Critical Infrastructure Workshop

Interdependencies and Crisis Management

Prof. Roberto Setola

Università CAMPUS BioMedico di Roma

Complex System & Security Lab

r.setola@unicampus.it

Bucarest – Romania, 10 October 2013

UCBM

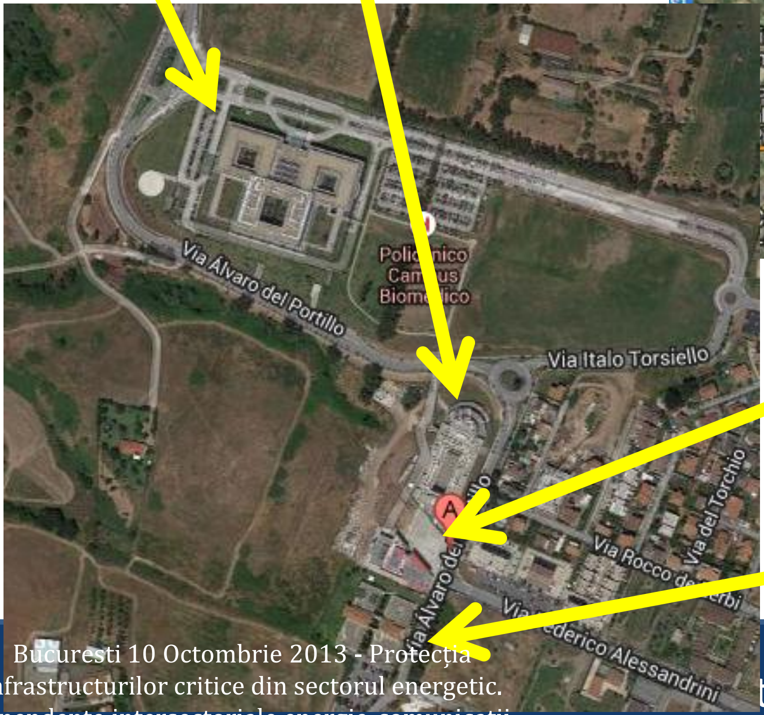
Università CAMPUS BioMedico di Roma (1991)

Located in the South of Rome
(just outside the GRA)

Mentana
Roma
Villa Ada
Tivoli
Frascati
Grottaferrata
Vitinia
Selcetta
A

Hospital

CIR Integrated Research Center



New building –
University Center
(opening on Nov 2013)

Center for Elderly

It includes two faculties:

- ❑ Medicine
- ❑ Engineering
  - ✓ Industrial
  - ✓ Biomedical
  - ✓ Chemical

UCBM (2)

- It is the first thematic Italian University centered on the Person
- Private University, ranked in the firsts position among universities in Italy.
- Recognized healthcare and education excellence center in Italy.

From 2008
VI editions

Master Degree in

HOMELAND SECURITY – Systems, Methods and Tools for Security and Crisis Management

www.MasterHomelandSecurity.eu

Coserity Lab

COSERITYLAB

Complex Systems & Security Lab @ University Campus Bio-Medico of Rome, Italy

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

www.coseritylab.it

- Roberto Setola (*Associated Professor)*
- Gabriele Oliva *(Post Doc)*
- **Mariacarla De Maggio** *(Project Manager)*
- Francesca De Cillis, Estefania Etcheves Miciolino, Claudio Romani *(PhD Students*)
- **Greg Fink** *(Staff Member)*
- Marco Tesei *(Junior Researcher)*

Coserity Lab

On Going EU Projects

- Security Liaison Officer (SLO)
  Identifying a Framework for the Protection of Critical Infrastructures
- FACIES
- CIPR Net
- THREV
- REFIRE
- METRIP
- SPARC

Past EU Project

- SecuFood
- CI²RCO
- MICIE
- ESTEC
- MIA
- ms³i
- HOPES
- AccuRobAs Accurate Robot Assistant
- CRESCO

Cooperation

(excluded partners of EU projects, not exhaustive)

- Enel L'ENERGIA CHE TI ASCOLTA.
- TELECOM ITALIA
- ENAV S.p.A. SOCIETÀ NAZIONALE PER L'ASSISTENZA AL VOLO
- SELEX Sistemi Integrati … canica
- AnsaldoSTS Una Società Finmeccanica
- VITROCISET
- INTERGRAPH
- Terna
- iPS a member of the RiSel Group
- Vigili del Fuoco

Critical Infrastructure Protection & Interdependencies

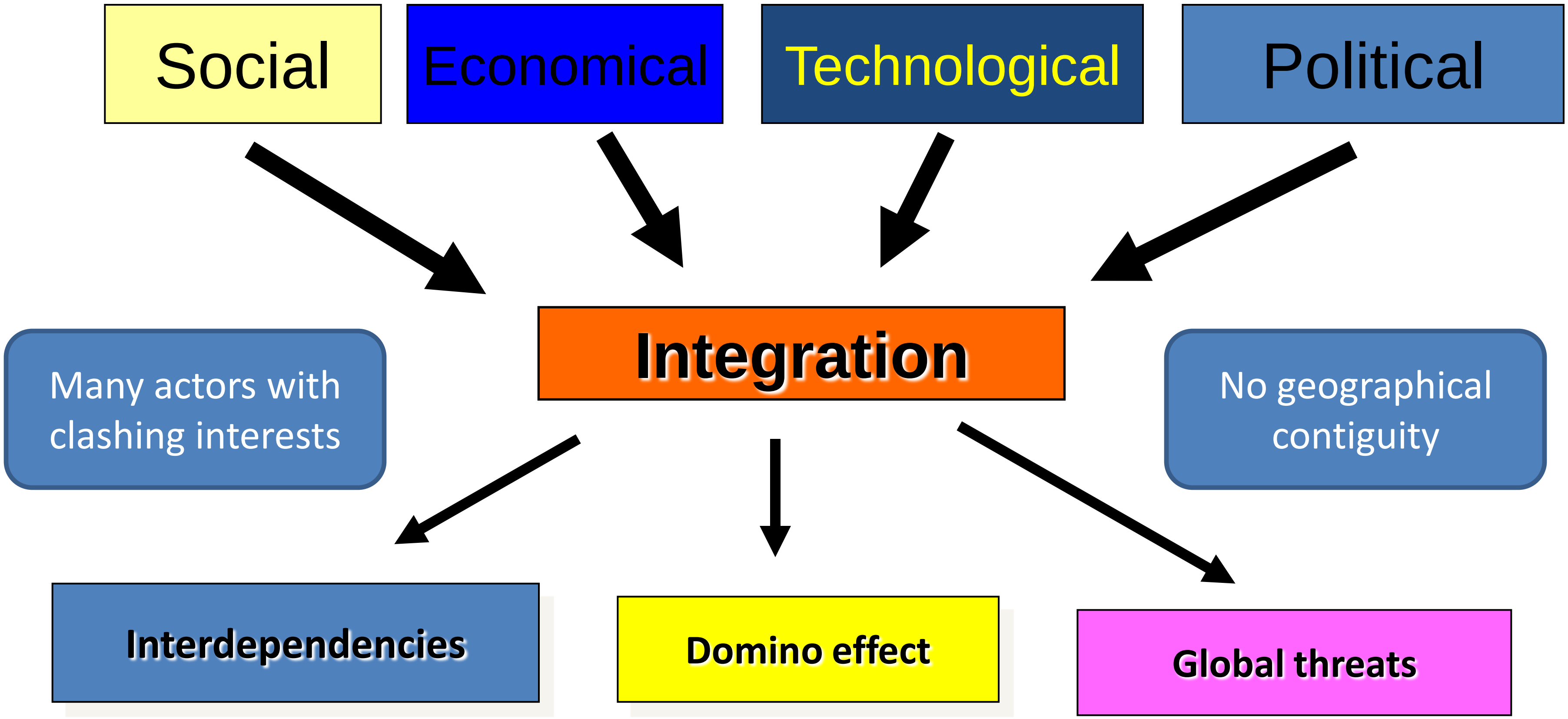
Dependency vs interdependency

- ***Dependency***: is the capability of an infrastructure to influence the state of an other infrastructure. It is a *unidirectional* relationship.
- ***Interdependency***: is a *bidirectional* relationship between two infrastructures through which the state of each infrastructure is influenced or is correlated to the state of the other.

Integration vs Dependability

…. for a lot of GOOD reasons

divide et impera



Social

Economical

Technological

Political

Integration

Many actors with clashing interests

No geographical contiguity

Interdependencies

Domino effect

Global threats

Dependency definiton (2)

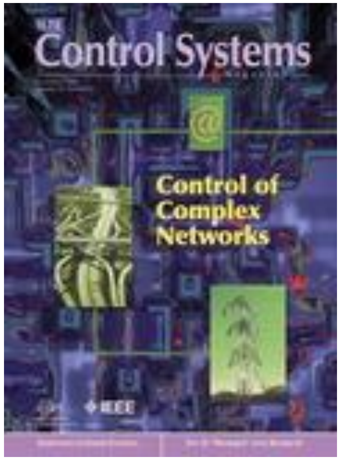
A depend on B when an event able to reduce the operational capability of B is able to reduce the operational capability of A

In other terms dependency is a differential (or better detrimental) property.

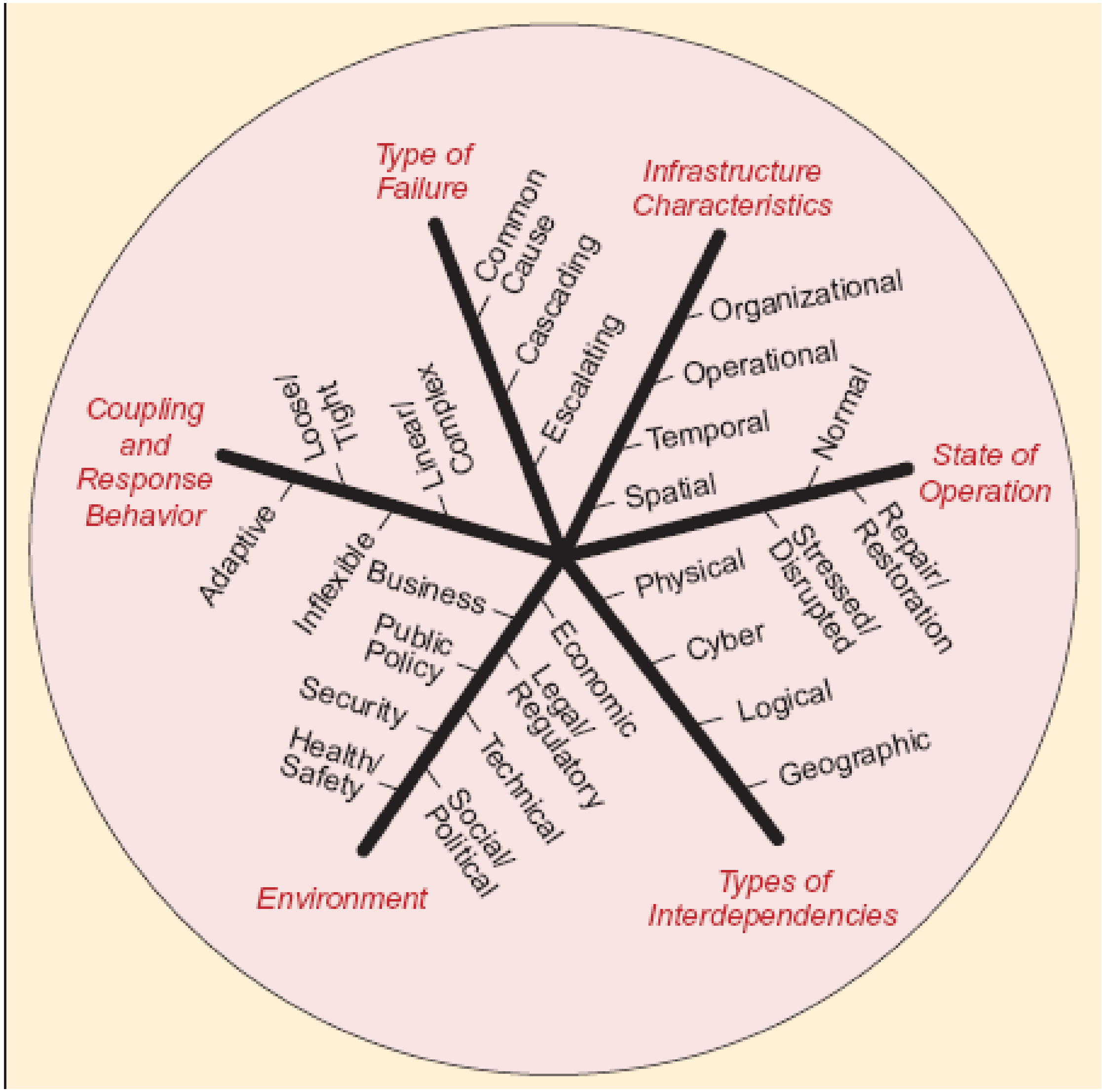
The degree of dependency is related to the detrimental variation induced in the dependent element

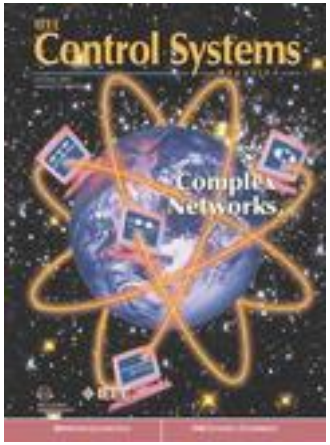
R. Setola, "How to Measure the Degree of Interdependencies among Critical Infrastructures", *Int. J. of System of Systems Engineering, (IJSSE),* vol. 2,pp. 38 -59, 2010

Dimensions for describing infrastructure interdependencies.



September 2011

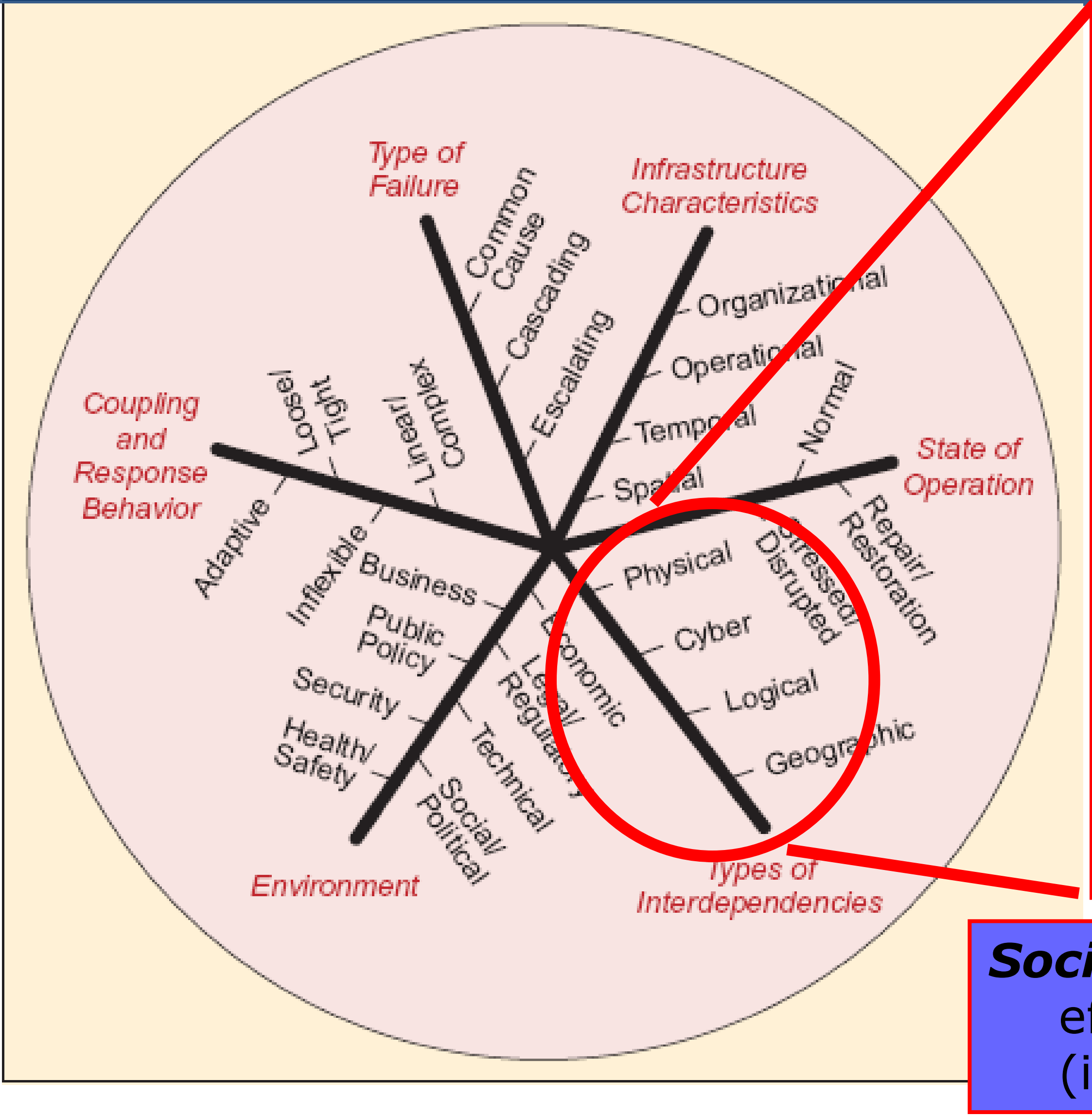




January 2012

S. Rinaldi, J. Peerenboom, and T. Kelly, “Identifying Understanding and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control System Magazine*, pp. 11–25, 2001.

Dimensions for describing infrastructure interdependencies.



Physical *Interd.:* if the operations of one infrastructure depends on the physical output(s) of the other.

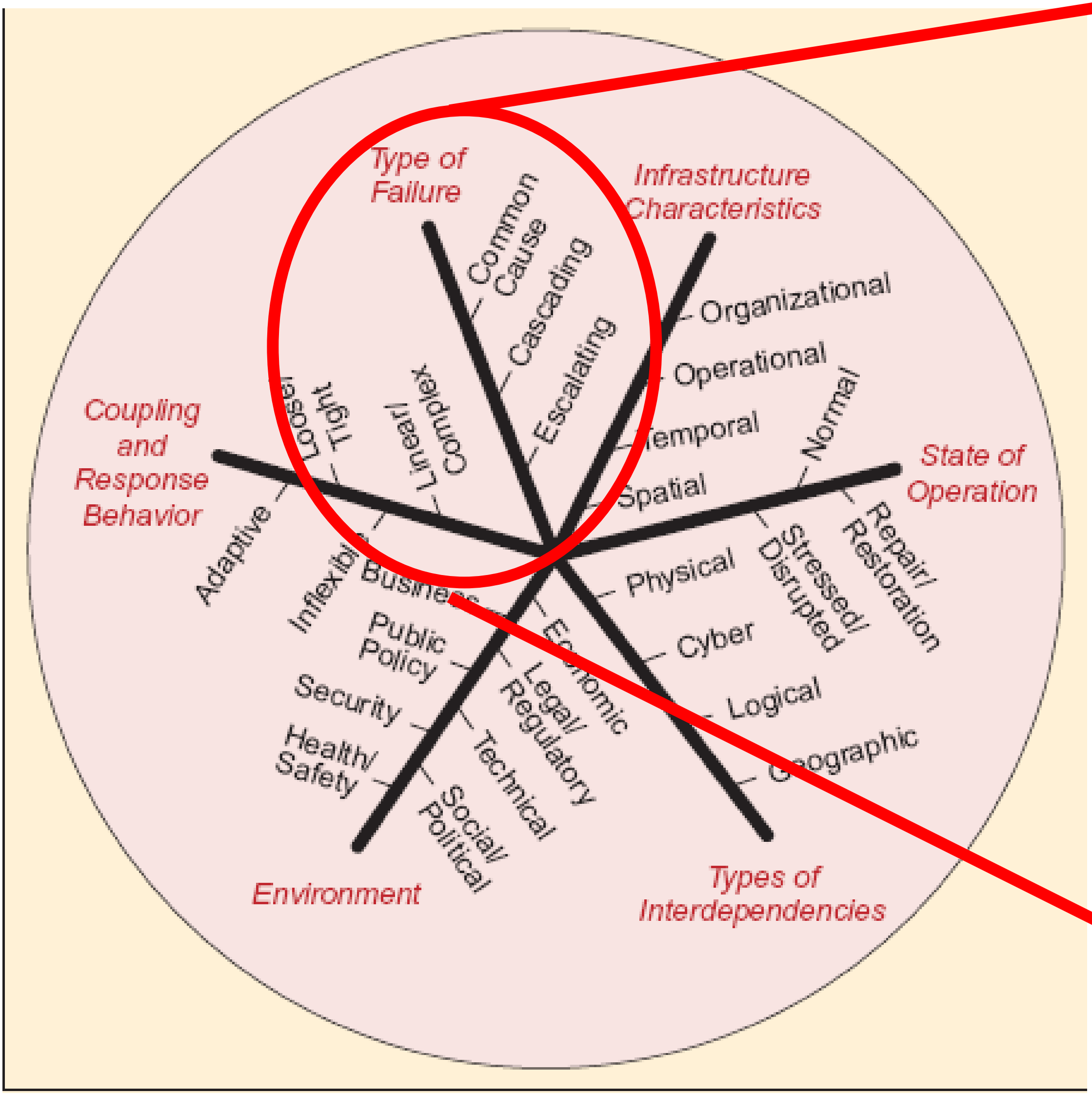
Cyber *Interd.:* if its state depends on information transmitted via cyberspace.

Geographical *Interd.:* when elements are in close spatial proximity.

Logical *Interd*.: any other causes (e.g. regulamentatory)

Sociologic *Interd*.: when coupling effects are mediated by (irrational) human behaviors

Type of failure.

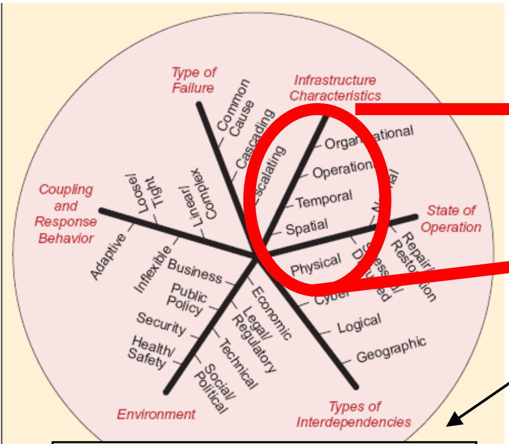


***Common cause**:* the same event produce failure in two or more infrastructures.

***Cascading**:* the failure into one infrastructure induce a domino effect on other infrastructures.

***Escalating**:* the failure of one infrastructure exacerbate the consequences of failure induced by some other causes.

Infrastructure Characteristics



Spatial	Temporal	Operational	Organizational

Part

Unit

Subsystem

System

Infrastructure

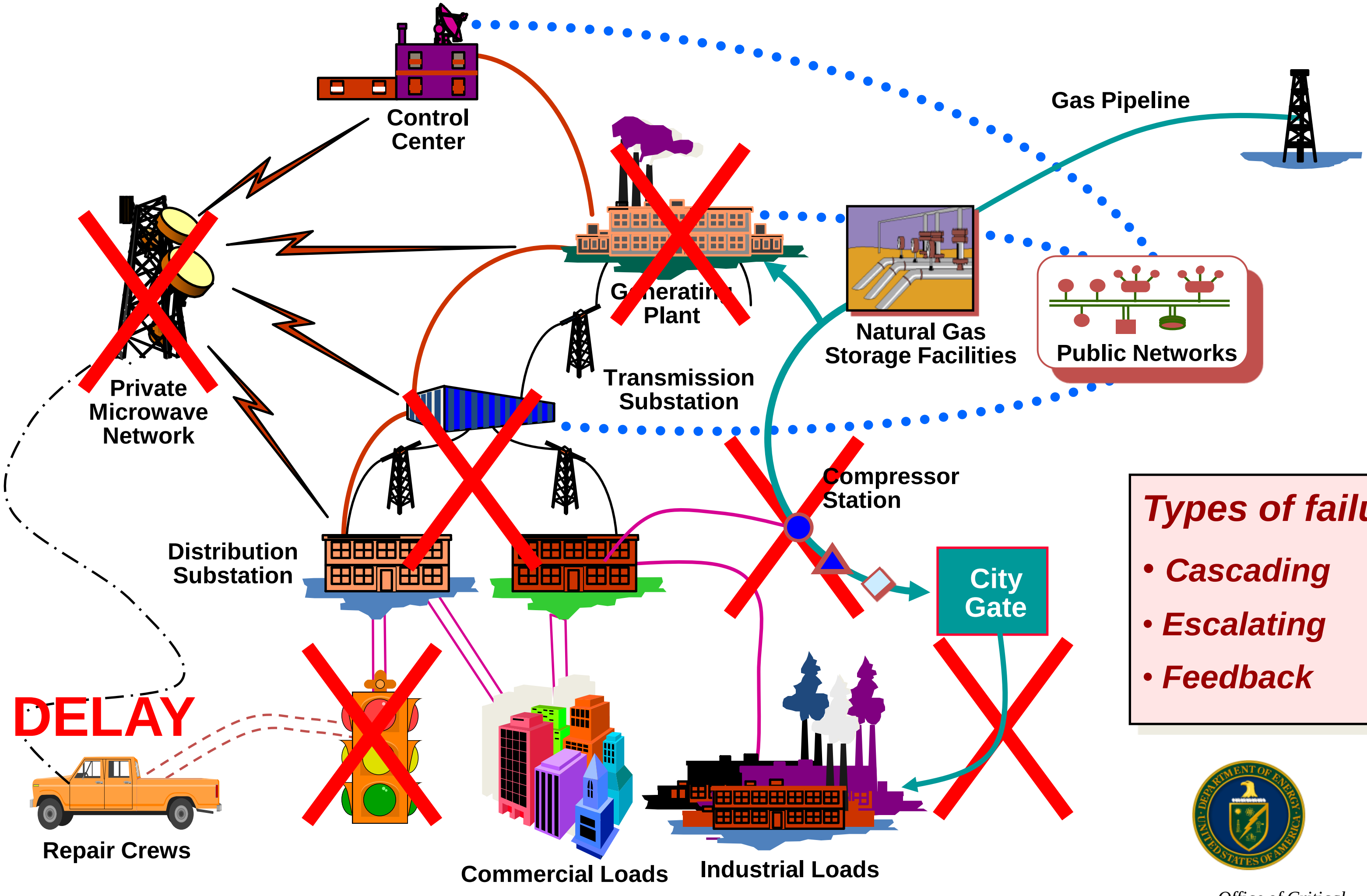
Interd.
Infrastr.

Interdependency are more relevant as scope increase

Relevant time scales vary from milliseconds to hours to years

The importance of each type of interdependency change w.r.t. time horizon

Example of Interdependencies in the Energy Industry



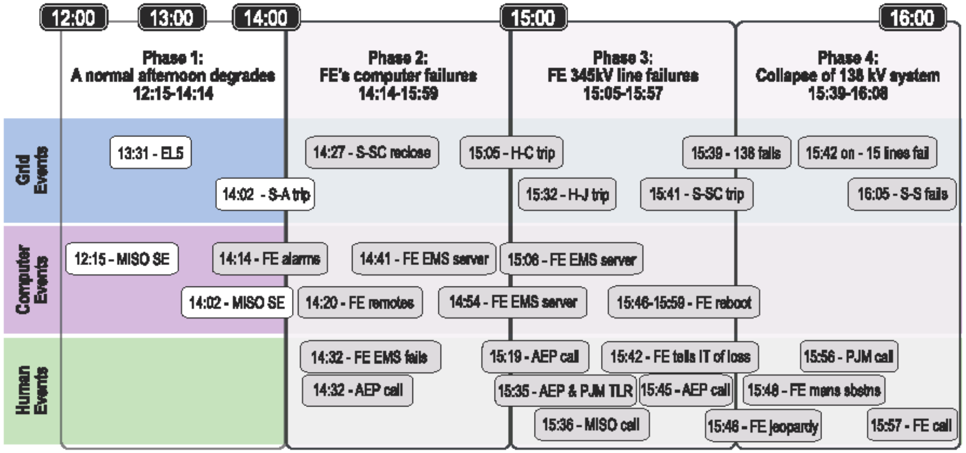
Types of failures:

- *Cascading*
- *Escalating*
- *Feedback*

Source 1998

Office of Critical Infrastructure Protection

MHR^3



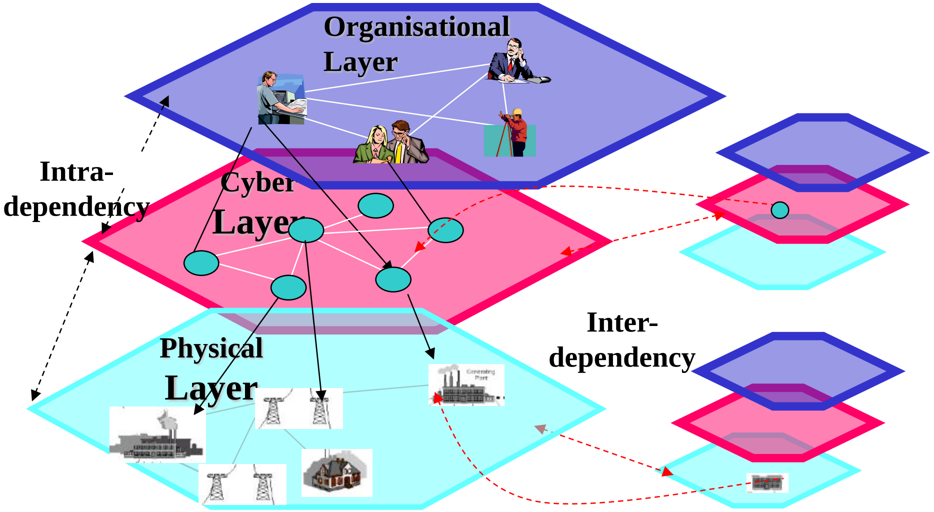
12:00 13:00 14:00 15:00 16:00

	Phase 1: A normal afternoon degrades 12:15-14:14	Phase 2: FE's computer failures 14:14-15:59	Phase 3: FE 345kV line failures 15:05-15:57	Phase 4: Collapse of 138 kV system 15:39-16:08
Grid Events	13:31 - EL5 14:02 - S-A trip	14:27 - S-SC reclose	15:05 - H-C trip 15:32 - H-J trip 15:41 - S-SC trip	15:39 - 138 fails 15:42 on - 15 lines fail 16:05 - S-S fails
Computer Events	12:15 - MISO SE 14:14 - FE alarms 14:02 - MISO SE	14:41 - FE EMS server 14:20 - FE remotes 14:54 - FE EMS server	15:06 - FE EMS server 15:46-15:59 - FE reboot	
Human Events		14:32 - FE EMS fails 14:32 - AEP call	15:19 - AEP call 15:42 - FE tells IT of loss 15:35 - AEP & PJM TLR 15:45 - AEP call 15:36 - MISO call	15:56 - PJM call 15:48 - FE mans sbstns 15:48 - FE jeopardy 15:57 - FE call

To correctly capture the complexity of the phenomena, it is mandatory to have an holistic vision able to agregate the different vision.

- Physical
- Logic
- Organization

Each layer is characterized by its own component, resource, fault and link



Same episodes

1998 – Galaxy IV (USA)

Source

Failure in a communication satellite

Consequences

- 40 millions pagers out-of-services
- 20 United Airline flights delayed
- Many radio stations unable to operate
- Congestion at high-way gas stations: due to impossibility to process credit card

2000 – Maroochy Shire (Australia)

Source

An ex-employer used a wireless Internet connection to penetrate into SCADA of sewage treatment plant

Consequences

- 47 "abnormal" accidents in January-April 2000
- 1.200.000 liters of raw sewage dispersed in the environment
- Potable water compromised in the area

2004 – Italy

Source

an incident in the air conditioned system of an important telco nodes in Rome

Consequences

- Blackout in mobile and wired communication for about 6 h in Roma
- About 5.000 banks and 3.000 post offices off-line
- 70% check-in desks at Fiumicino airport off-line
- ACEA (local electrical distributor) lost the control on half of the network (near miss)

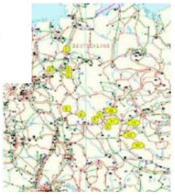
2006 - Europe

"We weren't very far from a European blackout"

spokesperson from RTE (French transmission system operator)

380kV lines across river Ems turned off at 21:30h to let the Norwegian Pearl through

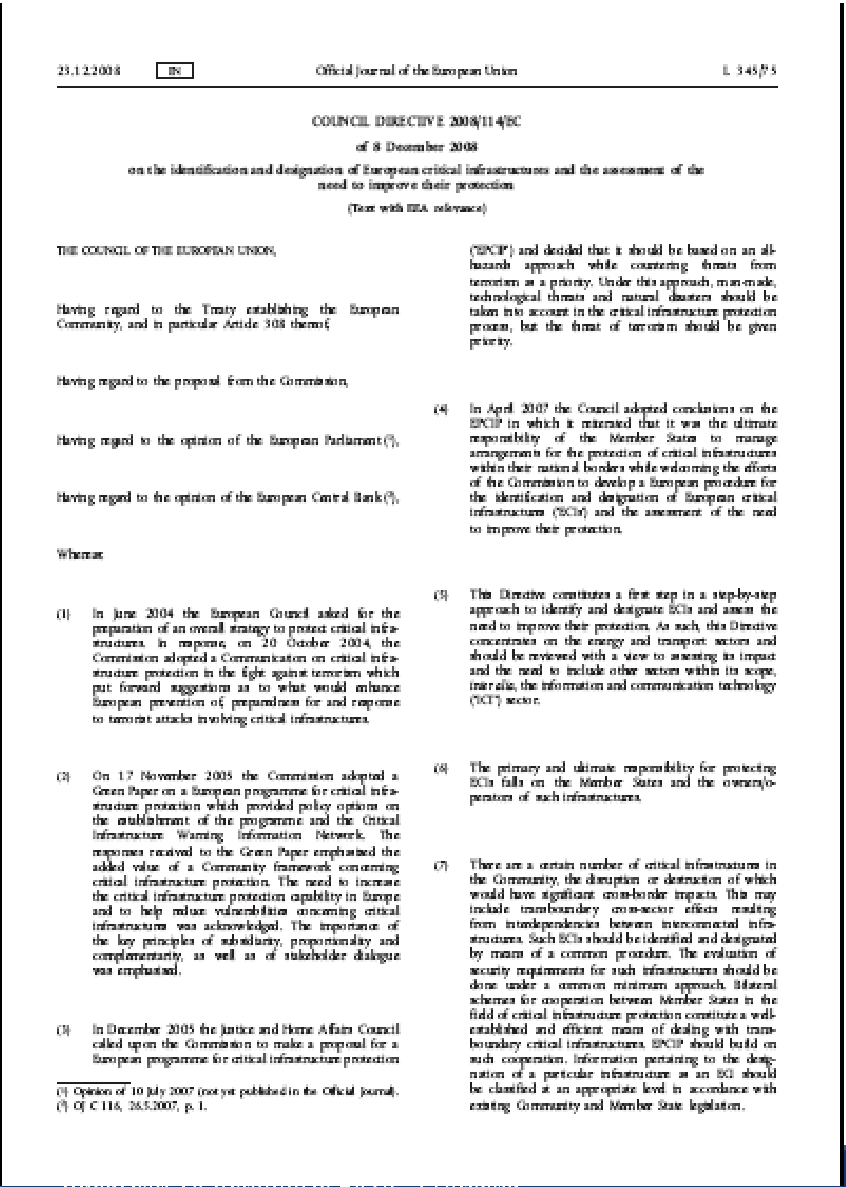
A large number of lines in Germany, Austria, Hungary and Croatia automatically tripped one after the other in a "domino" effect, as their automated protection systems detected load flows over the safety limit



15 million households affected in 11 countries

Power restored in 30 minutes in some places, 2 hours in Italy

EU Directive 2008/114EC



23.12.2008 EN Official Journal of the European Union L 345/75

COUNCIL DIRECTIVE 2008/114/EC

of 8 December 2008

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 308 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Having regard to the opinion of the European Central Bank [2],

Whereas:

(1) In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

(2) On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection ('EPCIP') and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

(4) In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection.

(5) This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector.

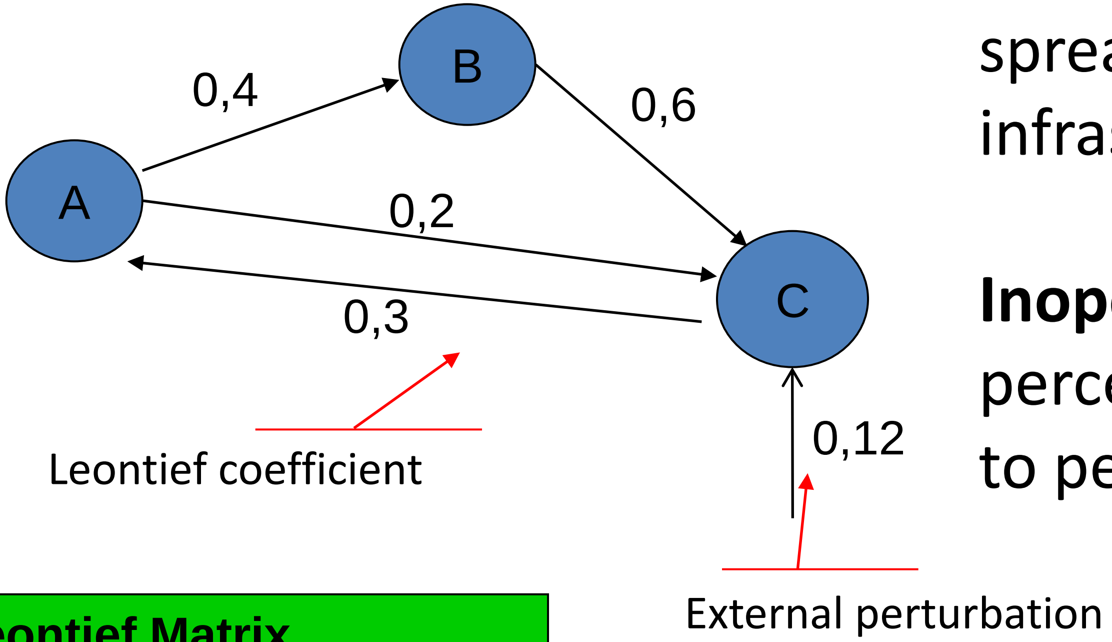
(6) The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures.

(7) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common minimum approach. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well-established and efficient means of dealing with transboundary critical infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

[1] Opinion of 10 July 2007 (not yet published in the Official Journal).
[2] OJ C 116, 26.5.2007, p. 1.

- Experts identify **the worst possible realistic scenarios** of disruption or destruction of that infrastructure (all hazards, **ex-ante exercise**)
- Each scenario is developed (*including cascading effects where possible*) and its impact assessed in terms of the 3 dimensions (casualties, economic and public effects)
- The effect are compared with thresholds

Input-Output Inoperability Model



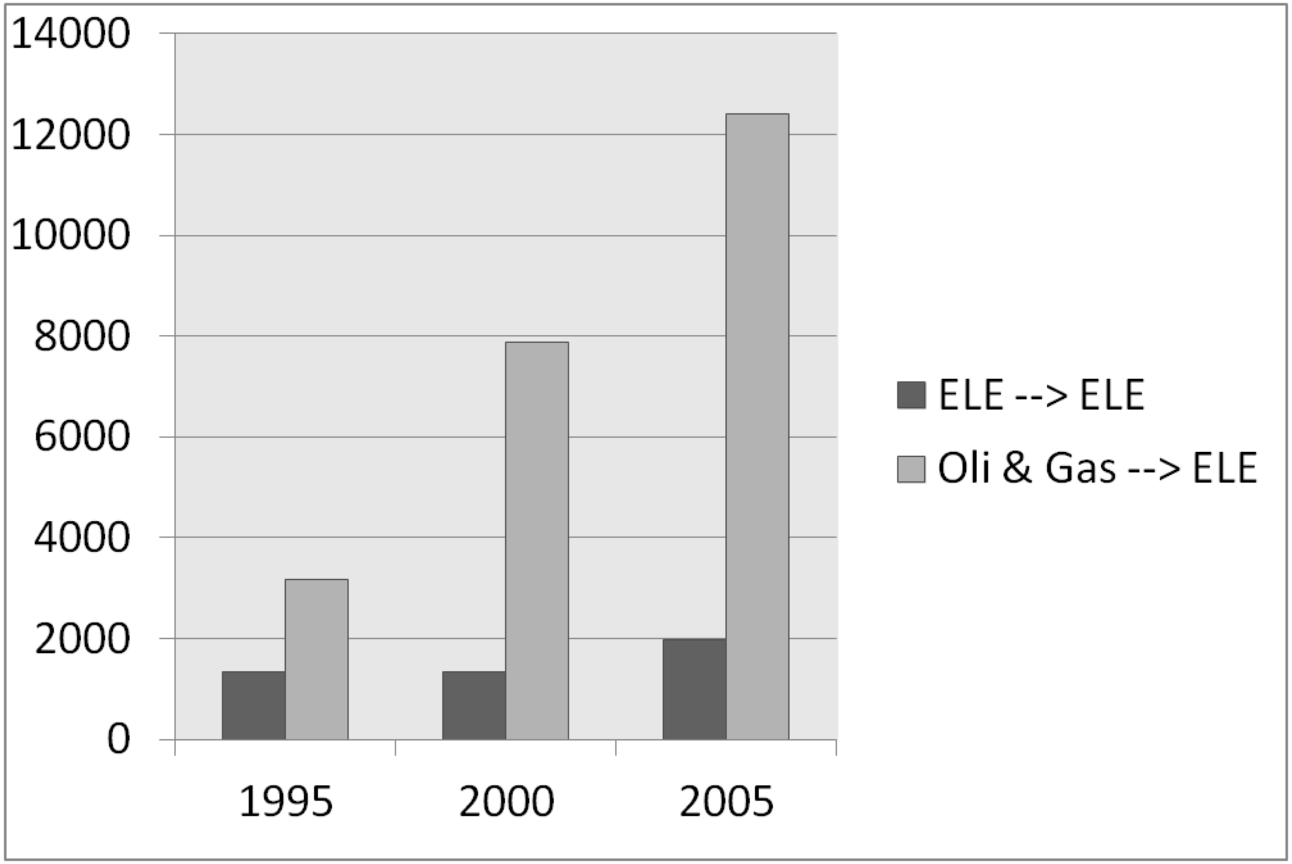
Analyse how inoperability spread among infrastructures

Inoperability = percentage of incapability to perform intend task

Leontief Matrix. Coefficients are the fraction of transmitted inoperability

$$q(k+1) = A^{*} q(k) + c^{*}$$

Evolution of Italian Scenario



The amount of inter-sectors economic exchanged grow largely than those of intra sector (main diagonal)

Source ISTAT data

Dependency index & Influnce gain

$$\mathbf{A} = \begin{pmatrix} 0 & * & * & * \\ * & 0 & * & * \\ * & * & 0 & * \\ * & * & * & 0 \end{pmatrix}$$

dependency index

$$\delta_i = \sum_j a_{ij}$$

Is a measurement of the robustness with respect to the transmitted inoperability

$$\rho_j = \sum_i a_{ij}$$

influence gain

Is a measurement of the influence that a specific infrastructure has on the global system

Steady-state solution

$$\bar{\mathbf{x}} = (\mathbf{I} - \mathbf{A})^{-1}\,\mathbf{c} = \mathbf{S}\,\mathbf{c}$$

If A is positive and stable, then

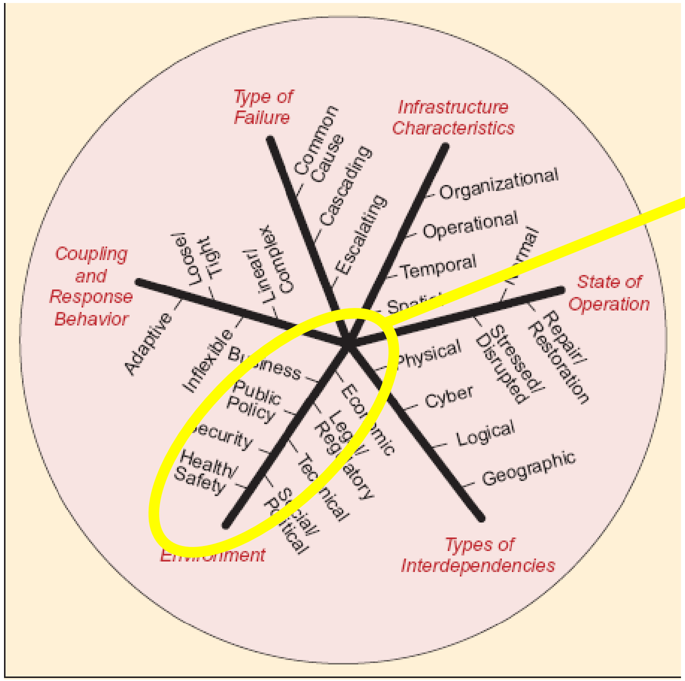
$$\mathbf{S} = [\mathbf{I} - \mathbf{A}]^{-1} = \mathbf{I} + \mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \cdots$$

Overall depencey index and influence gain

$$\bar{\rho}_j = \frac{1}{n-1}\sum_{i \neq j} s_{ij} \qquad \bar{\delta}_i = \frac{1}{n-1}\sum_{j \neq i} s_{ij}$$

R. Setola and S. De Porcellinis, “A Methodology to Estimate Input-output Inoperability Model Parameters”, *Critical Information Infrastructures Security 2007,* Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 149 – 160, 2008.

IIM Operational vs Economic



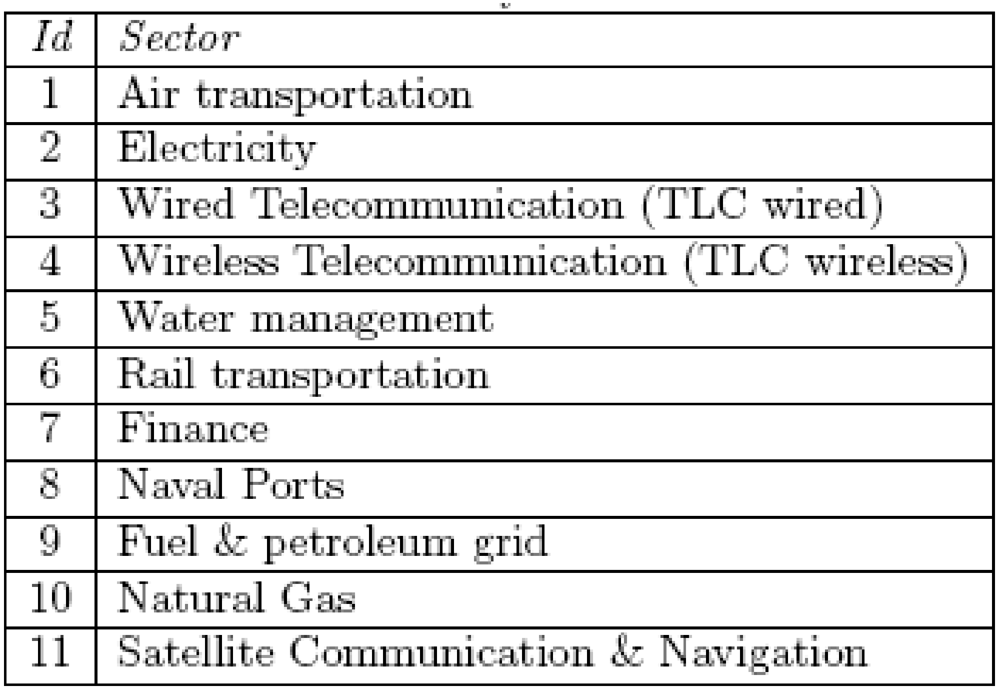
Economic (business) links represent just one of the dimension of dependency

Fukushima Nuclear plant

To capture (other) depedency we have to consider also ooperational dimension

The scenario

In our case study we consider 11 critical sectors



Id	*Sector*
1	Air transportation
2	Electricity
3	Wired Telecommunication (TLC wired)
4	Wireless Telecommunication (TLC wireless)
5	Water management
6	Rail transportation
7	Finance
8	Naval Ports
9	Fuel & petroleum grid
10	Natural Gas
11	Satellite Communication & Navigation

and 5 time slot

a) less than 1 h

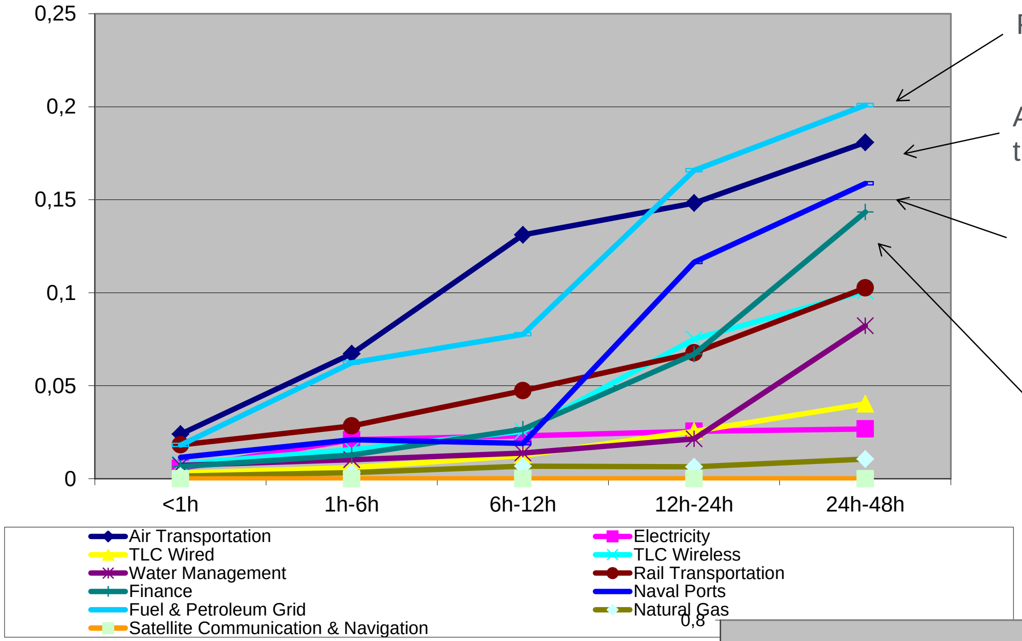
b) from 1 to 6 h

c) from 6 to 12 h

d) from 12 to 24 h

e) from 24 to 48 h

The results



Fuel & Petroleum

Air transportation

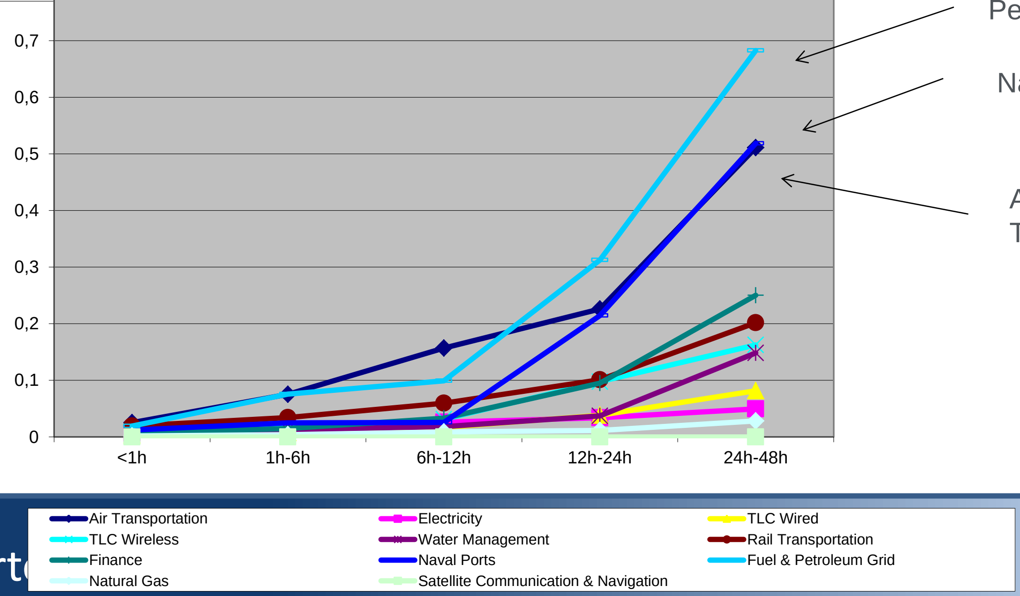
Naval Ports

Finance

__Normalised dependency index__

The curves cross each others, i.e. they relevance/fragility varies with the outage time

__Overall normalised dependency index__



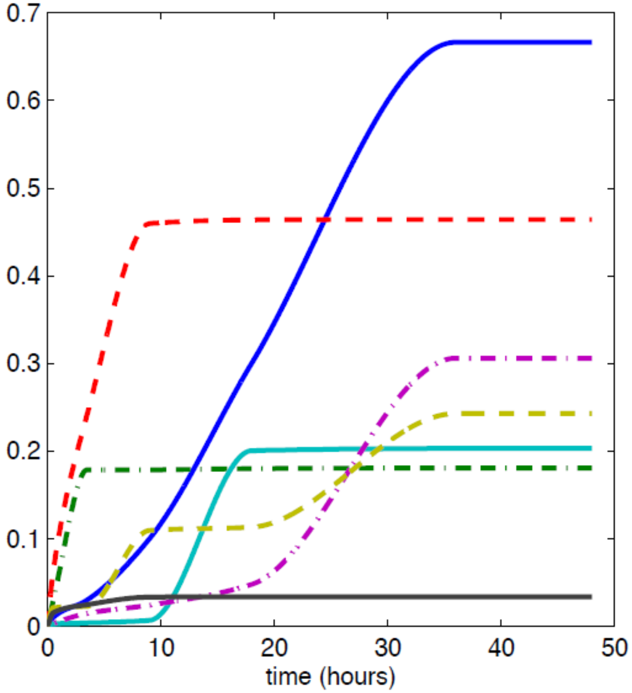
Fuel & Petroleum

Naval Port

Air Transportation

This phenomana should be considered when emergency plan are designed

Time Varying IIM



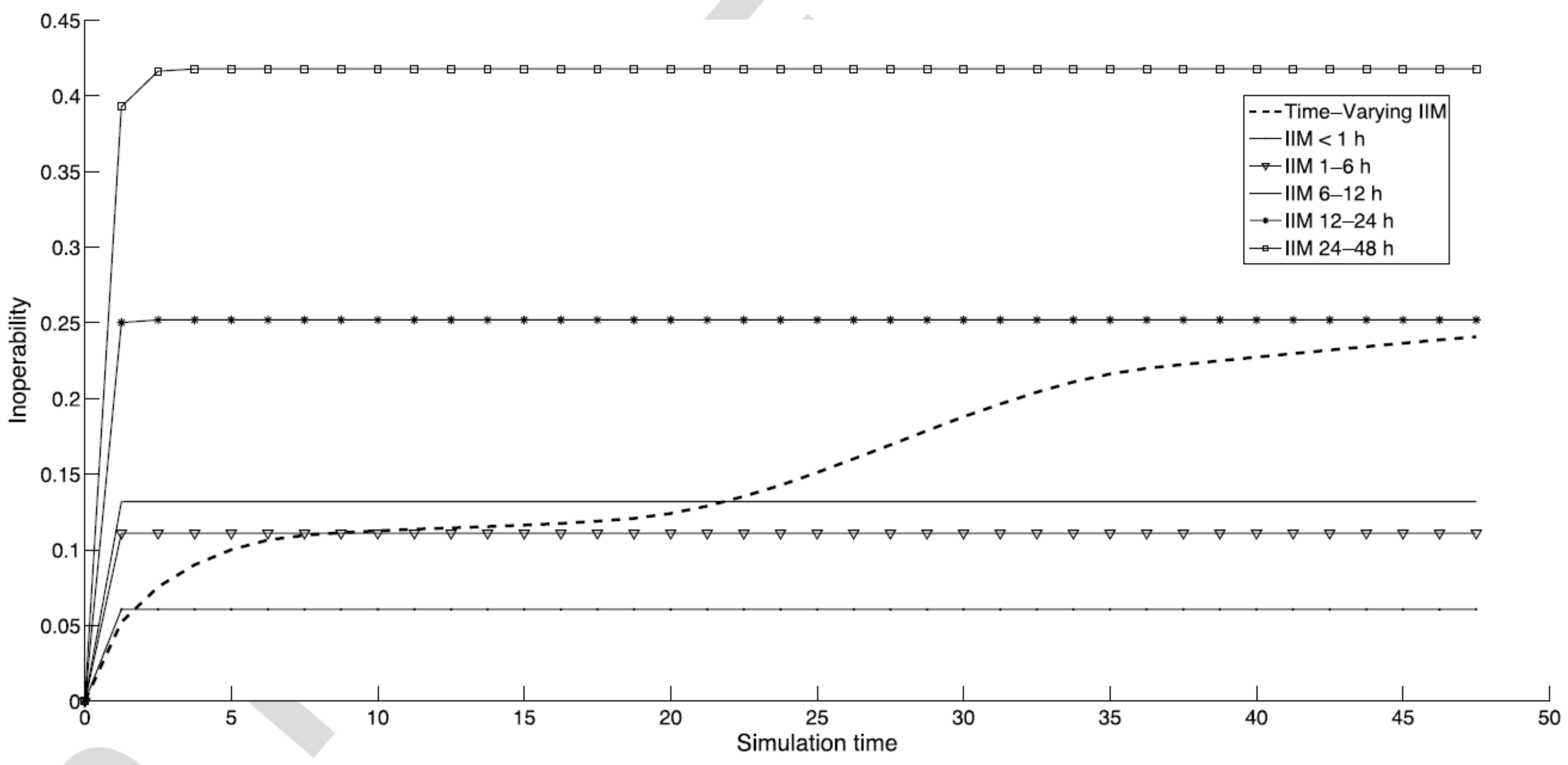
Constant: it does not change with outage period, i.e. direct link (no buffer or bck)

Linear + constant: buffer absorb partially the inoperability until expire

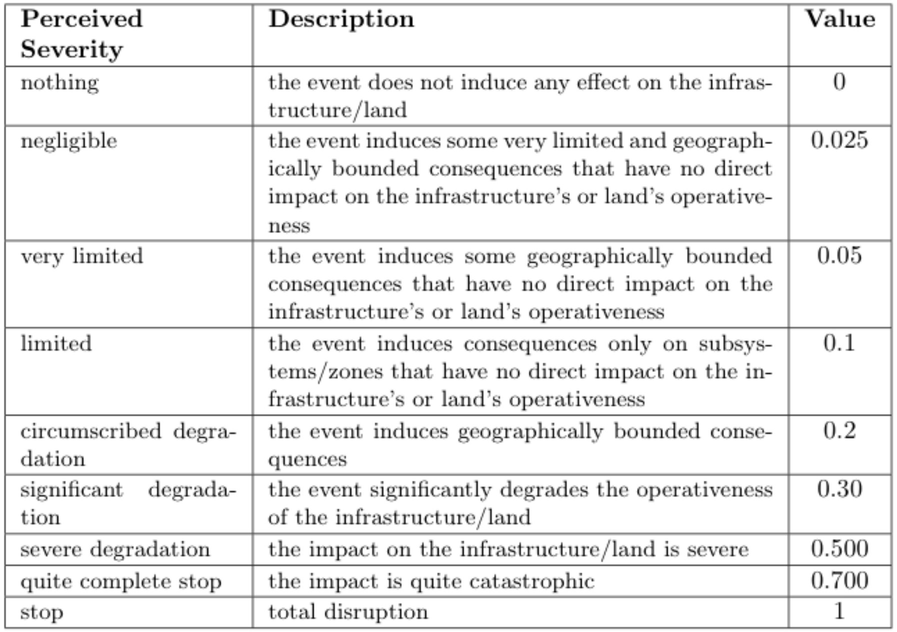
S-Shape: buffer absorb quite completely inoperability for a while but when expire there is a rapid degradation (no graceful degradation)

Double S-Shape: there are two type of buffers which designed to support general and prioritary aspects

Time Varing IIM vs constaant IIM

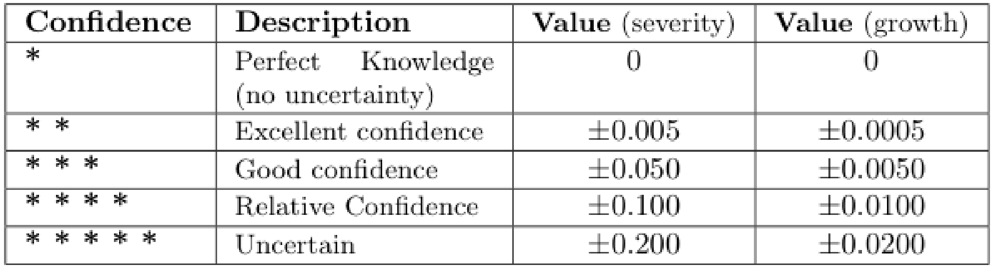


Neglecting the variation of the dependency coefficients can drive to large error



Perceived Severity	Description	Value
nothing	the event does not induce any effect on the infrastructure/land	0
negligible	the event induces some very limited and geographically bounded consequences that have no direct impact on the infrastructure's or land's operativeness	0.025
very limited	the event induces some geographically bounded consequences that have no direct impact on the infrastructure's or land's operativeness	0.05
limited	the event induces consequences only on subsystems/zones that have no direct impact on the infrastructure's or land's operativeness	0.1
circumscribed degradation	the event induces geographically bounded consequences	0.2
significant degradation	the event significantly degrades the operativeness of the infrastructure/land	0.30
severe degradation	the impact on the infrastructure/land is severe	0.500
quite complete stop	the impact is quite catastrophic	0.700
stop	total disruption	1

Criticality Scale



Confidence	Description	Value (severity)	Value (growth)
*	Perfect Knowledge (no uncertainty)	0	0
* *	Excellent confidence	±0.005	±0.0005
* * *	Good confidence	±0.050	±0.0050
* * * *	Relative Confidence	±0.100	±0.0100
* * * * *	Uncertain	±0.200	±0.0200

Confidence Scale

Data collected via questionnarie have also information about the quality of data

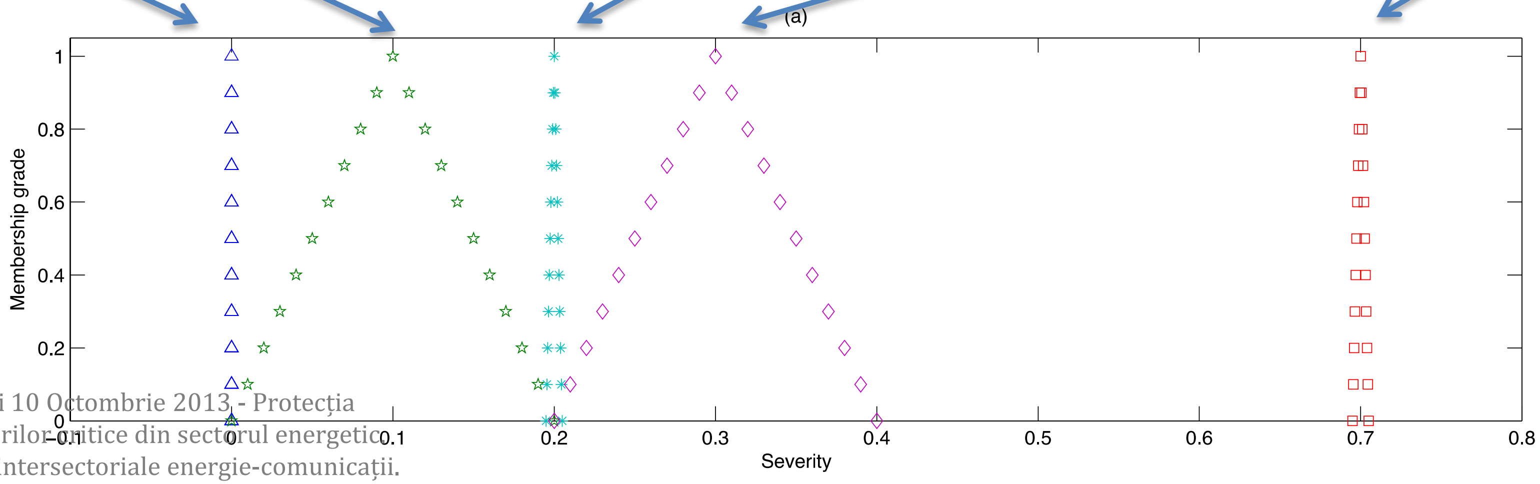
Nothing (Certain)

Limited (Relative Confidence)

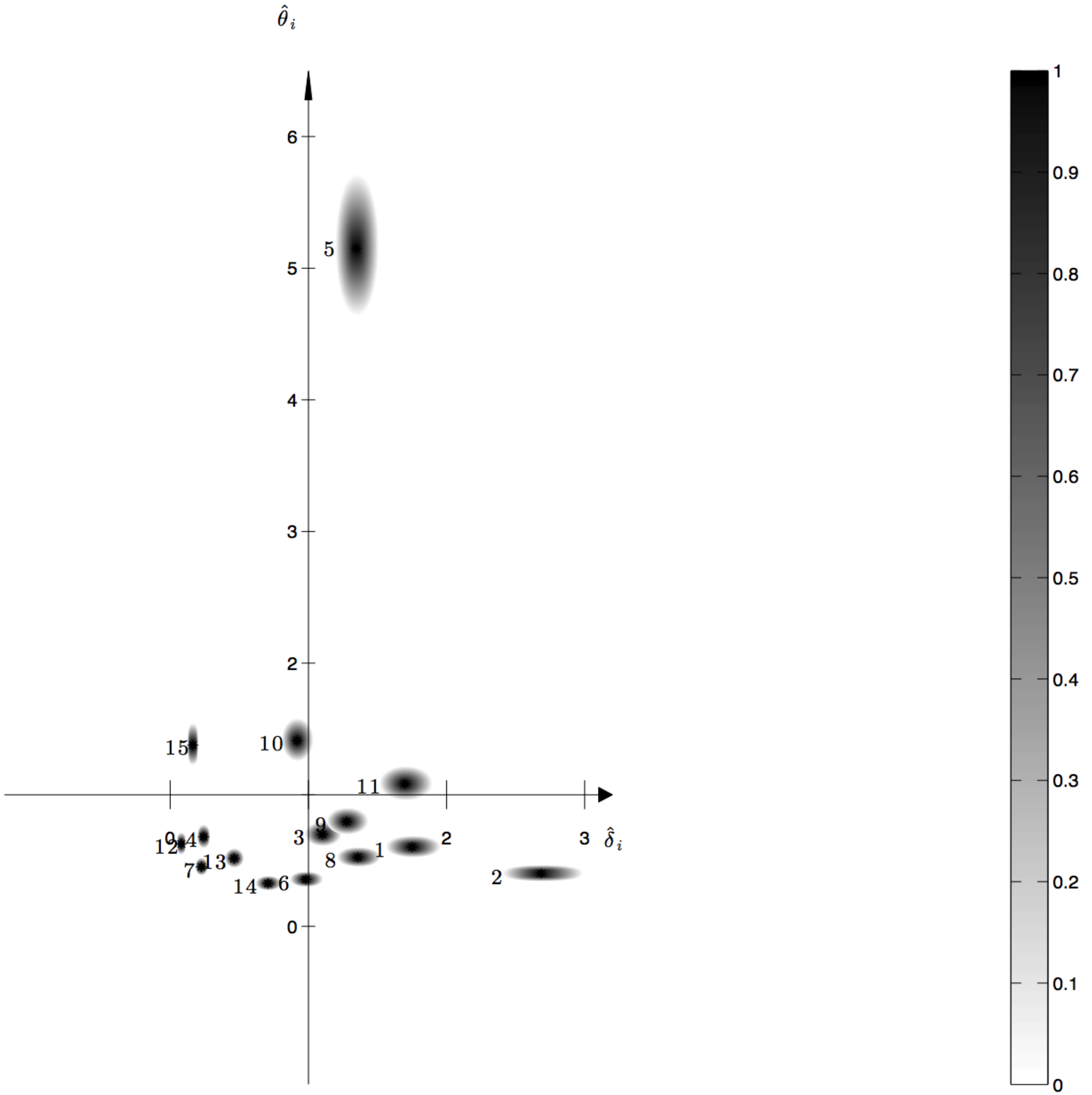
Circumscribed (Excellent Confidence)

Significant (Relative Confidence)

Quite Catastrophic (Excellent Confidence)

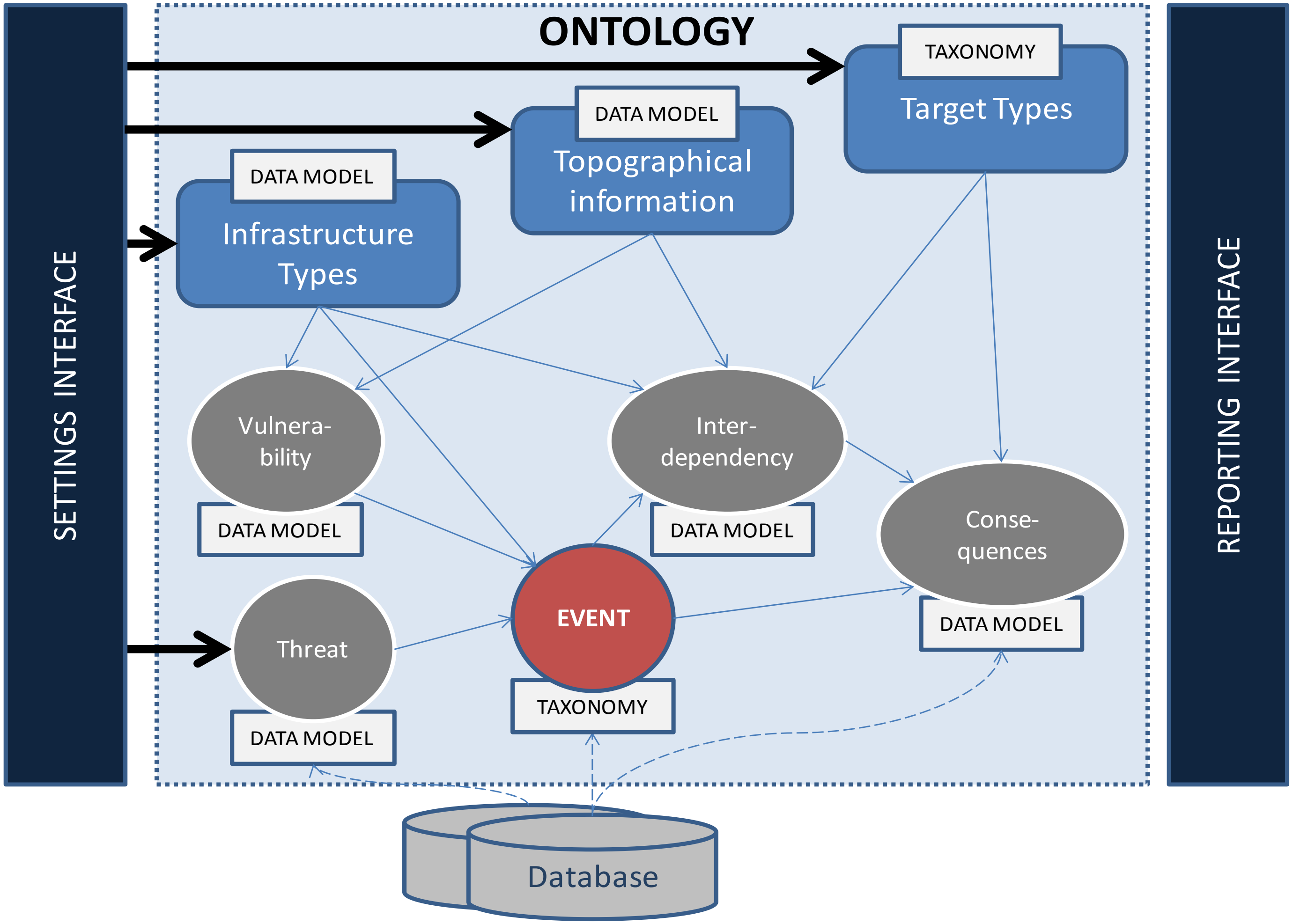


Criticality map



(dependency index, influence gain) plan

THREVI^2 - PATHFINDER Tool

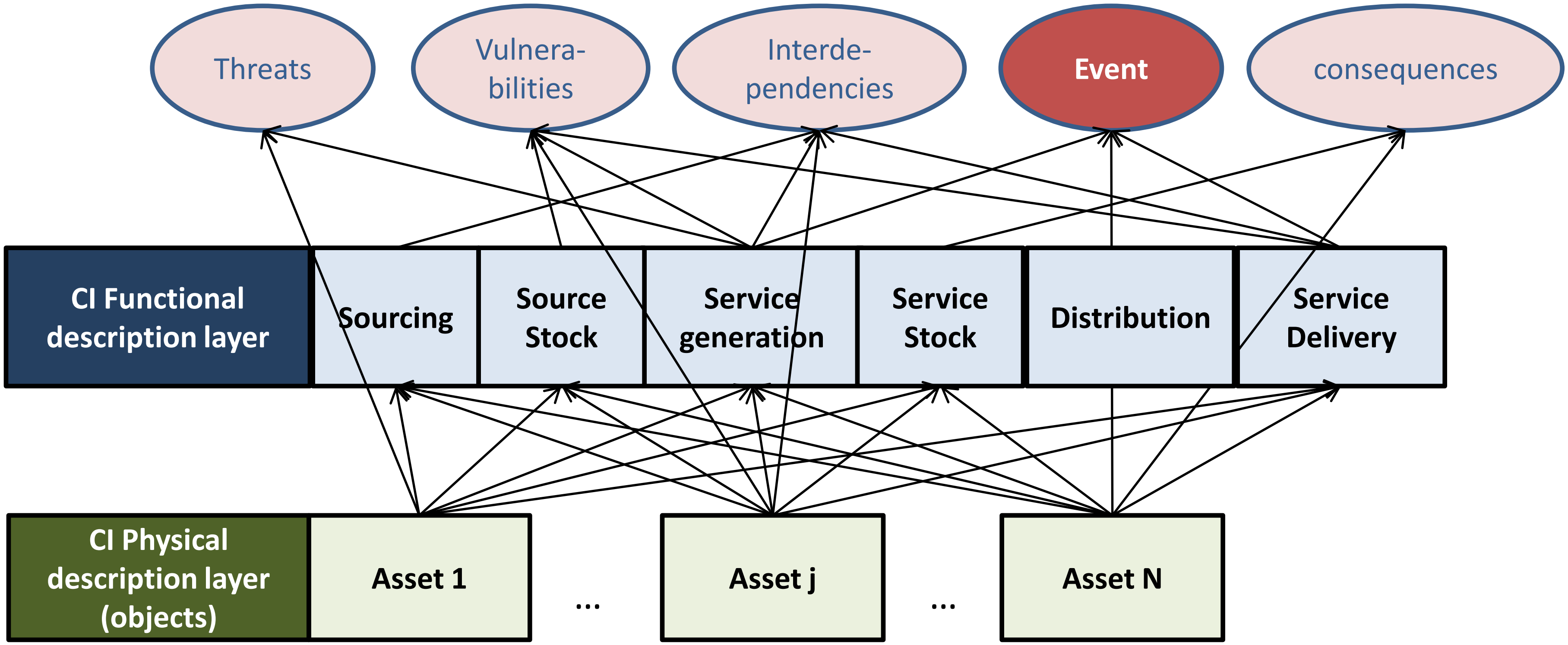


THREVI^2

hreat - ulnerability ath
dentification for
ritical nfrastructures

Infrastructure Topology and Asset Taxonomy (ITAT) framework

THREVI^2



Threats

Vulnera-bilities

Interde-pendencies

Event

consequences

CI Functional description layer

Sourcing

Source Stock

Service generation

Service Stock

Distribution

Service Delivery

CI Physical description layer (objects)

Asset 1

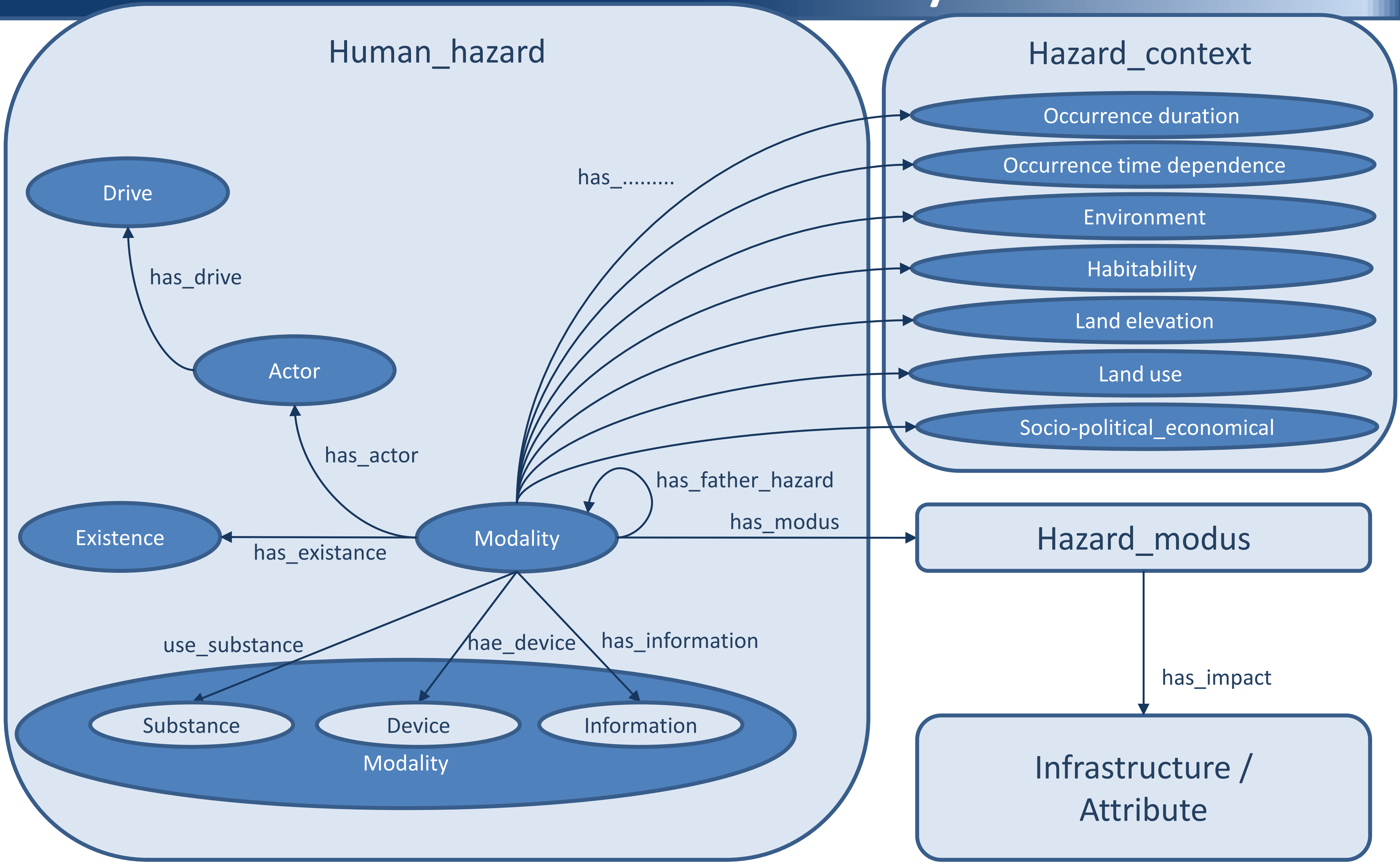
…

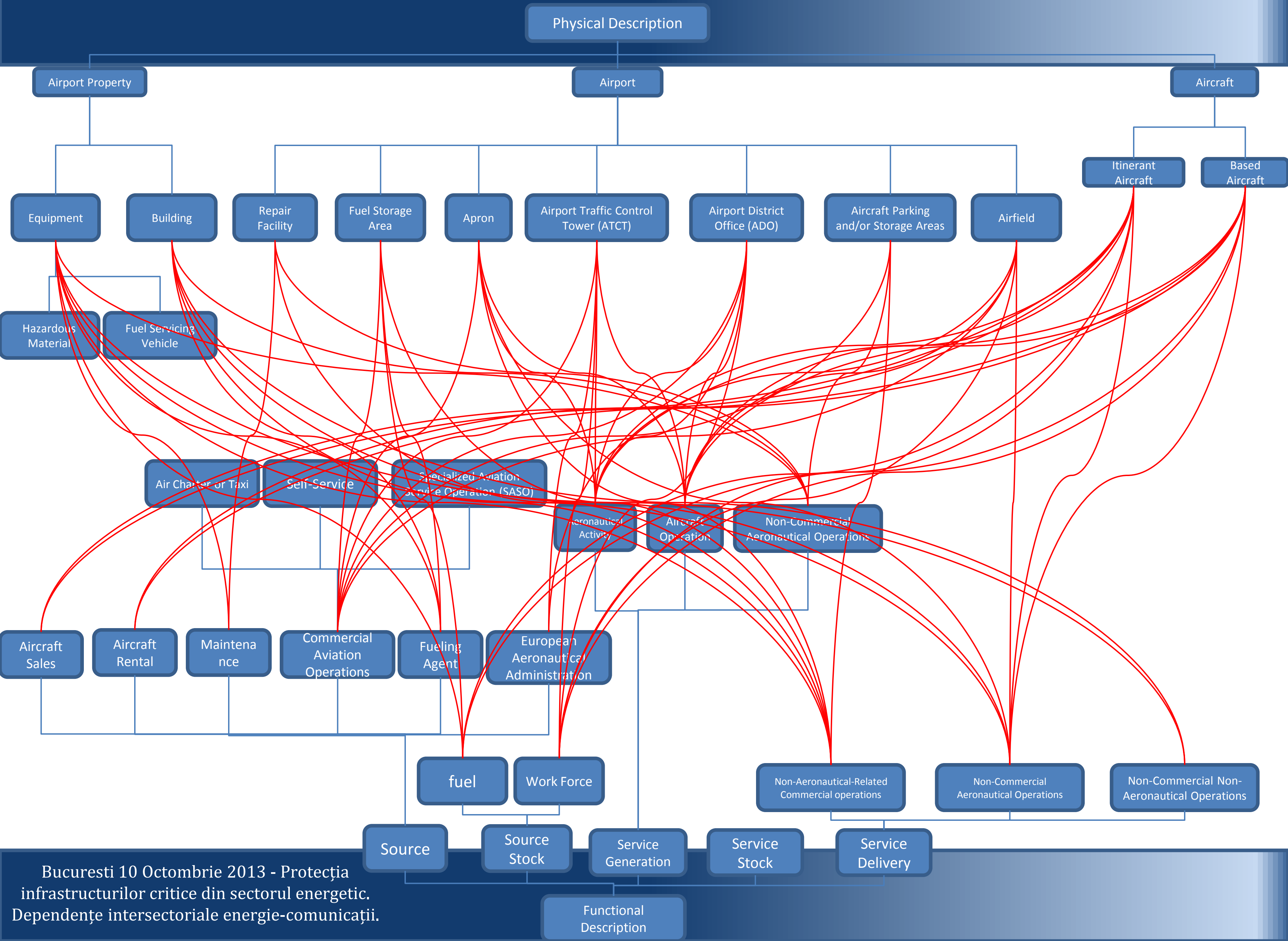
Asset j

…

Asset N

Event taxonomy





Physical Description

Airport Property

Airport

Aircraft

Itinerant Aircraft

Based Aircraft

Equipment

Building

Repair Facility

Fuel Storage Area

Apron

Airport Traffic Control Tower (ATCT)

Airport District Office (ADO)

Aircraft Parking and/or Storage Areas

Airfield

Hazardous Material

Fuel Servicing Vehicle

Air Charter or Taxi

Self-Service

Specialized Aviation Service Operation (SASO)

Aeronautical Activity

Aircraft Operation

Non-Commercial Aeronautical Operations

Aircraft Sales

Aircraft Rental

Maintenance

Commercial Aviation Operations

Fueling Agent

European Aeronautical Administration

fuel

Work Force

Non-Aeronautical-Related Commercial operations

Non-Commercial Aeronautical Operations

Non-Commercial Non-Aeronautical Operations

Source

Source Stock

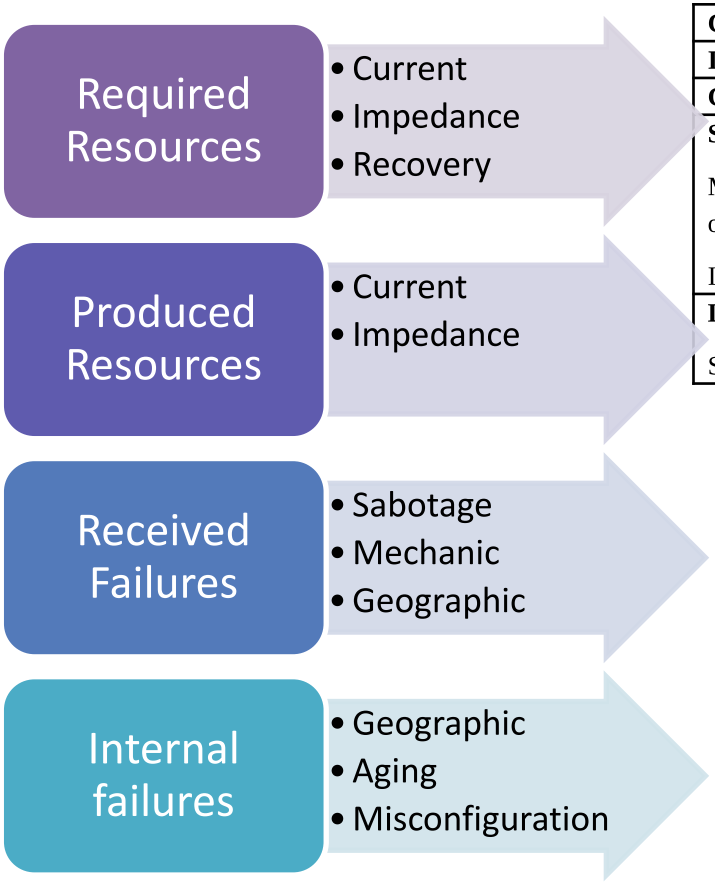
Service Generation

Service Stock

Service Delivery

Functional Description

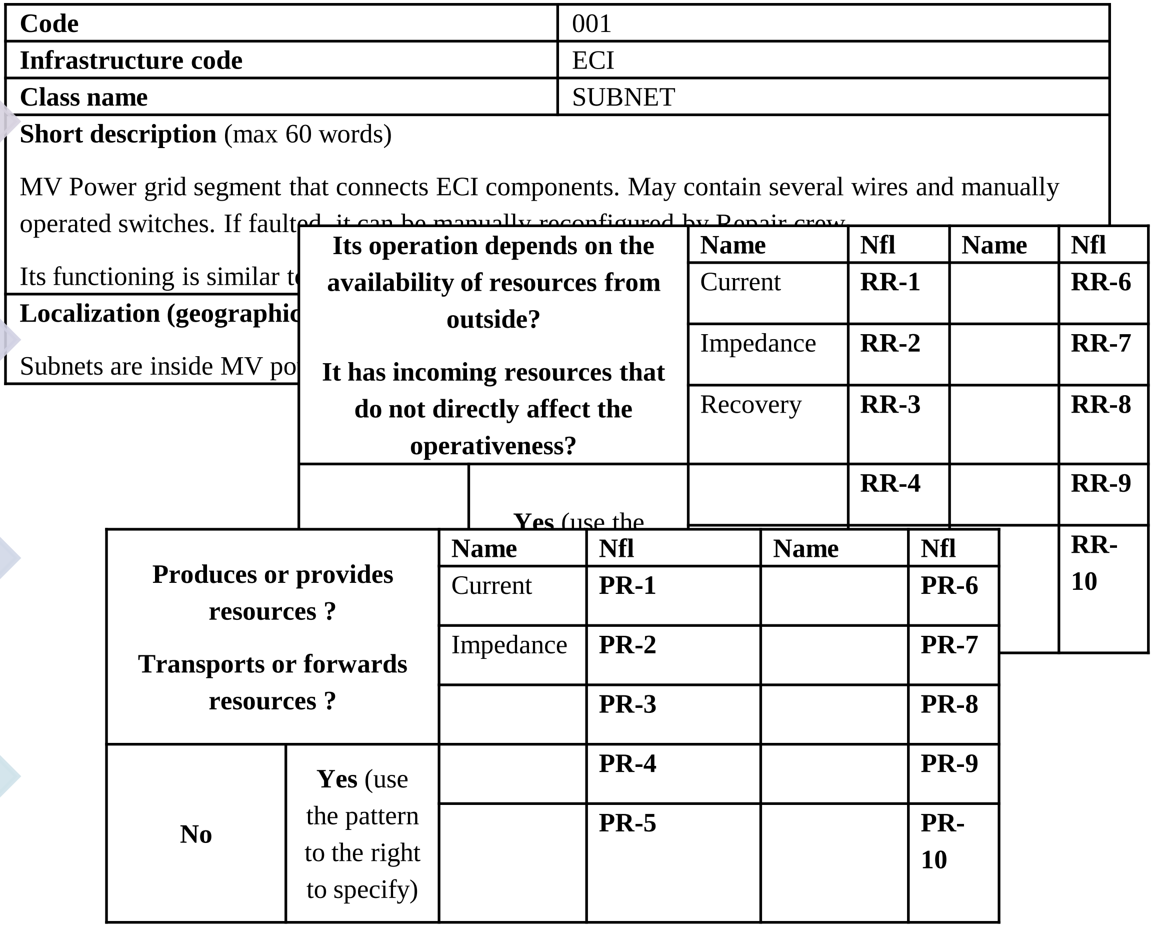
ENTITY DESCRIPTION USING QUESTIONNAIRES


Required Resources
- Current
- Impedance
- Recovery

Produced Resources
- Current
- Impedance

Received Failures
- Sabotage
- Mechanic
- Geographic

Internal failures
- Geographic
- Aging
- Misconfiguration

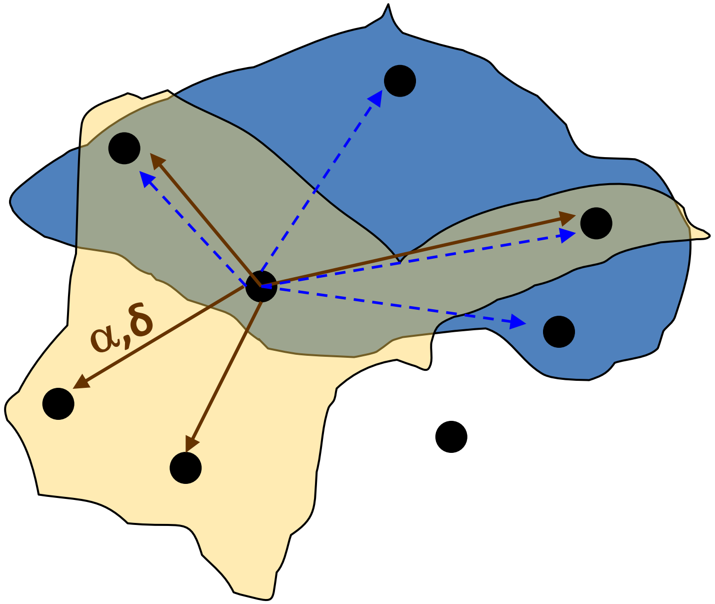


Code	001
Infrastructure code	ECI
Class name	SUBNET
Short description (max 60 words) MV Power grid segment that connects ECI components. May contain several wires and manually operated switches. If faulted, it can be manually reconfigured by Repair crew. Its functioning is similar t	
Localization (geographic	
Subnets are inside MV po	

		Name	**Nfl**	**Name**	**Nfl**
Its operation depends on the availability of resources from outside? **It has incoming resources that do not directly affect the operativeness?**		Current	**RR-1**		**RR-6**
		Impedance	**RR-2**		**RR-7**
		Recovery	**RR-3**		**RR-8**
	Yes (use the		**RR-4**		**RR-9**
					RR-10

		Name	**Nfl**	**Name**	**Nfl**
Produces or provides resources ? **Transports or forwards resources ?**		Current	**PR-1**		**PR-6**
		Impedance	**PR-2**		**PR-7**
			PR-3		**PR-8**
No	**Yes** (use the pattern to the right to specify)		**PR-4**		**PR-9**
			PR-5		**PR-10**

Several "concept" of proximity



Geographyc proximity .

Cyber proximity.

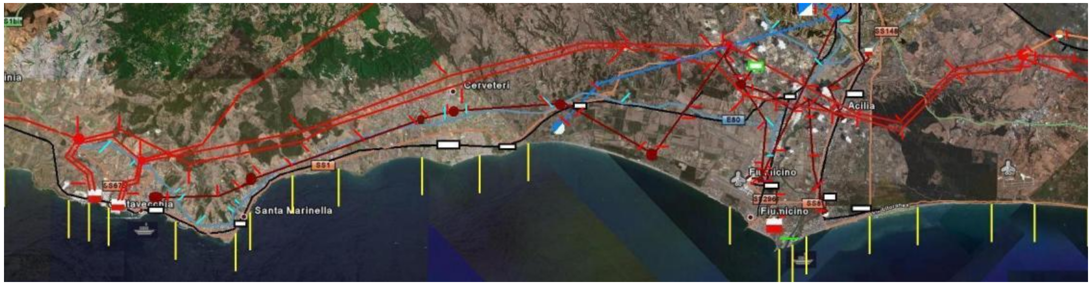
Dependency among antity are modelled via weight incidence matrices

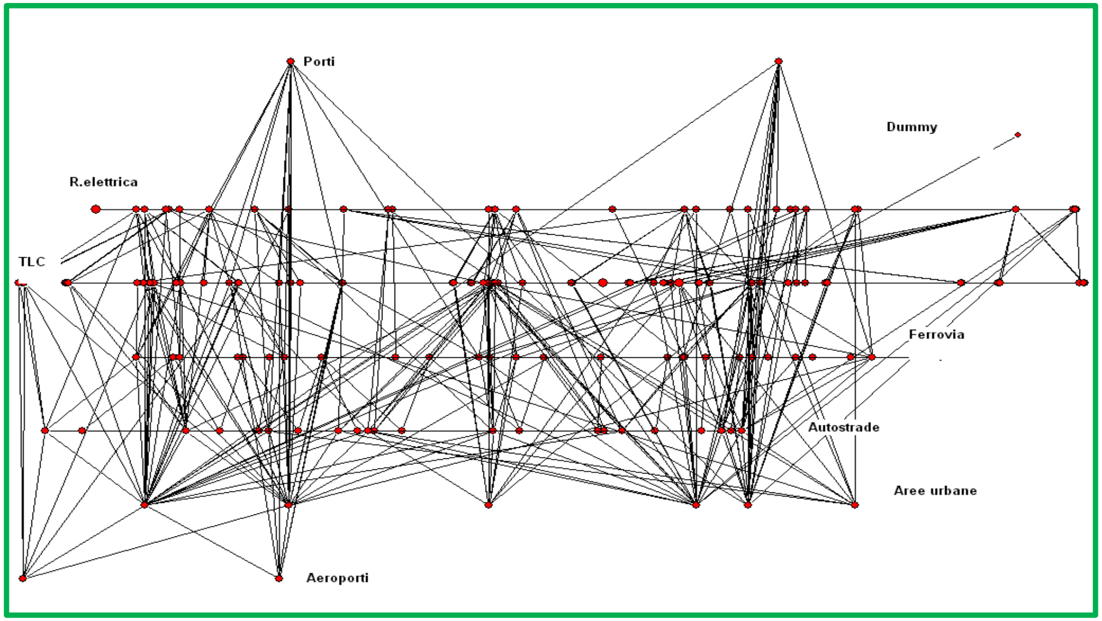
(each one describe a specific type of interaction – hence generate different set of neighbour)

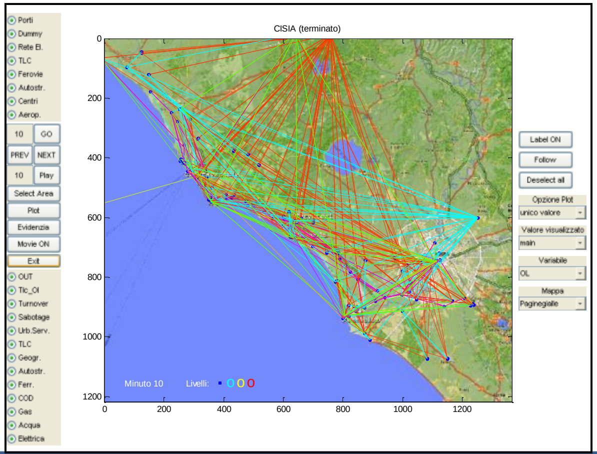
Any arc is characterised by delay δ and attenuation/gain α A.

CISIA Case-study 2007

Infrastructure	Macro-components
Electric Grid	35
Urban areas	6
Air-ports	2
Sea-ports	2
Railway	27
Highways	23
TLC	141







Opzione Plot: unico valore

Valore visualizzato: main

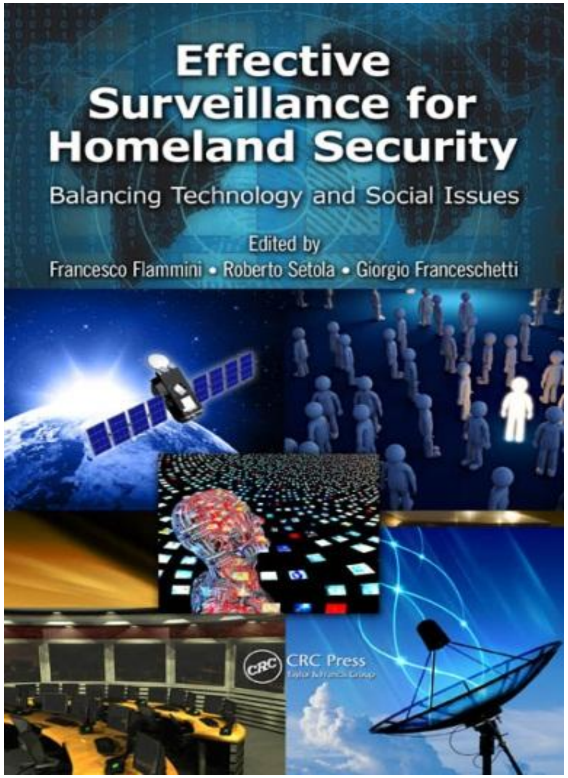
Variabile: OL

Mappa: Paginegialle

233 Entities
844 Link

SELEX Sistemi Integrati
Una Società Finmeccanica

My more recent book


Effective Surveillance for Homeland Security
Balancing Technology and Social Issues
Edited by
Francesco Flammini • Roberto Setola • Giorgio Franceschetti
CRC Press

. lammini, \. etola, . . ranceschetti,
“ffective urveillance for omeland ecurity, \ ress,

r.setola@unicampus.it

IIM with Technician point of view

Identify IIM parameters on the base of operative technicians' expertise (operators' perceptions)

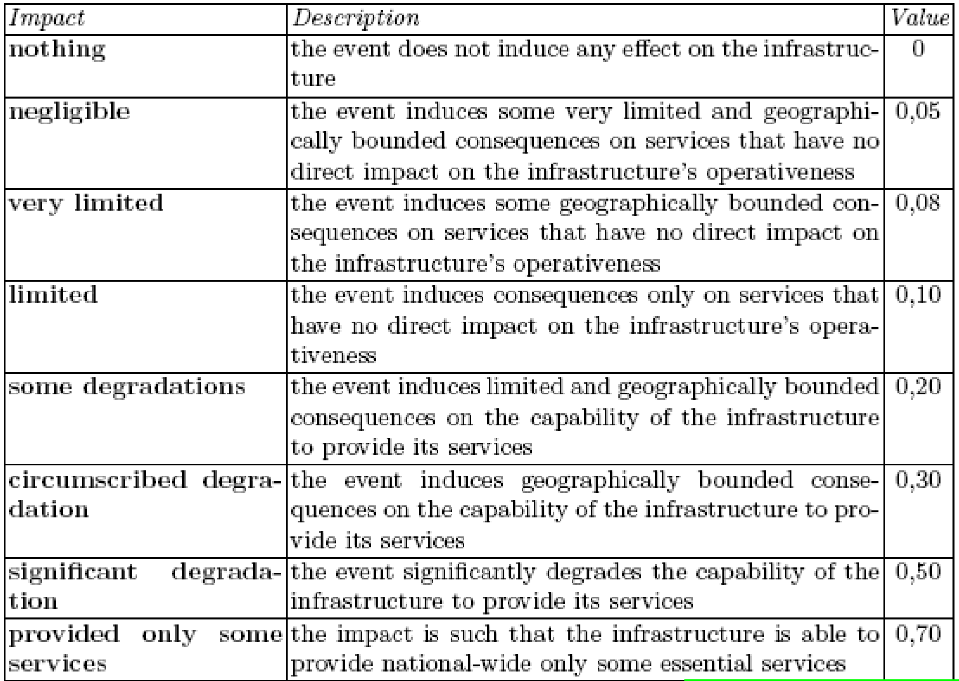
Ask to experts the follow question

Which is the impact on *your* infrastructure of the complete absence of services provided by *yyy* infrastructure for a time period of *zzz*

In this way we try to acquire directly from their expertise an estimation about the dependency parameters to set-up a technical oriented IIM

R. Setola, S. De Porcellinis, and M. Sforna "Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model", *Int. J. Critical Infrastructure Protection (IJCIP),* pp. 170 - 178, 2009.

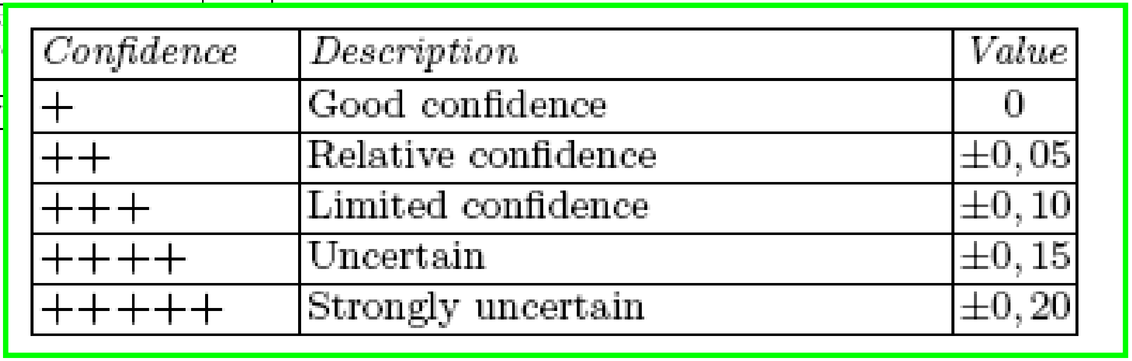
How to answer



Impact	*Description*	*Value*
nothing	the event does not induce any effect on the infrastructure	0
negligible	the event induces some very limited and geographically bounded consequences on services that have no direct impact on the infrastructure's operativeness	0,05
very limited	the event induces some geographically bounded consequences on services that have no direct impact on the infrastructure's operativeness	0,08
limited	the event induces consequences only on services that have no direct impact on the infrastructure's operativeness	0,10
some degradations	the event induces limited and geographically bounded consequences on the capability of the infrastructure to provide its services	0,20
circumscribed degradation	the event induces geographically bounded consequences on the capability of the infrastructure to provide its services	0,30
significant degradation	the event significantly degrades the capability of the infrastructure to provide its services	0,50
provided only some services	the impact is such that the infrastructure is able to provide national-wide only some essential services	0,70
quit complete stop	the impact is such that the infrast provide, in some geographically ar sential servicese	
stop	the infrastructure is unable to prov	

The experts have to use linguistic value extracted from a predefined scale

They have also to express a **grade of confidence** (accuracy) about each one of their estimation



Confidence	*Description*	*Value*
+	Good confidence	0
++	Relative confidence	±0, 05
+++	Limited confidence	±0, 10
++++	Uncertain	±0, 15
+++++	Strongly uncertain	±0, 20