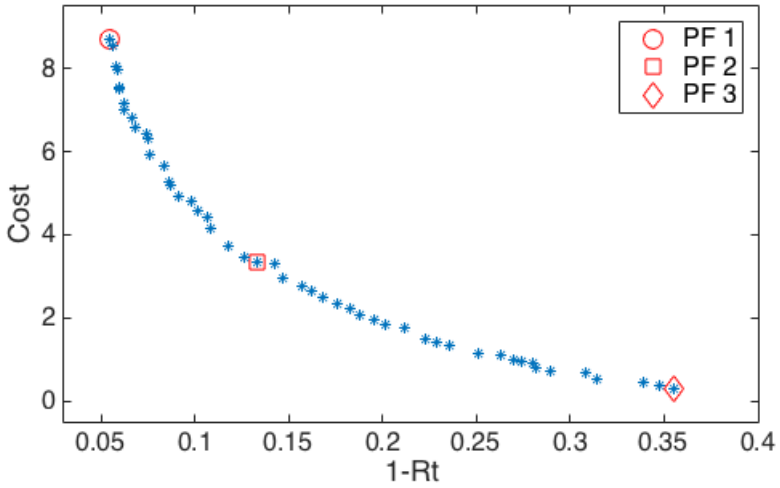
The resilience enhancement activities i_v.

Objective functions

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

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

Pareto Front



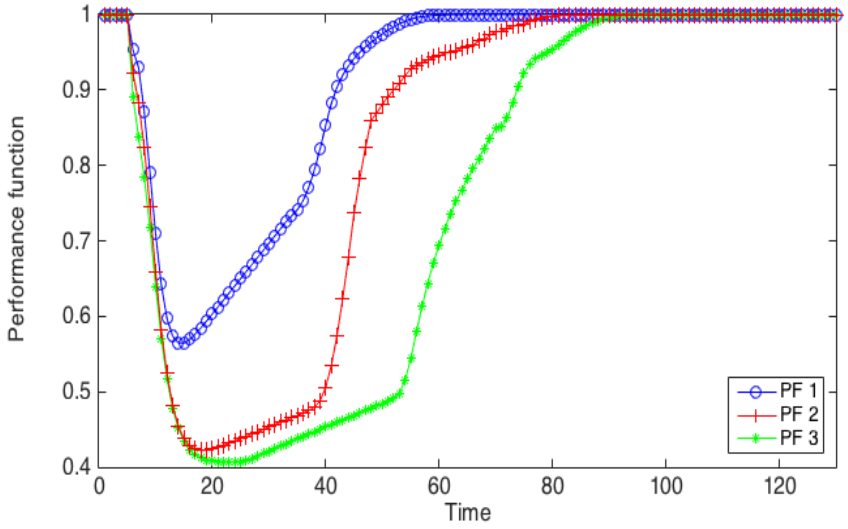
Three optimal values

- 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 $f_2 = Cost$.

