

The need to improve local self-awareness in CIP/CIIP

ENEA

Italian National Agency for New Technologies,
Energy and the Environment

Sandro Bologna

bologna@casaccia.enea.it

University
CAMPUS Bio-
Medico di Roma



Roberto Setola

r.setola@unicampus.it

Presentation Outline

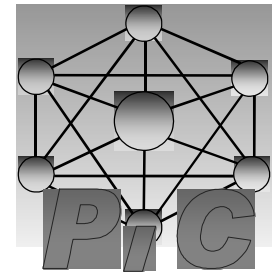
- The third millennium infrastructures' framework
- Some 'interdependency-related' episodes
- CIP/CIIP domains of actions
- What CIP/CIIP need: cultural action and local self-awareness

Let us introduce me

Researcher in System Theory (Modeling & Simulation of complex system)



Technical responsible of Italian Government Working Group on Critical Information Infrastructure Protection (PIC)



Member of G8 Senior Expert Group on CIIP



Critical Infrastructures

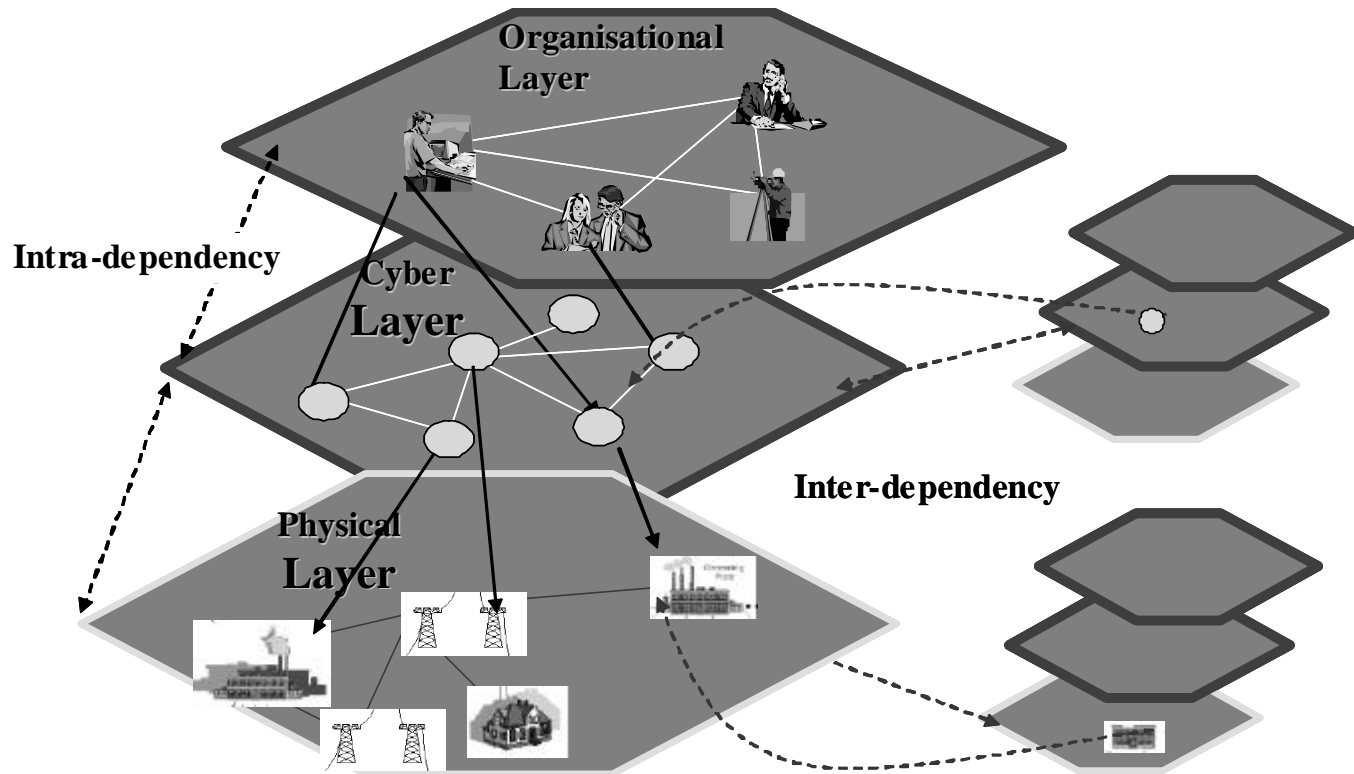
Critical Infrastructures *are* systems and assets, whether physical or virtual, so vital for a state that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[US Patriot Act 2001]

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of European Citizens or the effective functioning of the EU or the governments of its Member States

[EU Commission 2005]

Inter- and Intra-dependencies links





**Some episodes from literature that
emphasize the new role of inter-
dependencies and their consequences**

1998 – Galaxy IV (USA)

Source

Failure in a communication satellite

Lesson learned

There exist many hidden interdependencies that can amplify the consequences of any failure

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 an Internet connection to penetrate into SCADA of sewage treatment plant

Consequences

- 1.200.000 liters of raw sewage dispersed in the environment

Lesson learned

- SCADA may be cracked
- Insider may have enough information to crack a SCADA system
- Connect SCADA on public network increase its vulnerability

2003 - Slammer

Source

bug into a common used software (Microsoft SQL server)

Consequences (some...)

- Finance: in USA 13.000 ATM out-of-work; in Italy 11.000 postal office off-line
- Emergency: 911 in Seattle stopped
- Transportation: many flights delayed or canceled in Huston
- Electricity: SCADA of two US utilities stopped

Lesson learned

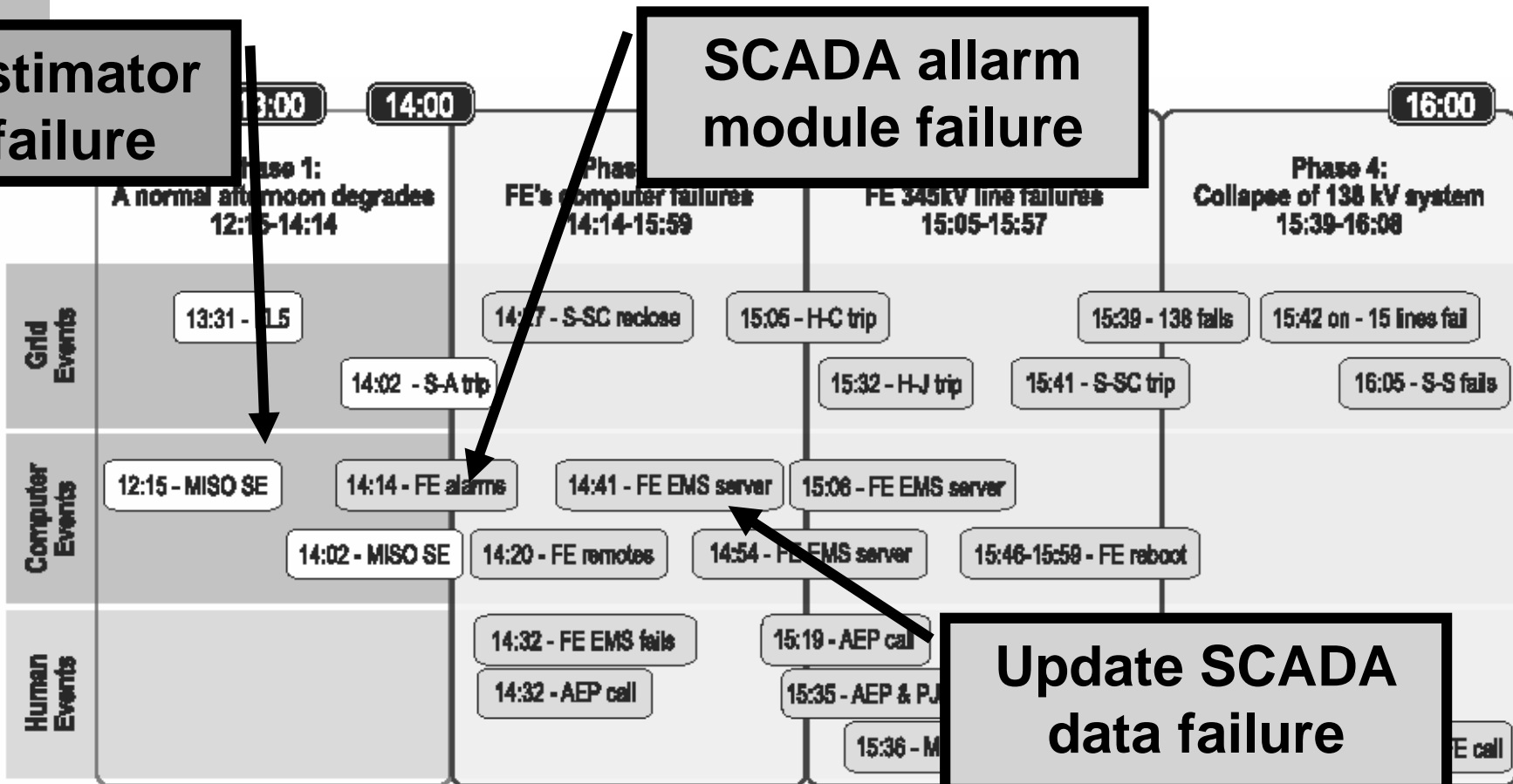
- Even in the presence of a critical vulnerability, patch are not (always) installed
- Internet-related threats are global (world) threats
- Interdependencies, cascade and domino effects complicate the scenario

2003 – US & Canada blackout

Estimator failure

SCADA allarm module failure

Update SCADA data failure



2004 – Italy

Source

an incident at 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

Lesson learned

- Do not forget physical threats !
- Hidden (and dangerous) interdependencies

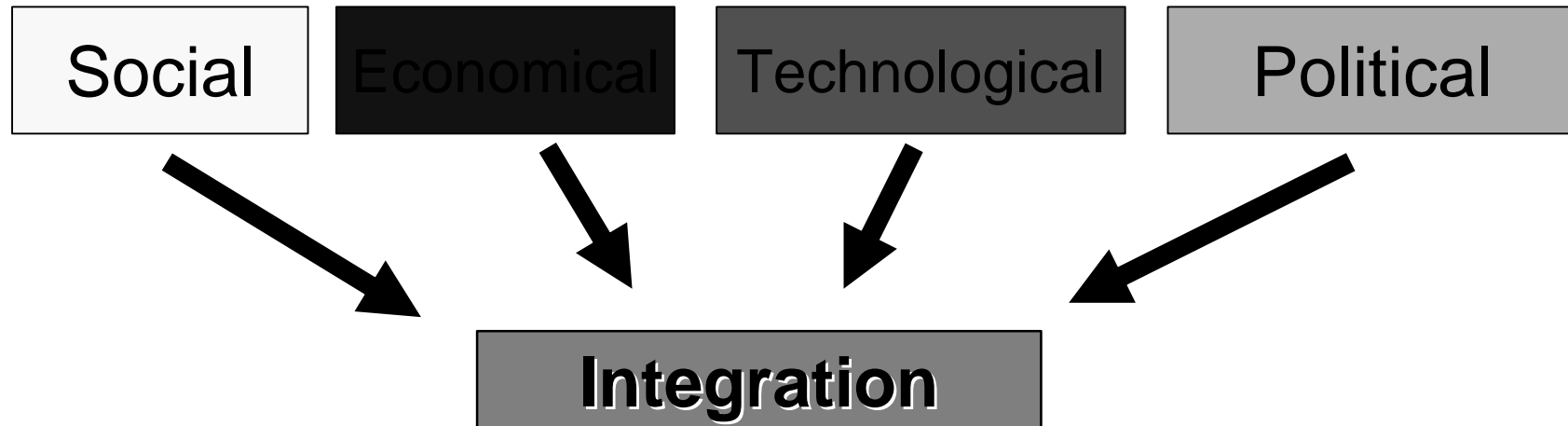
Corner-stone elements

- Increased role of ICT in Critical Infrastructures
- Increased interdependencies among CI
- Increased threats both natural and malicious (terrorism ?)
- Need to consider both cyber and physical threats
- Physical events affect cyberspace, and cyber events may have dramatic consequences on physical world

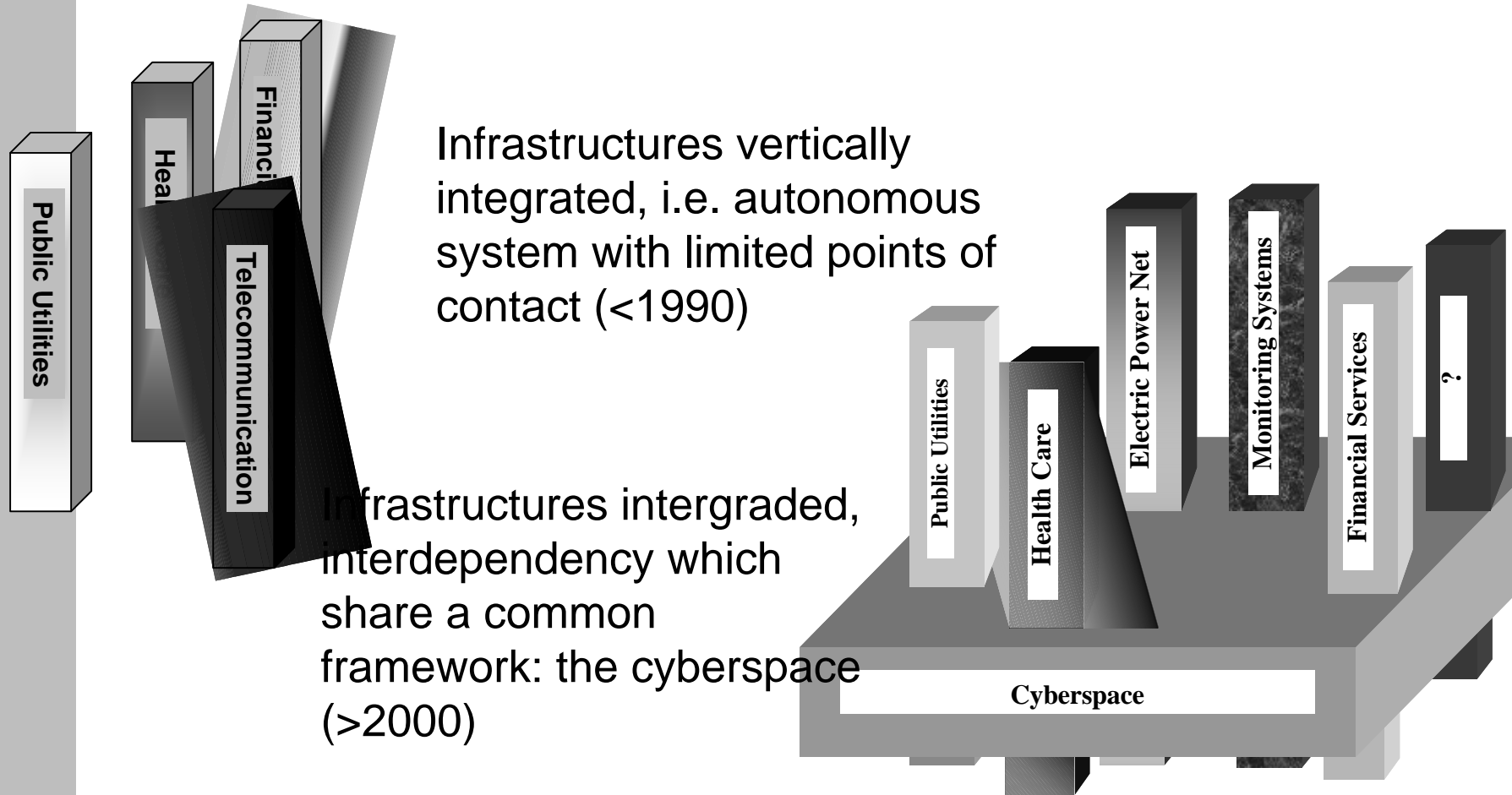
Some years ago, in Rome, someone told that a good strategy for manage complex system is

Dividit et Imperat

Today, for a lot of GOOD reasons...



Third millennium socio-techno scenario



CIP & CIIP

We need strategies to guarantee that the different infrastructures are able to correctly and continuously supply their **services** in spite of any events.

Note that the emphasis is on service provided rather than on **assets** (this is a more challenge task !)

CIP – Critical Infrastructure Protection

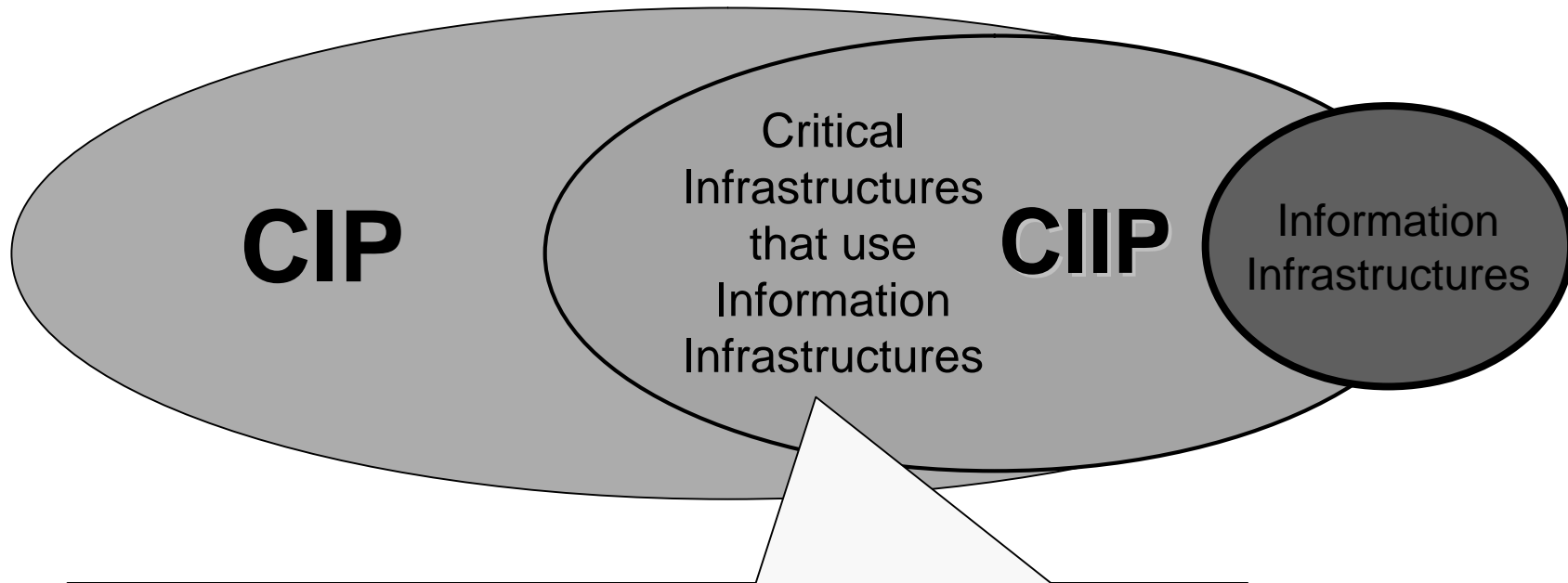
Strategies to improve security, correctness and availability of services supplied by critical infrastructures with respect to any malicious or natural events (physical and/or cyber)

CII – Critical Information Infrastructure

In literature there are at least two different meanings for this expression:

- “The” information infrastructure, i.e. Internet
- ICT elements devoted to monitor, control, supervision (physical) critical infrastructures (i.e. a “component” needs to guarantee critical infrastructure functionality)

Critical Information Infrastructure Protection



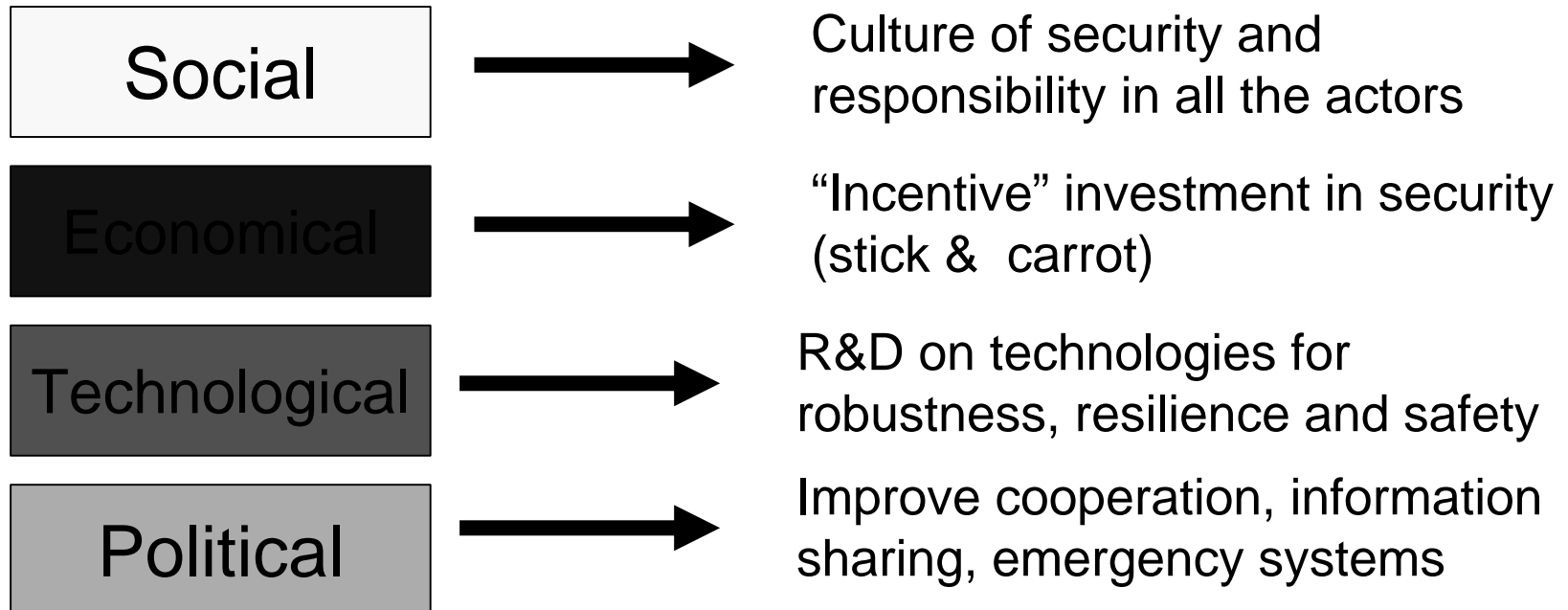
Protection of Infrastructures, critical for the Country, that use for their management, control, monitor or supervising one or more information infrastructures

CIIP¹ IT security

- The focus is on “security” of CI services
- Firewall, anti-virus, CERTS etc. are not tailored on CI needs (e.g. SCADA, DCS, etc.)
- We need to consider consequences of cascade and domino phenomena
- We need to have a multi point-of-view which consider needs and requirements of the different CI (together with that of IT)

Critical Infrastructures are becoming a huge and incredible complex system of systems

This introduce vulnerabilities, and to improve system robustness we had to work on



CIP/CIIP vs Y2K (1)

	<i>Y2K</i>	<i>CIP/CIIP</i>
<i>Technical aspect</i>	Easy	Complex
<i>Problem source</i>	Well known and single	Unknown, multiple and concurrently
<i>Time scheduling</i>	A single event with a well known time scheduling	Many events can happen in any time (even concurrently) and with unpredictable sequences.
<i>Type of the problem</i>	Well known: a bug in software	Unpredictable either accidental or malicious and may affect any component of any critical infrastructures.

CIP/CIIP vs Y2K (2)

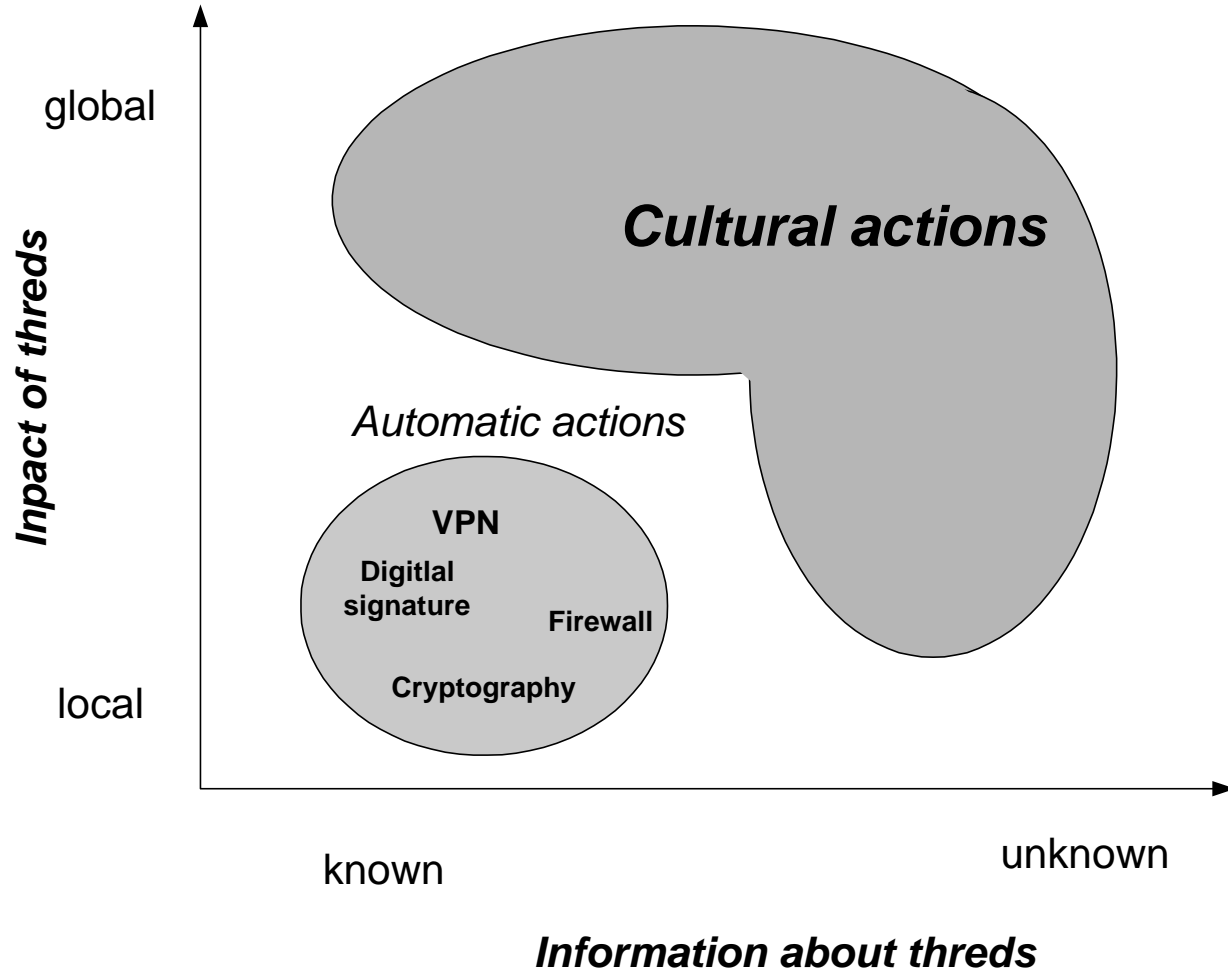
	<i>Y2K</i>	<i>CIP/CIIP</i>
<i>Strategies to overcome it</i>	Easy and well known (difficulties only for implementation process).	Unknown
<i>Relation with technological innovation</i>	The use of last generation of off-the-shelf software was generally a good solution to overcome the problem	Actually, there is no technology able to guarantee problem solving

CIP/CIIP vs Y2k (3)

While for Y2K solutions were quite always limited to technological level (e.g., adopt the latest version of the software) for CIP/CIIP technological solutions represent only a component of a more challenge task.

CIP/CIIP strategies must be primarily based on enhancement of the human factor and specifically on cultural actions.

CIP/CIIP needs cultural actions



From technical point of view

Think **GLOBALLY** act **LOCALLY**

We need to improve LOCAL capability to autonomously reacts to anomaly situations in order to prevent cascade failure and to guarantee minimum level of services

From centralized to decentralized control strategies ?

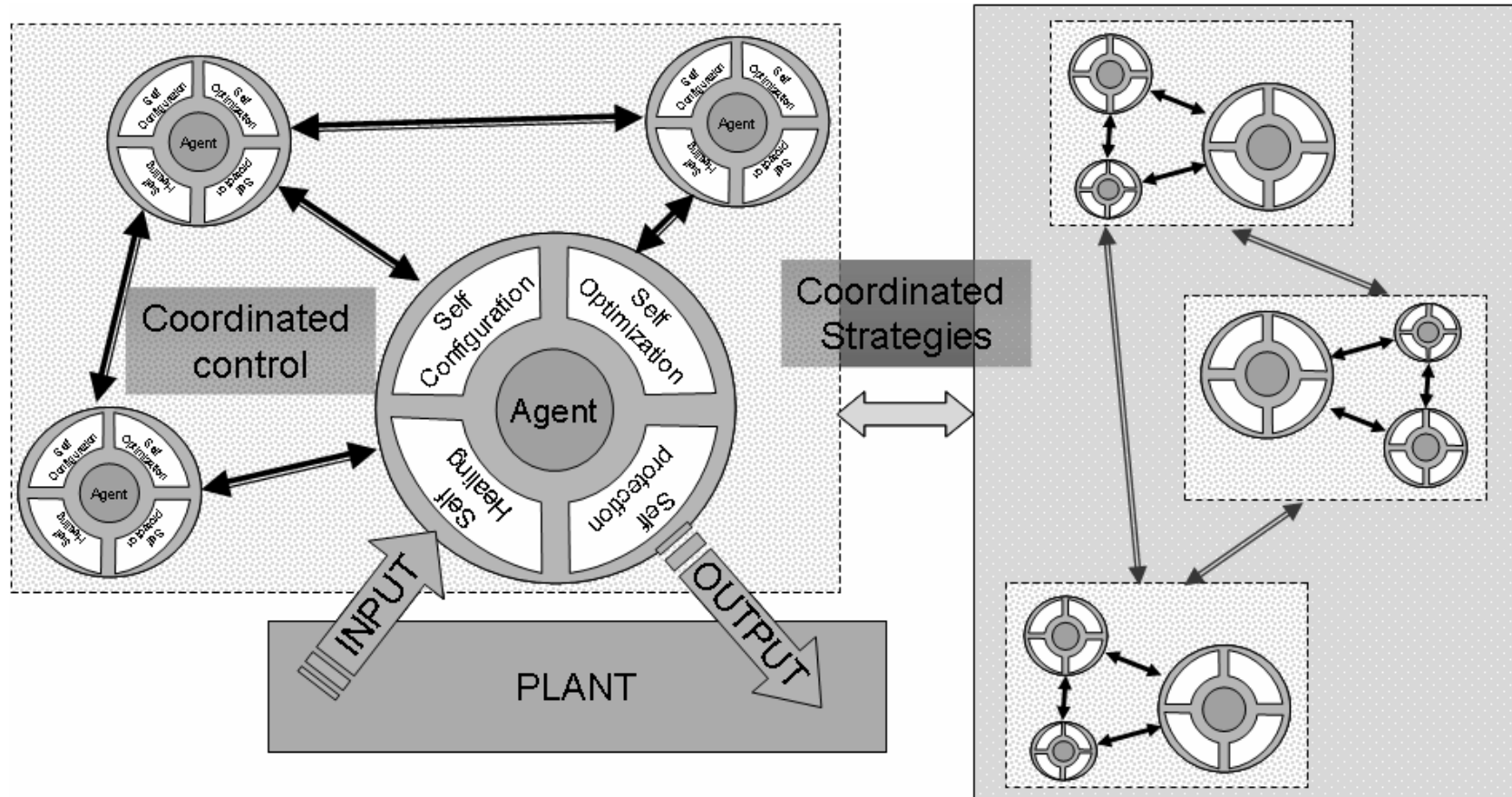
Centralized control strategies are able to perform global optimization and guarantee high efficient strategies, **BUT** they are prone to vulnerabilities induced by interdependencies especially for that which concern the communication network (erroneous command or absence of commands)

Decentralized strategies are more able to prevented cascade failure and to improve “local” resilience, **BUT** they may not guarantee global-optimal behavior neither high level of efficiency

Local self awareness strategies

Even interoperability of system create vulnerabilities, and technological innovation is at the base of CIP/CIIP problem, also its solution should be based on an increased (and appropriate) use of information sharing and technological innovation!

Hybrid control strategies



Merge local and global strategies

- **Local vision:** each element should be able to identify the presence of internal or external failure (self-healing capability) and, consequentially, autonomously generates behaviours to mitigate the consequences
- **Global vision:** to adequately understanding its environment the agent needs to exchange information with the other agents located in the neighbourhood and with elements able to supply global view

Thank you

Questions ?

r.setola@unicampus.it