Directive 2008/114/CE: Operator Security Plan and Risk Analysis

Bucharest CIP Conference, 27-28 October 2011

Sandro Bologna
AIIC President
s.bologna@infrastrutturecritiche.it

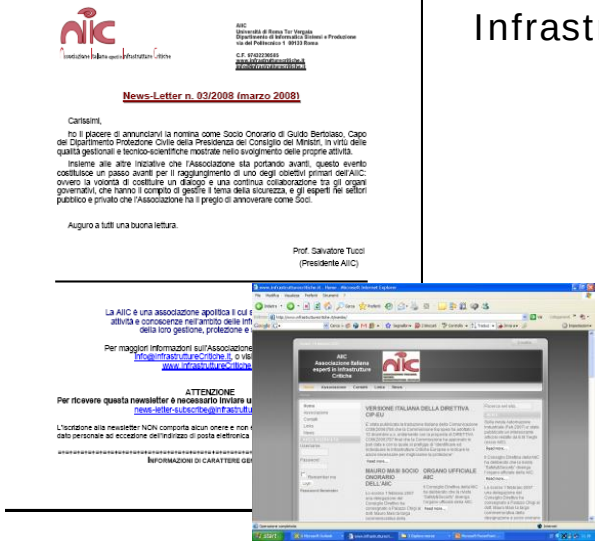
AIIC – Associazione Italiana esperti Infrastrutture Critiche

Non-governmental and non-profit scientific association legally registered in Italy that aims at exchanging experiences and knowledge related to the critical infrastructures to create an interdisciplinary and inter-sectorial shared approach among experts of different fields

CRITIS 2011
6TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY
SEPTEMBER 8-9, 2011. LUCERNE, SWITZERLAND

NetONets^{2011}

Networks of Networks: Systemic Risk and Infrastructural Interdependencies



European Critical Infrastructure

European Directive n. 114 / 2008 / EC

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

ECI Operator Security Plan (OSP)

The OSP will identify critical infrastructure assets and which security solutions exist or are being implemented for their protection. The ECI OSP procedure will cover at least:
1. identification of important assets;
2. **conducting a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact**; and
3. identification, selection and prioritisation of counter-measures and procedures with a distinction between:
— permanent security measures, which identify indispensable security investments and means which are relevant to be employed at all times. This heading will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,
— graduated security measures, which can be activated according to varying risk and threat levels.

Vulnerabilities of Critical Infrastructures to Natural Hazards

- **England August 2004**
- **Gudrun January 2005 (Sweden, Norway, Finland, ...)**
- **Kyrill January 2007 /Germany, Austria, Ceck, ...)**
- **Klaus January 2009 (France, Spain, ...)**
- **Wolfgang July 2009 (Switzerland, Poland, ...)**

Vulnerabilities of Critical Infrastructures to Technological Accidents

- **Toulouse (France) September 2001**
- **Liege (Belgium) October 2002**
- **Priolo (Italy) April 2006**
- **Coryton (UK) October 2007**
- **Viareggio (Italy) June 2009**

Vulnerabilities of Critical Infrastructures to Terrorist Attacks

- **United States September 2001**
- **Madrid (Spain) March 2004**
- **Londra (UK) July 2005**

Vulnerabilities of Critical Infrastructures to Cyber Attacks

- **US - 2006:** Hacker penetrated the Water Filtering Plant's production system
- **Estonia 2007**: Including banks, ministries, newspapers and broadcasters organizations
- **Poland - 2008:** City's SCADA Tram System
- **Iran- 2010:** Stuxnet

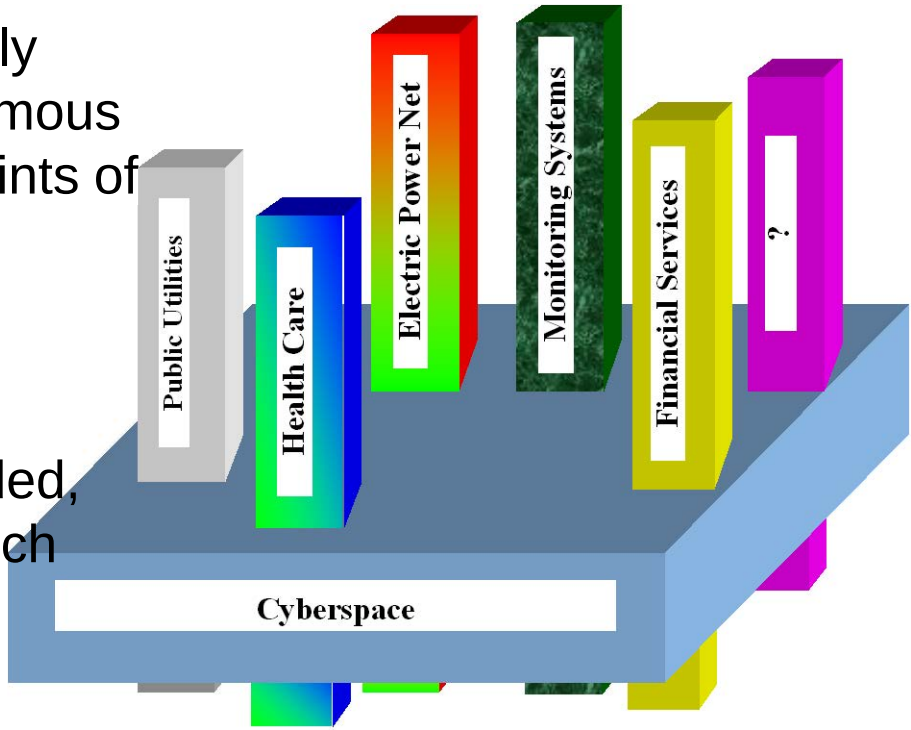
Increasing Mutual Dependency: Third millennium socio-techno scenario

<2000

Infrastructures vertically integrated, i.e. autonomous system with limited points of contact

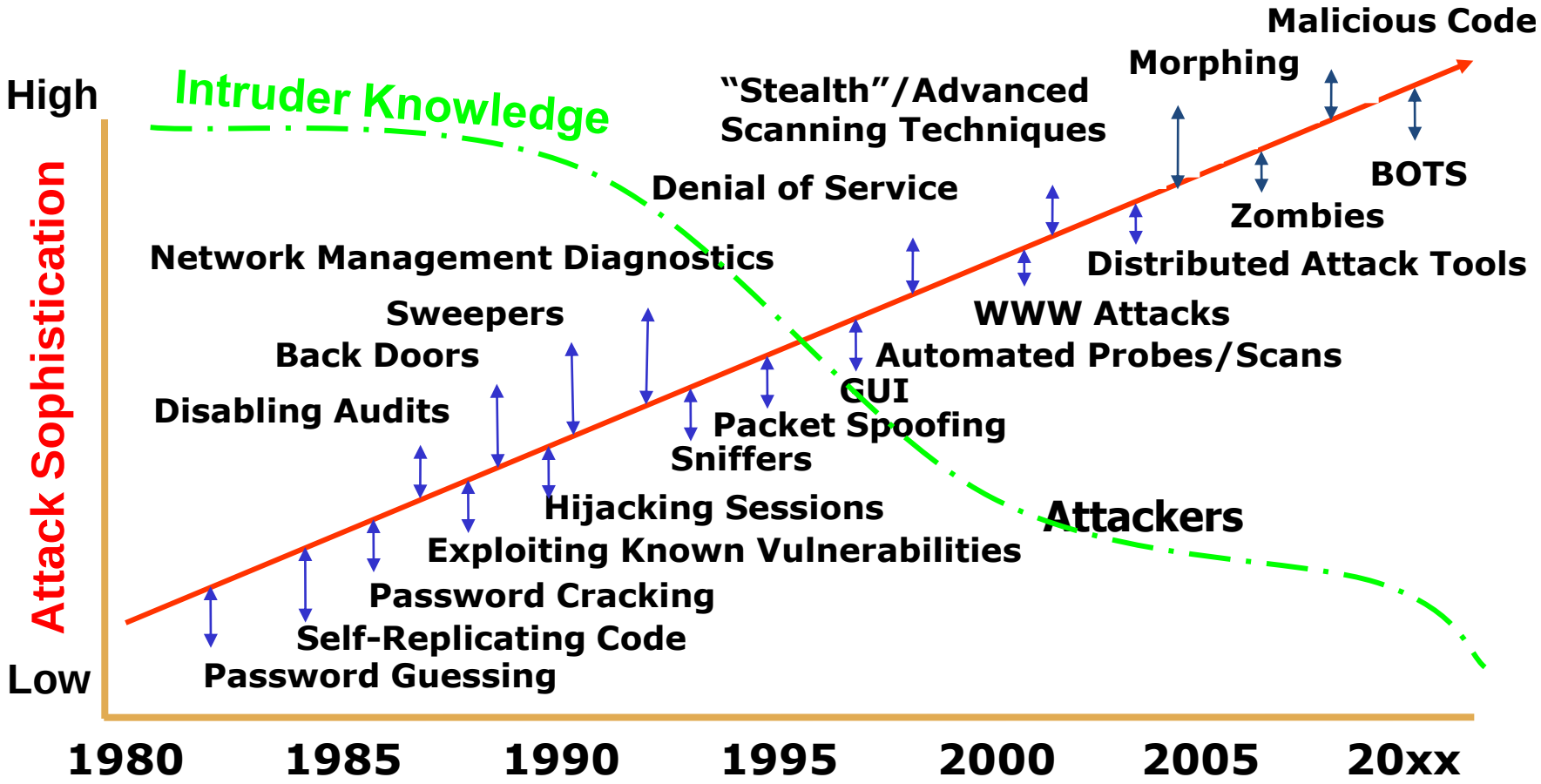
>2000

Infrastructures intergraded, mutual dependency which share a common layer: the cyberspace



Interdependencies/Interconnections are the risk multiplier

Cyber Threat Trends



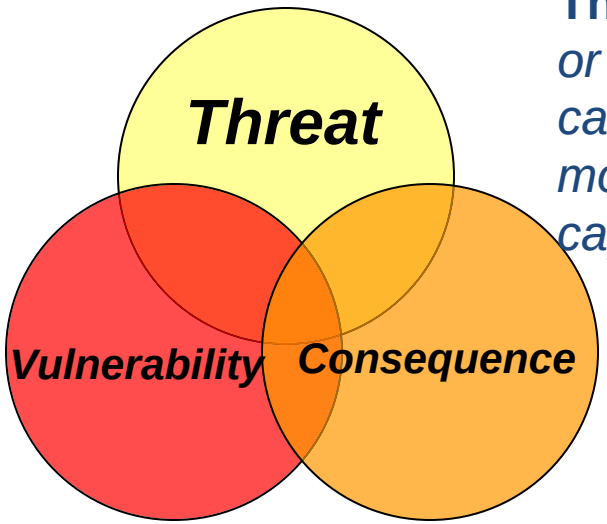
Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

How to decide what to protect

No Organization has enough resources to protect all their potential targets to the extent that it would like. The dictum of Frederick the Great, "**He who defends everything defends nothing**", remains relevant. Threats are not the same as risks. Separating the two requires Organization to perform risk analysis, a process of distinguishing among the things that absolutely must be protected from those that can be given less attention. The process of risk analysis shall be based on risk criteria relevant for the Organization.

Threat: *Any person, circumstance or event with the potential to cause loss or damage - includes motivation, actor, intent and capabilities*

Vulnerability: *Any weakness that can be exploited by an adversary or through accident. Ease of exploit, exposure, impact, deployment*

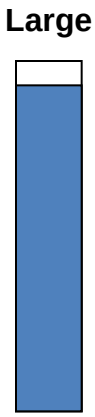


Consequence: *The amount of loss or damage that can be expected from a successful attack.*

The Risk Equation

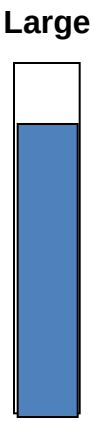
*Risk = Likelihood (*PA*) x Vulnerability* (PSA) *x Impact*

The Risk Equation



Identify Threats

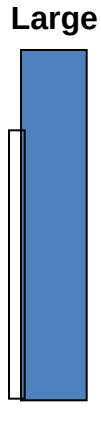
Analyze Vulnerabilities



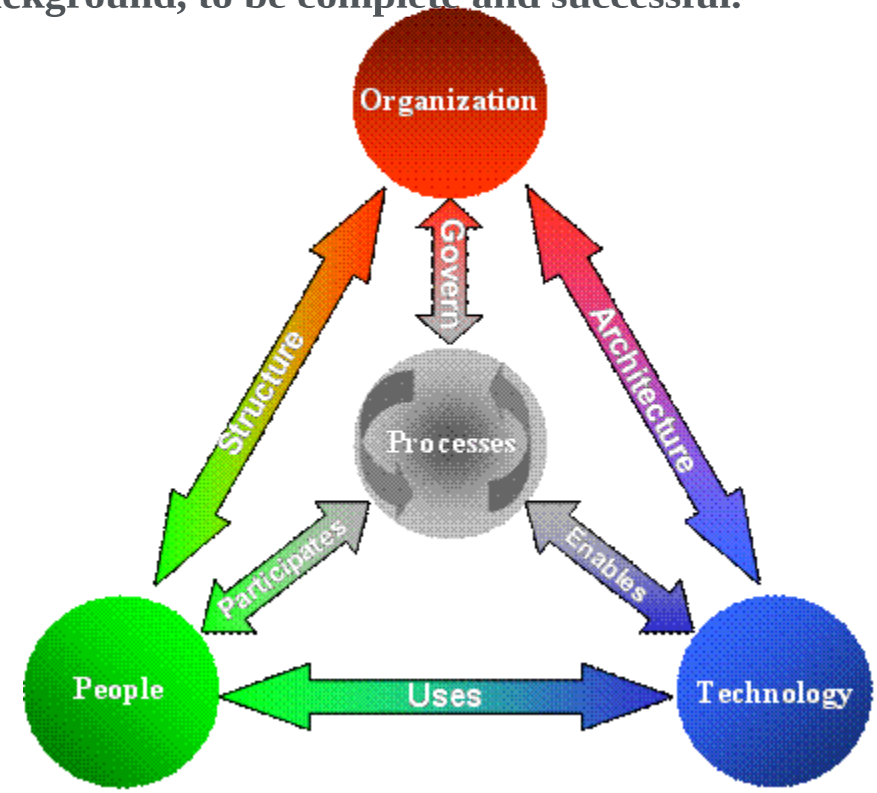
$$\text{Risk} = \frac{\text{Threats x Vulnerabilities}}{\text{Countermeasures}} \text{ x Impact}$$

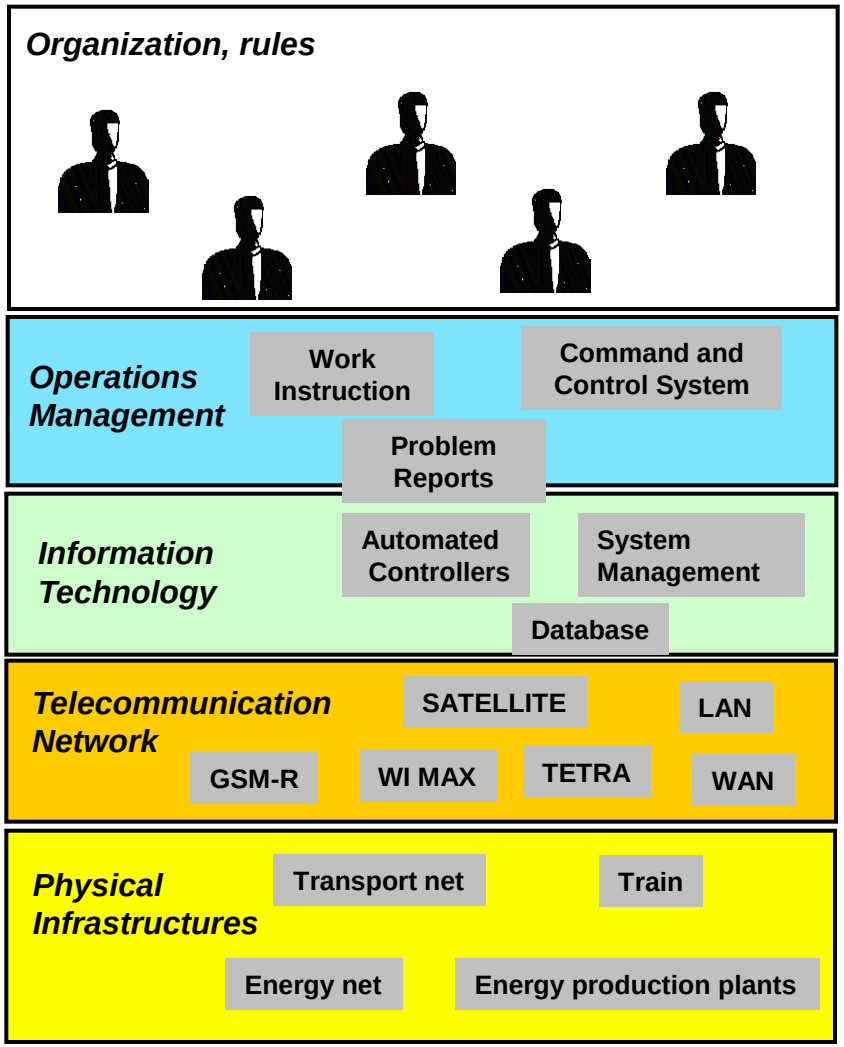
Security Requirements

Evaluate Consequences



A Critical Infrastructure is not only made of technologies but especially of people, processes and organizations.
The Risk Analysis and Risk Management must take in consideration all these components, plus cultural background, to be complete and successful.





Identify Hazards

Technical failures
Human failures
Natural hazards
Terrorist attacks
Sabotages

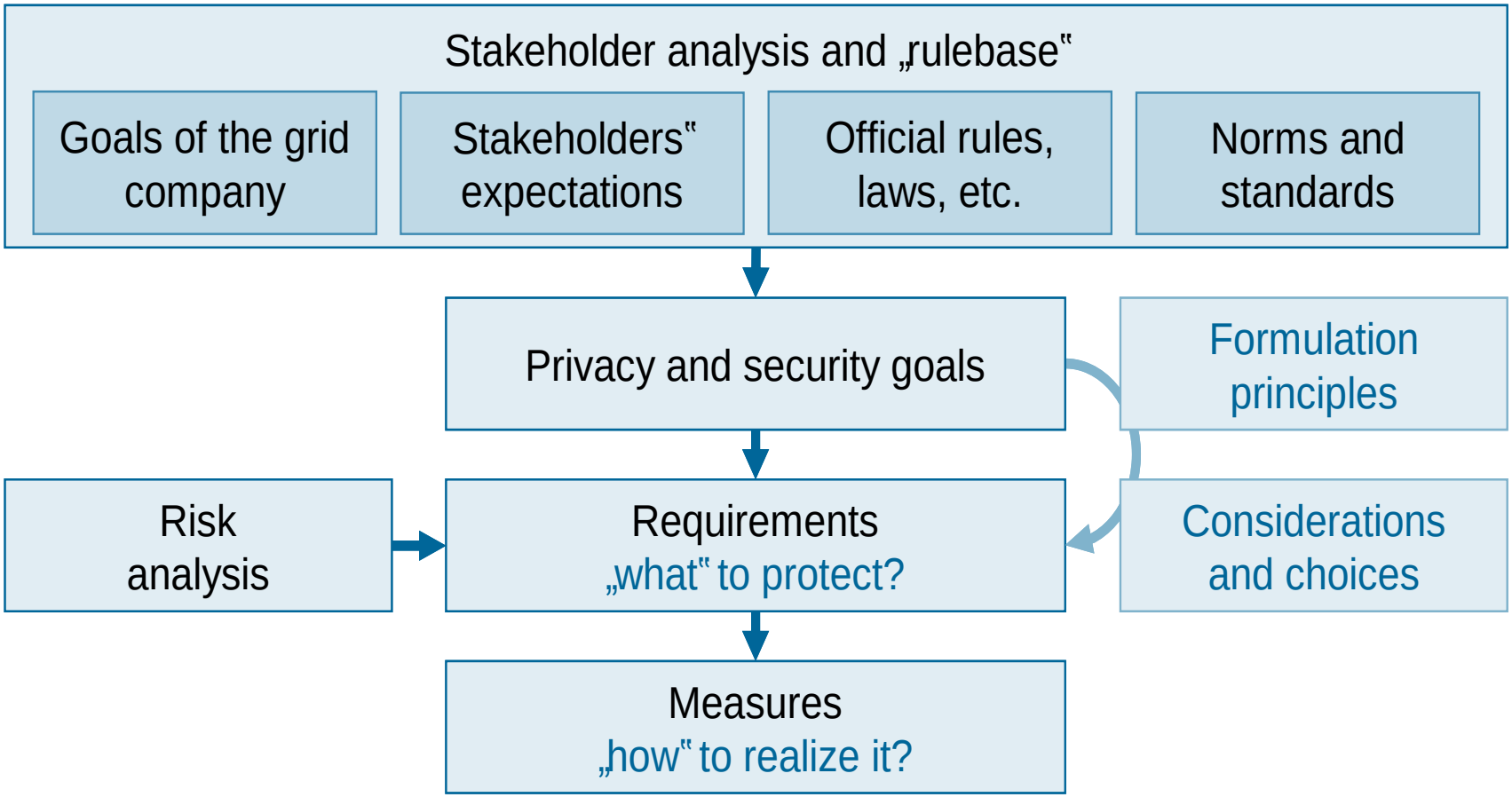
Analyze Vulnerabilities

Technical elements
Human elements
Information systems
Processes
Organization
Location
Concentration of CIs

Evaluate Consequences (Impacts)

Severity of impact (human loss, economic, social)
Incident Management Preparedness
Continuity of Operation

Countermeasures Definition Process



More information: http://www.netbeheernederland.nl/Content/Publications/Publications.aspx - Privacy and Security of AMI (main document)

Conclusions

- CI Risk Analysis is a multi-dimension multi-disciplinary challenge and needs to consider not only Technical Failures but also Human Failures, Natural Events, Terrorism, Sabotage, …. among all the possible Hazards

- Risk Analysis should be mandatory before to assume any Countermeasures, but it is not the only factor influencing "what" to protect and "how" to protect

www.InfrastruttureCritiche.it