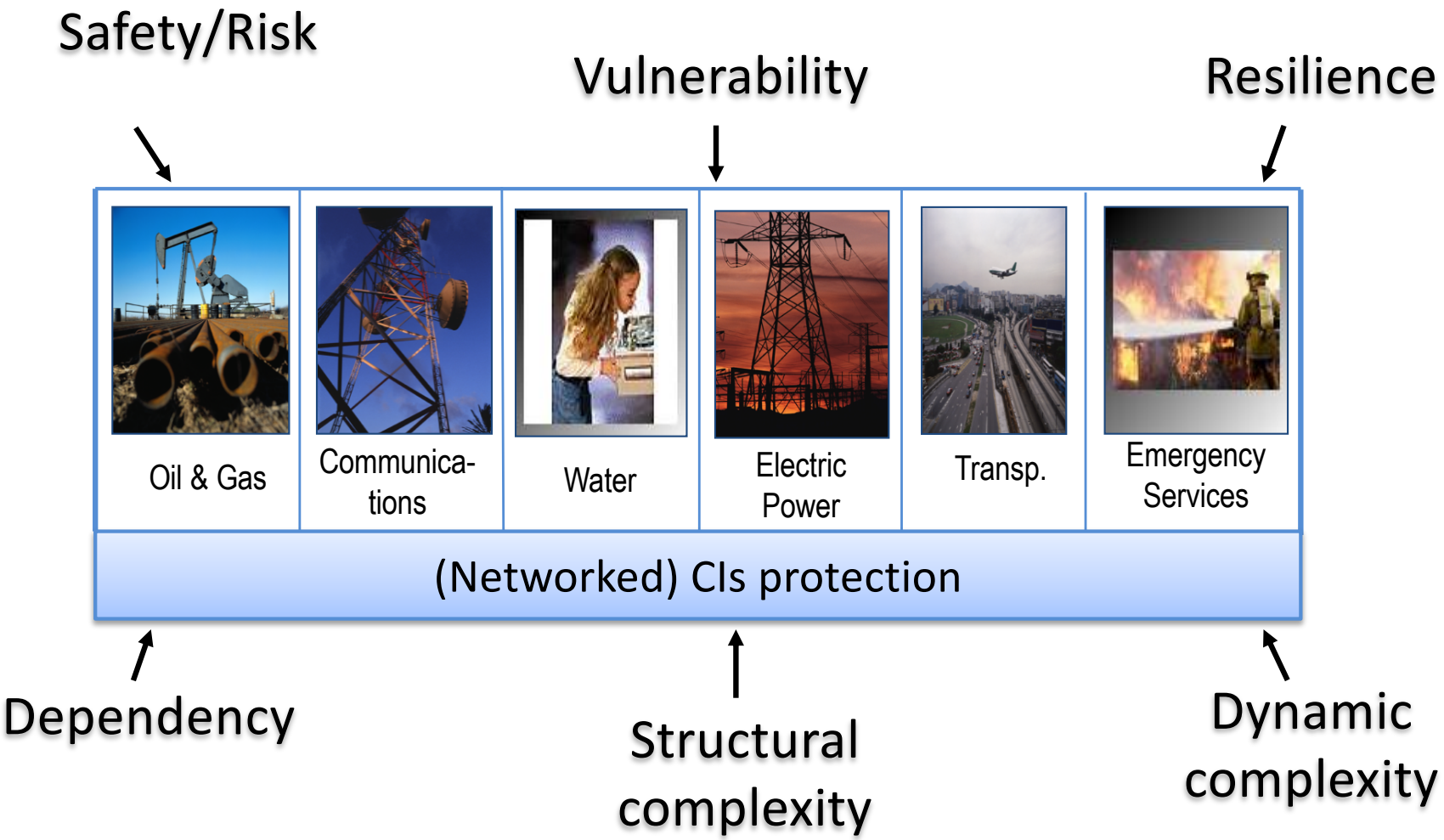
Resilience-oriented decision making

Optimal investment of RES activities

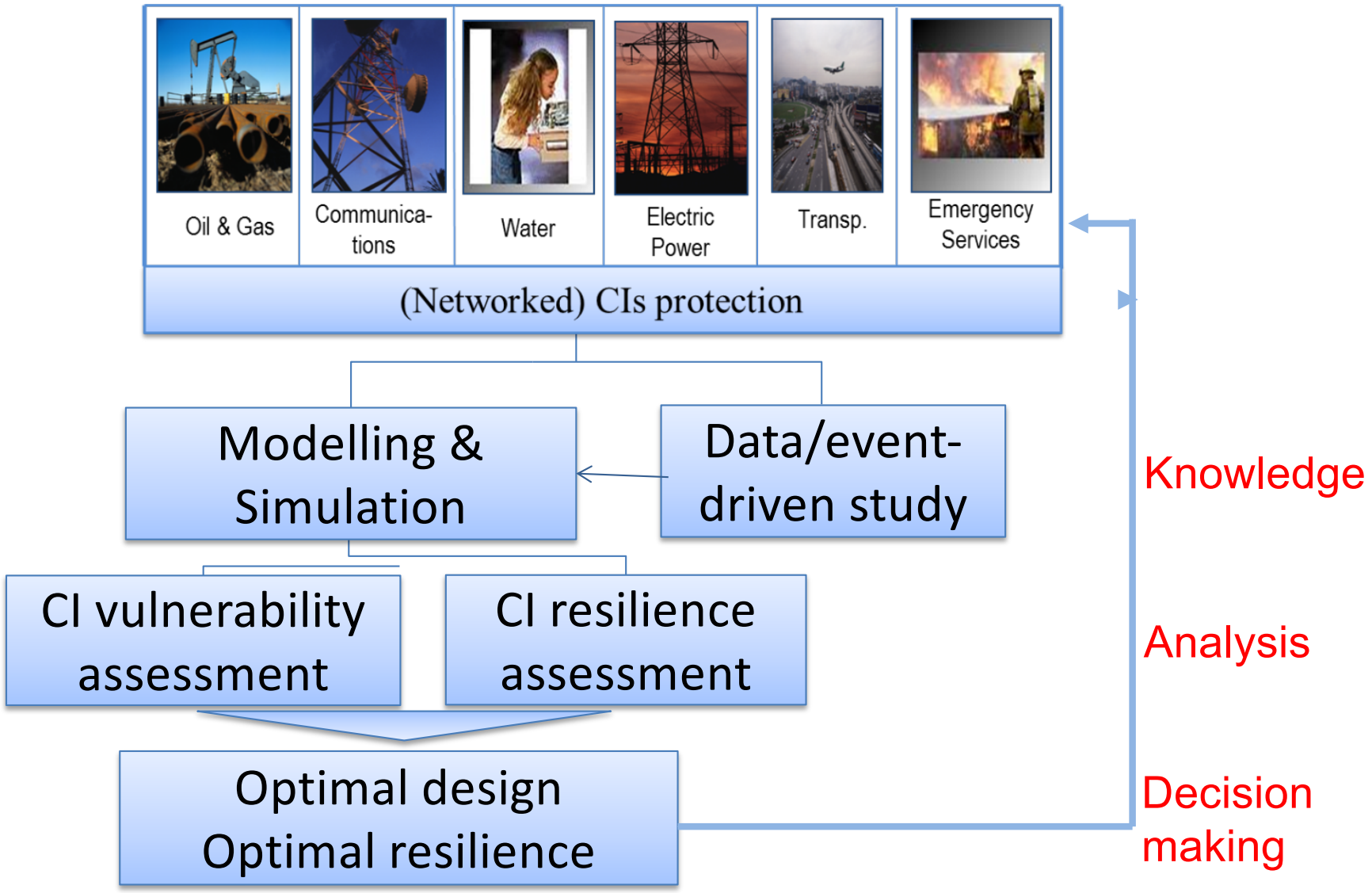
R_t	0.9454	0.8667	0.6447
$Cost$	8.7107	2.3275	0.7243



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

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-phyiscal 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.

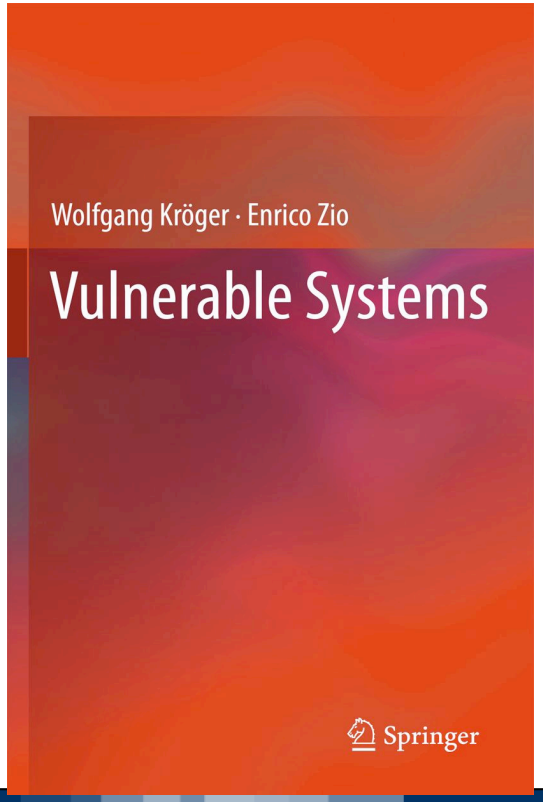
The World we live in is rapidly changing in many ways. Digitalization is bringing new opportunities of connectivity, monitoring and awareness, and is changing the way we communicate and socially behave. Mobility and social pressure are changing the landscape in which we live and operate. Continuous advancements 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
0951-8320/

Learning material

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



AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS

Enrico 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.

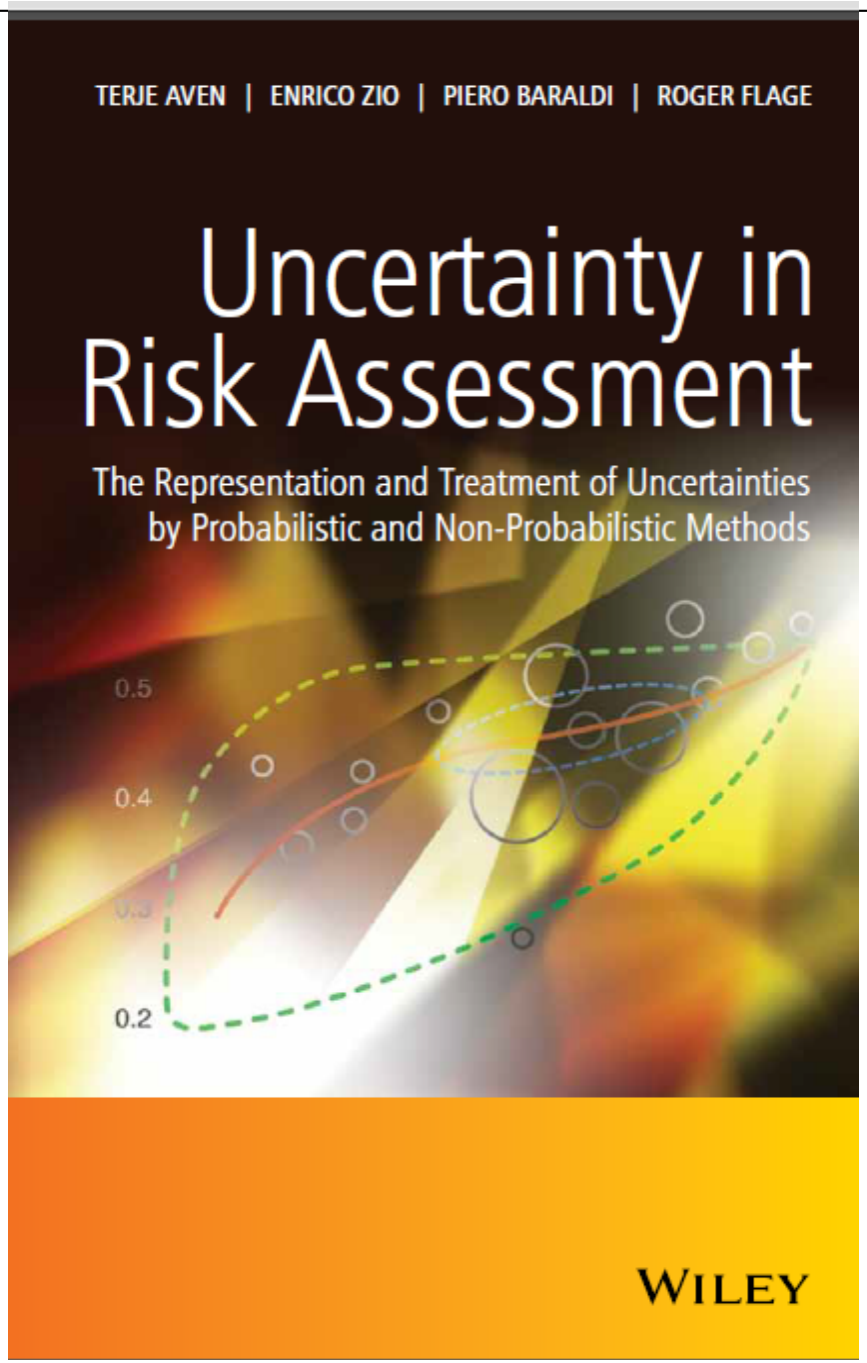
World Scientific
www.worldscientific.com
6442 hc

ISBN-13 978-981-270-639-3
ISBN-10 981-270-639-9

Zio

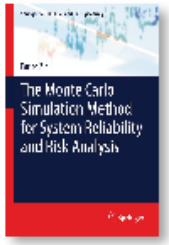
Series in Quality, Reliability and Engineering Statistics Vol. 13

AN INTRODUCTION TO THE BASICS OF RELIABILITY AND RISK ANALYSIS


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 introduction: definition of critical infrastructure, safety, vulnerability, risk, resilience
Logic Methods: Fault Trees + Exercises
Logic Methods: Event Trees + Exercises
Logic Methods: GTST-MLD (with application to CPS)
Homework assignment (project)
Input Output Inoperability Model
Complexity theory and centrality measures
Decision analysis for resilience (Game theory, Adversarial Risk Analysis, …)

Assignments and evaluation

- **Project (+2)**
- **Exam: written questions + exercises**

Thanks…

…for your attention…
…and for being resilient