Colloquia

LE PRINCIPALI METODOLOGIE DI ALL HAZARDS RISK ASSESSMENT PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

Roma, 26 gennaio 2017

Ing. Luisa Franchina e Dr. Michele Kidane Mariam

Critical Infrastructure Definition & Key Features 1/4

European directive 114/2008:

- ✓ **CRITICAL INFRASTRUCTURE**: an **asset, system** or **part thereof** located in Member States which is **essential for the maintenance of vital societal functions, health, safety, security, economic** or **social well-being** of **people**, and the **disruption or destruction** of which would have a **significant impact** in a Member State as a result of the failure to maintain those functions;

Critical Infrsturture Definition & Key Features 2/4

- **Each Member State identifies its critical infrastructures on the basis of what they determine essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being.**

Examples of critical infrastructures sectors:

- ✓ **Water**
- ✓ **Food**
- ✓ **Agriculture, forestry and fishing**
- ✓ **Environment**
- ✓ **Commerce**
- ✓ **Culture, icons, aggregation site**
- ✓ **Energy**
- ✓ **Finance**
- ✓ **Industry**
- ✓ **Information and communication**
- ✓ **Institution and public administration**
- ✓ **Health services**
- ✓ **Services**
- ✓ **Transport and logistic**

ASSOCIAZIONE ITALIANA ESPERTI in INFRASTRUTTURE CRITICHE

	EU	G8	USA	RUS	UK	NL	FR	GER	SWE	JP	AUS	CAN	CH
ICT and MEDIA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
WATER, DAMS, SURFACE WATER MNGT	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓
ENERGY	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
NUCLEAR (radiological hazard), HAZARDOUS MATERIALS	✓		✓			✓	✓	✓		✓		✓	
FOOD	✓		✓		✓	✓					✓	✓	✓
AGRICULTURE			✓	✓							✓	✓	
HEALTH, MEDICAL SERVICES	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
FINANCE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TRANSPORT, POSTAL, PIPELINES and LOGISTIC	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
CHEMICHAL INDUSTRY and BIOTECH	✓		✓			✓	✓					✓	✓
SPACE	✓												
MONUMENTS ICONS			✓								✓	✓	✓
GOVERNMENT ADM		✓	✓	✓	✓	✓		✓		✓		✓	✓
DEFENSE INDUSTRY BASE, DEFENSE			✓	✓							✓	✓	✓
COMMERCIAL FACILITIES			✓										
EMERGENCY SERVICES		✓	✓		✓						✓	✓	✓
CRITICAL MANUFACTURING			✓										
VERY LARGE INFORMATION SYS				✓									
UTILITY INCLUDING WARMING SYSTEMS				✓									
INDUSTRY				✓									
MUNICIPAL SERVICES				✓					✓				
CIVIL DEFENSE				✓									✓
LEGAL ORDER, PUBLIC SAFETY						✓	✓						
HAZARDOUS MATERIALS								✓					
SERVICES, OTHER								✓					
RETAIL, PROVISIONS									✓				
PROTECTION & SAFETY									✓			✓	✓

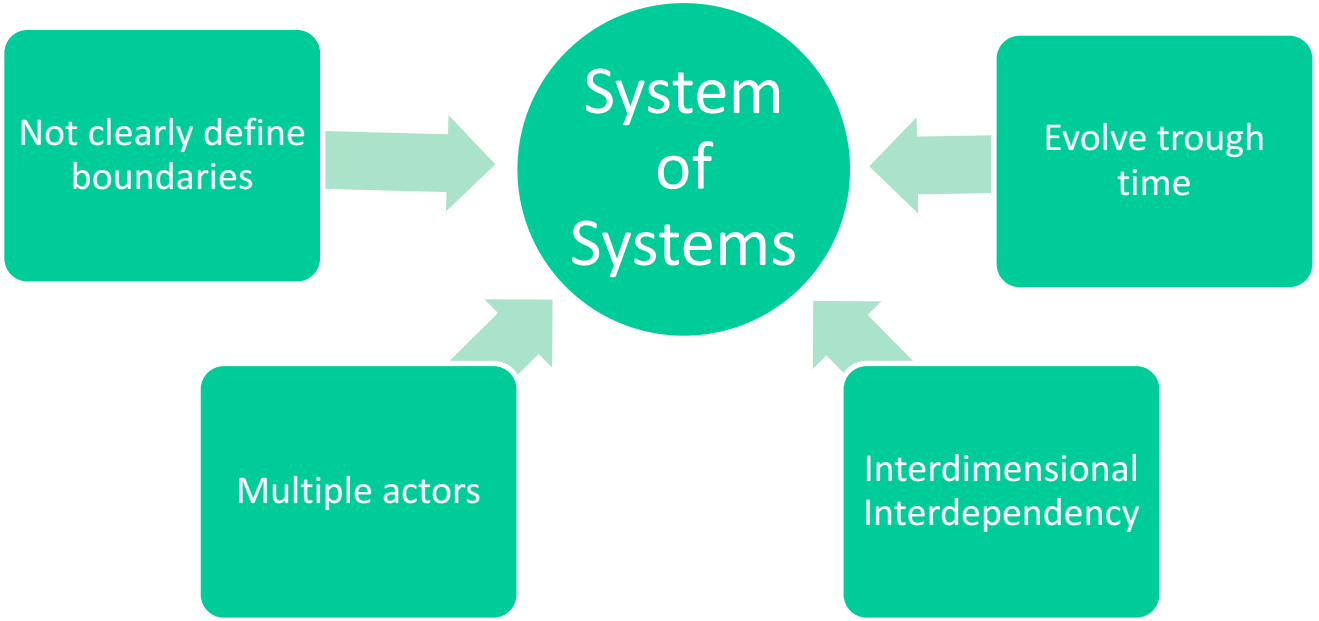
Critical Infrsturture Definition & Key Features – Interdipendences 3/4

- **Critical Infrastructure have 4 types cross and intra sectoral Interdependencies** (Rinaldi et al. , 2001)**:**
  - **Physical:** The operation of one infrastructure depends on the material output of the other
  - **Cyber:** Dependency on information transmitted through the information infrastructure.
  - **Geographic:** Dependency on local environmental effects that affects simultaneously several infrastructures
  - **Logical:** Any kind of dependency not characterized as Physical, Cyber or Geographic

- Besides cross-sectoral interdependencies (e.g. ICT and Electricity, Satellite navigation and Transport), at European level one **can identify intra-sectoral interdependencies of national infrastructures that form European infrastructures**
  - Example: high voltage electricity grid is composed by the interconnected national high-voltage electricity grids

Critical Infrsturture Definition & Key Features – System of Systems 4/4

- **Therefor Critical Infrastructure can be defined as**



Risk, Hazard and Protection definition

- ✓ **Protection**: all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to **deter**, **mitigate** and **neutralise** a **threat, risk or vulnerability** (2008/114/EC);

- ✓ **Risk:** a combination of the consequences of an event (hazard/threat) and the associated likelihood/probability of its occurrence. (ISO 31010)

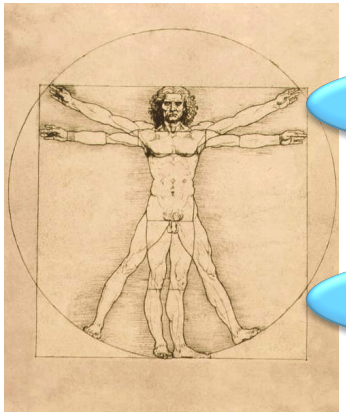
- ✓ **Hazard:** a dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage(UNISDR, 2009).

Hazards

Natural
Predictable and Unpredictable

Dimensions:
- Land
- Water
- Air
- Space
- Cyber

Human
Voluntary and accidental



- Conventional
- Unconventional

CYBER
- REMOTE
- LOCAL

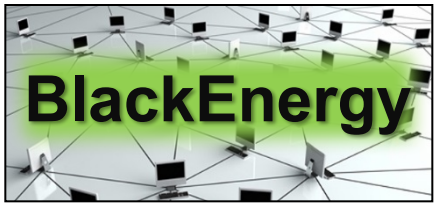
Cyber threats

Threat actors are more sophisticated, with access to tools that make it easy to infiltrate critical infrastructure

- Nation States
- Intelligence
- Hacktivists
- Insiders
- Terrorists

Hackers exploit SCADA holes to take full control of critical infrastructure

By Darlene Storm
January 15, 2014 12:51 PM EST 3 Comments



- Understand you
- Stuxnet variants
- New Exploits

- Valid Credentials
- Access
- Sabotage
- Data

Risk Assessment

- ✓ Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation. (ISO 31010)

Risk Identification

- ✓ Finding
- ✓ Recognizing
- ✓ Describing risks

Risk Analysis

- ✓ Comprehend the nature of risk
- ✓ Determine Impact and probability
- ✓ Determine level of risk

Risk Evaluation

- ✓ Prioritizing risk
- ✓ Evaluate whether risk or/and its magnitude i acceptable/tolerable

Risk Assessment – Risk 1/2

- Risks are the combination of the consequences of an event or hazard and the associated likelihood of its occurrence (ISO 31010).
- The consequences are the negative effects of an event expressed in terms of:

✓ **Human impacts**

✓ **Economic and environmental impacts**

✓ **Political/social impacts**

- When the extent of the impacts is independent of the probability of occurrence of the hazard, which is often the case for purely natural hazards, such as earthquakes or storms, risk can be expressed algebraically as:

Risk = hazard impact * probability of occurrence

Risk Assessment – Risk 2/2

- The Impact of an hazard is conditioned by preparedness or preventive behaviors and practices in place, e.g. evacuation plan, contingency plan, security measures etc.
- Impacts are often expressed in terms of **vulnerability** and **exposure**
  - ✓ **Vulnerability V** is defined as the characteristics and circumstances of a community, system or asset that make it susceptible to the damaging effects of a hazard (UNISDR, 2009)
  - ✓ **Exposure E** is the totality of people, property, systems, or other elements present in hazard zones that are thereby subject to potential losses (UNISDR, 2009)
- Therefore Risk can not always be expressed solely as a product between two terms but should be expressed as the following functional relationship:

$$\textbf{Risk} = f(\textbf{ probability of occurrence} * \textbf{E} * \textbf{V})$$

Risk Assessment – Impact Assessment 1/2

In Critical Infrastructure Protection, impact assessment should consider the following type of impacts :

Human impacts

- ✓ the number of affected people
- ✓ the number of deaths,
- ✓ the number of severely injured or ill people,
- ✓ the number of permanently displaced people

Economic and environmental impacts

- ✓ the sum of the costs of cure or healthcare,
- ✓ cost of immediate or longer-term emergency measures,
- ✓ costs of restoration of buildings, public transport systems and infrastructure, property, cultural heritage, etc.,
- ✓ costs of environmental restoration and other environmental costs (or environmental damage),
- ✓ costs of disruption of/to economic activity,
- ✓ value of insurance pay-outs,
- ✓ indirect costs on the economy,
- ✓ indirect social costs, and other direct and indirect costs, as relevant

Risk Assessment – Impact Assessment 2/2

Political/social impacts

- ✓ public outrage and anxiety
- ✓ encroachment of the territory,
- ✓ infringement of the international position,
- ✓ violation of the democratic system,
- ✓ social psychological impact,
- ