A PUBLIC PRIVATE PARTNERSHIP FOR A NATIONAL CERT: EVALUATING THE CYBER-RISK IN CIP

Prof. Stefano Panzieri

Dept. of Computer Science & Automation

Italian Association for Critical Infrastructures

Study Group on National Cyber Security Strategies of Prime Minister Council

A I I C (Associazione Italiana esperti Infrastrutture Critiche)

scientific association born in 2006 to promote an interdisciplinary culture able to develop:

- **Strategies**
- **Methodologies**
- **Tools**
- **Technologies**

for the Protection of Critical Infrastructures in Italy

AIIC Associate Companies

EUSTEMA
Making Innovation

IBM

TELECOM ITALIA

THALES

Terna

Enel
L'ENERGIA CHE TI ASCOLTA.

D'APPOLONIA

FASTWEB
un passo avanti

THEOREMATICA

Intermatica
global solution carrier

Deloitte.

FORMIT

RSE
Ricerca Sistema Energetico

INTERGRAPH

akhela

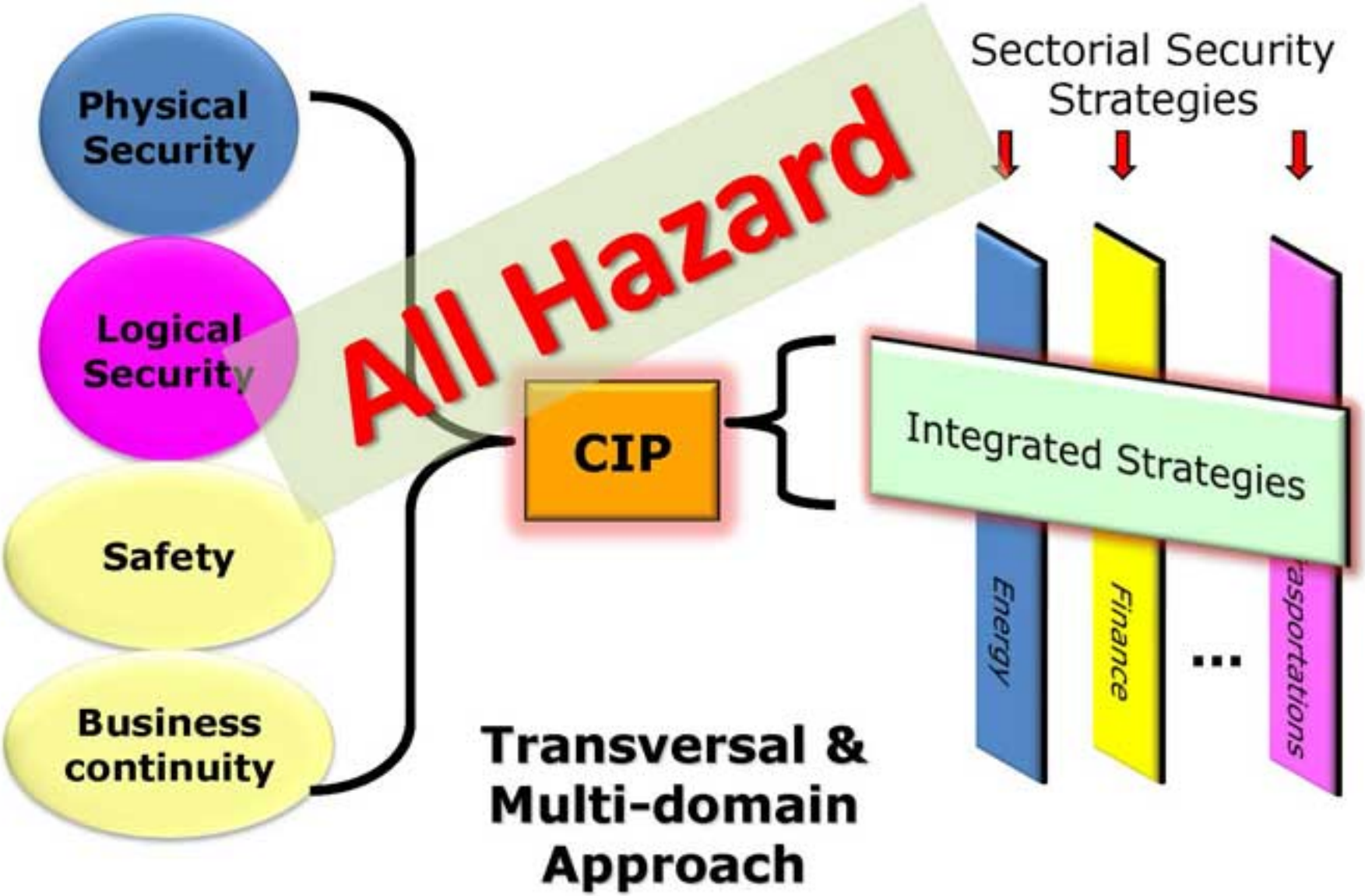
ASTER
TECHNOLOGY & ENGINEERING

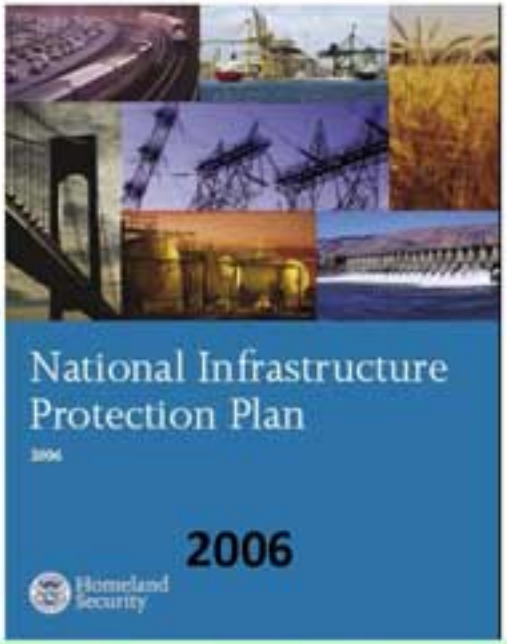
programatic

sia

mediaservice.net
CORPORATE SECURITY & IMAGE

Which Security?





Public Private Partnership

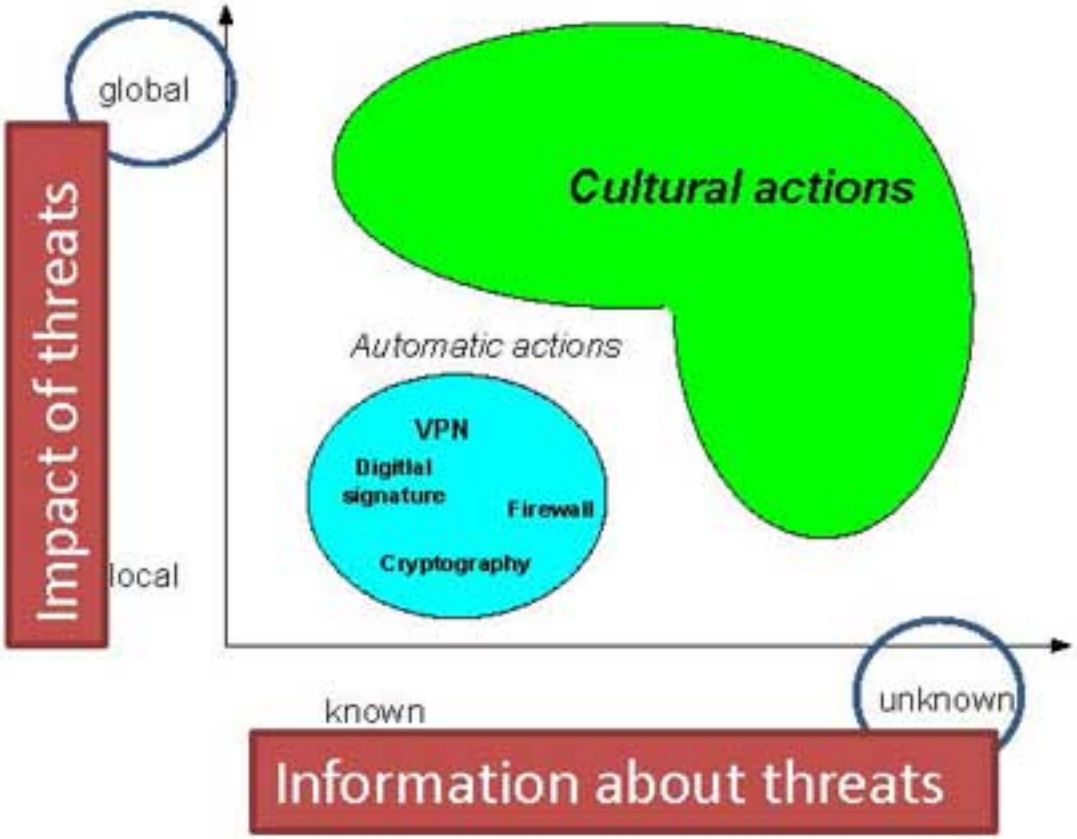
European Directive 2008/114/EC

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

January 12, 2009
(in Italy ratified on April 2011
DL 11/4/2011, n. 61)

Direct **terrorist attacks** and **natural, manmade**, or **technological hazards** could produce catastrophic losses …. Attacks using components of CI/KR as weapons could have even more devastating physical and psychological consequences

EVOLUTION OF RESPONCE



A *collaborative* security culture is mandatory !

Required Synergy

- COM(2009) 149.
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: **Protection of Critical Information Infrastructure**
  - Guarantee the maximum of **security and resilience**
  - Shared responsibility: **no one** has alone the required instruments

Digital Agenda

- COM(2010) 245
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: **A Digital Agenda for Europe.**
  - A great obstacle among others: the increasing of cyber crime
    - Within 2012: **National CERTs**
    - Within 2013: **European Center for Cyber Crime**

- A great discussion in **Italy** in this moment for the formulation of **Italian Digital Agenda** in June that will be mainly related to
  - Hi-capacity telecommunication networks
  - Cloud Computing / Data Centers

With, we hope, some attention to cyber security...

(Study Group on NCSS)

National/Governmental CERTs

- COM(2011)163
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS **on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'**

- CIIP ACTION PLAN: Action for Preparedness and prevention:
  - The **European Public-Private Partnership for Resilience** (EP3R): it aims at fostering the cooperation between the public and the private sectors on strategic EU security and resilience policy issues. ENISA played a facilitating role for the activities of EP3R.

  - [Have been developed] the **minimum set of baseline capabilities and services and related policy recommendations for National/Governmental CERTs** to function effectively and act as the key component of national capability for preparedness, information sharing, coordination and response. These results will be a building block to establish, with the support of **ENISA**, a network of well-functioning National/Governmental CERTs in all Member States by 2012. Such a network will be the backbone of the European Information Sharing and Alert System (EISAS) for citizens and SMEs, to be built with national resources and capabilities by 2013.

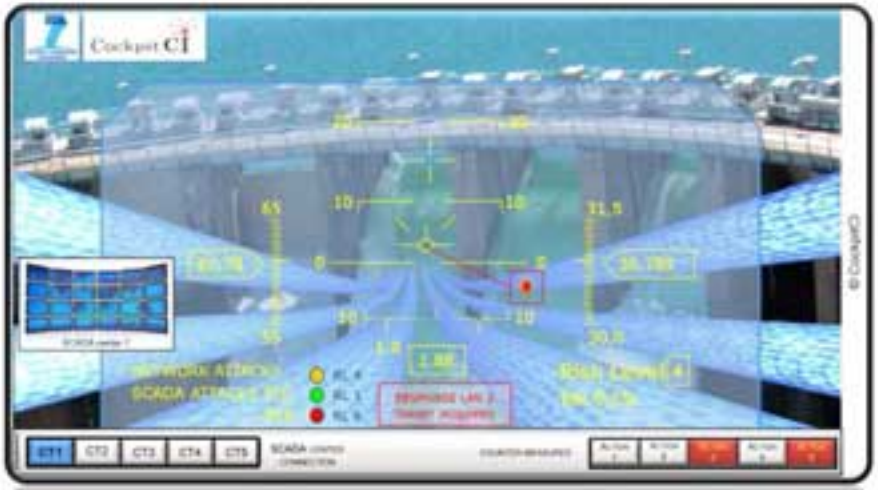
Public Private Partnership

- A Public Private Partnership **can be the answer** for:
  - Developing of common intelligence models (how manage data)
  - Information sharing
  - Definition of common (hence effective) answers to cyber threat
  - Managing a CERT able to give early warnings (easier if participated by private sector)
  - Information exchange about governmental studies as well as industrial vulnerabilities
  - Definition of prevention actions in the private sector
  - Divulgation of best practices in private sector
  - Evaluation of economic losses
  - Public opinion
  - Education

ENISA Good practice guide on PPP

- **ENISA**, *Cooperative Models for Effective Public Private Partnership – Good Practice Guide, 2011.*
- Some good reasons to participate in a PPP for the private sector:
  - The organization recognize that the impact of a problem goes beyond the boundaries of the organization itself
  - Non senior management in the organization to tackle with security problems
  - The National (Cyber) Security Strategy is not adequate
  - The organization want influence the upcoming N(C)SS or on the sector regulation
  - An organization want to better understand its vulnerabilities
  - The organization recognize that the information sharing is too low
  - There is a lack of trust between companies of the same sector

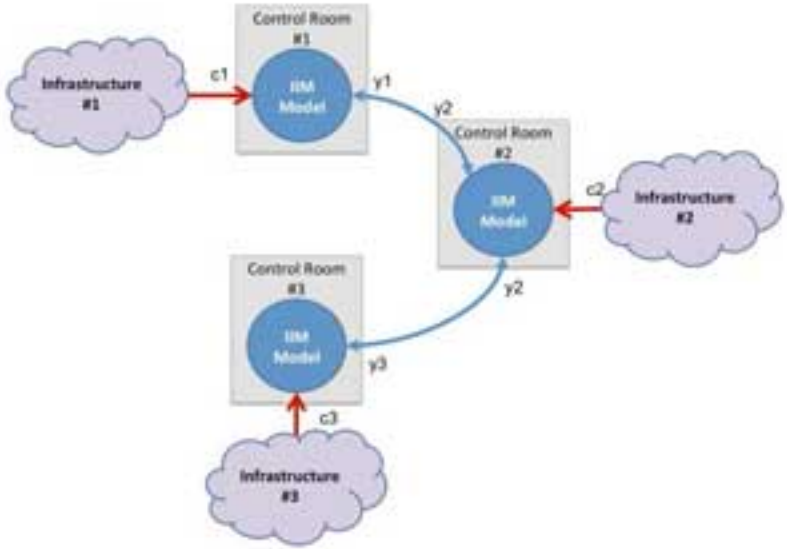
FP7 - CockpitCI



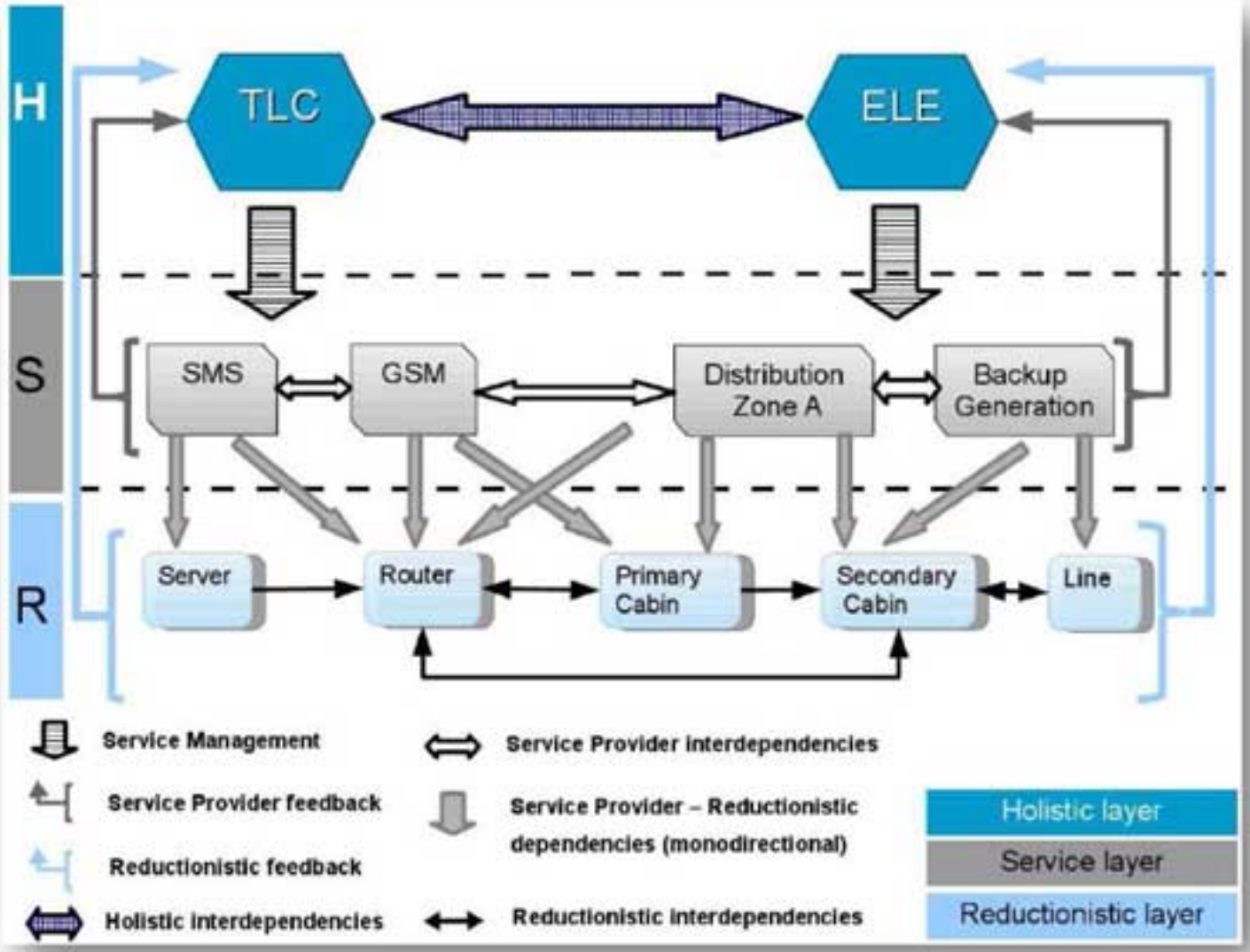
- CockpitCI aims to improve the resilience and dependability of Critical Infrastructures (CIs) by the automatic detection of cyber threats and the sharing of real-time information about attacks among CI owners. This objective highlights the importance of achieving cyber awareness and to achieve it beyond the boundary of the single CI. A particular importance is given to the sharing of real-time information among CI

FP7 - CockpitCI

- CockpitCI aims to identify, in real time, the CI functionalities impacted by cyber-attacks and assess the degradation of CI delivered services. This information should be conveyed to SCADA and security operators to greatly increase their awareness of the situation and improve their capability to handle the situation



THE MIXED HOLISTIC-REDUCTIONISTIC MODELLING PERSPECTIVE

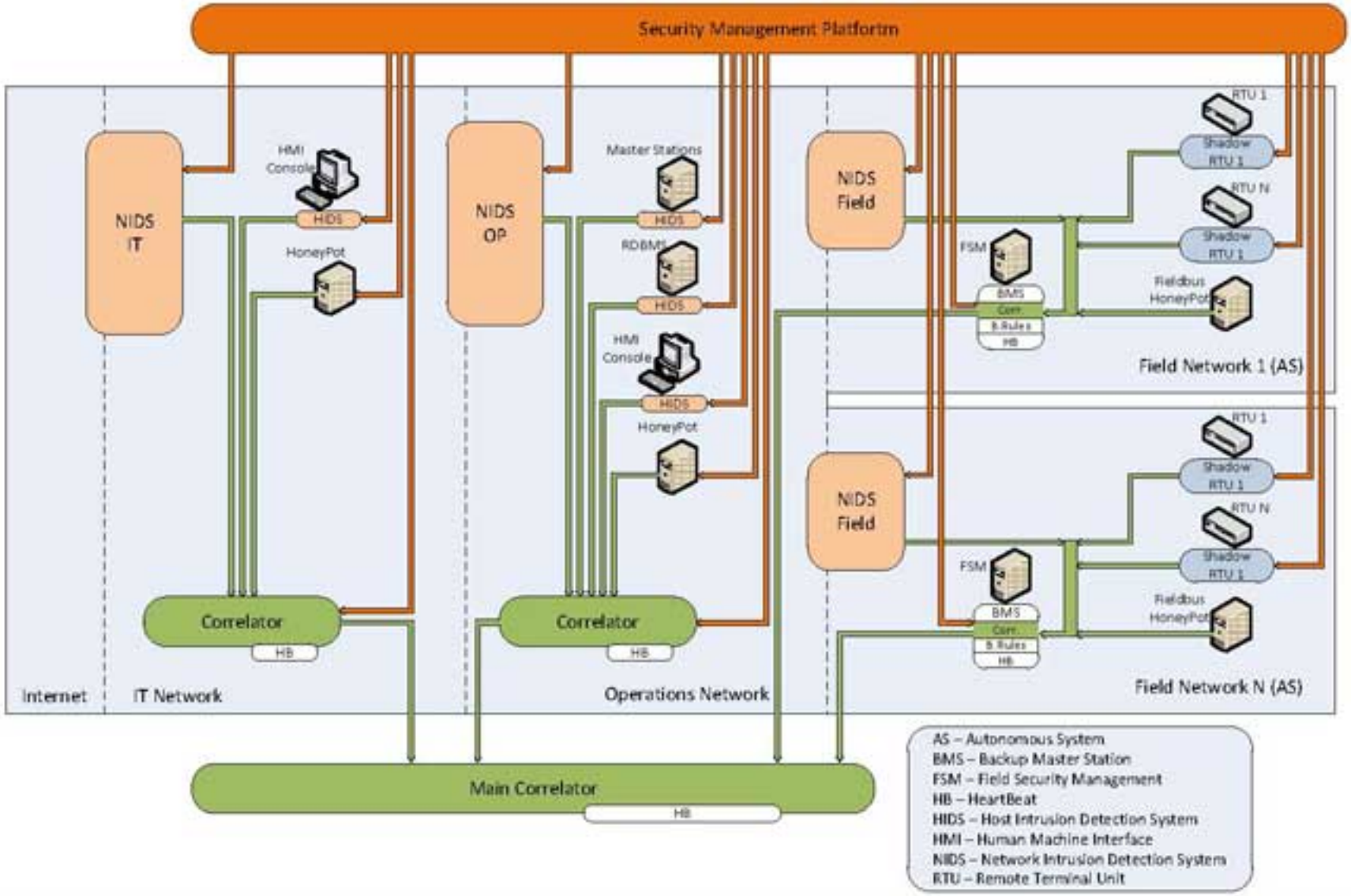


Behaviours (physical or logical or political) not emerging fro R layer

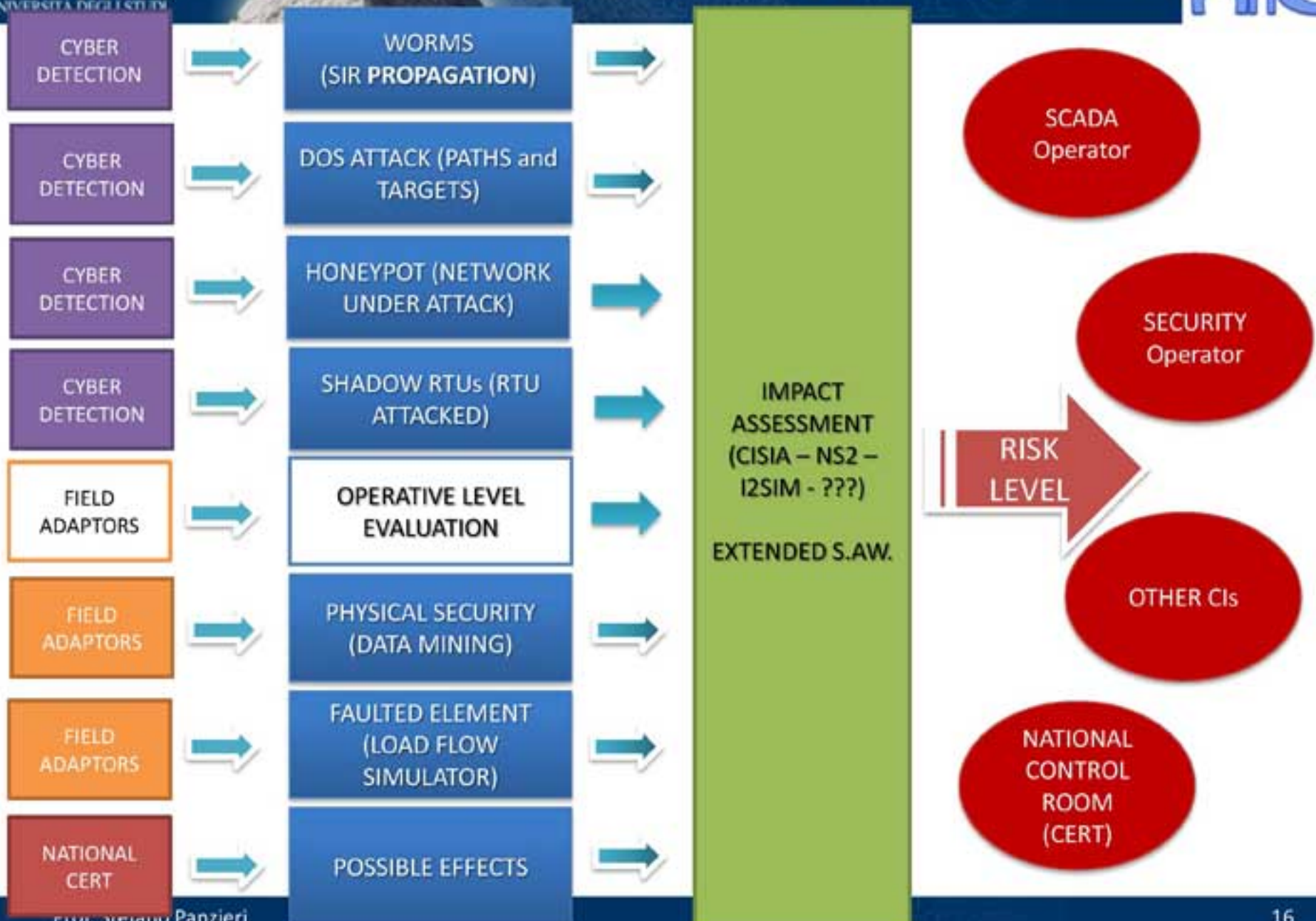
Expressions of both holistic and red. models

Inter-Infrastructure Homogeneous layer capturing interdependencies

SCADA cyber attack detection



FROM OLISTIC ASSESSMENT TO IMPACT EVALUATION



- CockpitCI aims to classify the associated risk level, broadcast an alert at different security levels and activate a strategy of containment of the possible consequences of cyber-attacks.

- CockpitCI aims to leverage the ability of field equipment to counteract cyber-attacks by deploying preservation and shielding strategies able to guarantee the required safety. This capability should be carefully evaluated because CI operators fear that "local automatic reactions may happen during "normal" activities inducing catastrophic behaviour".

IMPROVED RTU AWARENESS

- RTUs can be puzzled because they have no idea of
  - what they are doing
  - why
  - with whom
- We need to increase the awareness of RTUs or build for them the required awareness
  - Local misuse/anomaly detection
  - Process modeling
  - Central warning dispatching
- Hence, some special behaviors could bet triggered
  - Normal operation
  - Alerted
  - Double check commands
  - Disconnected for a time (fail safe outputs)
  - BMS (extended emergency shutdown)
  - [...]


Thank You!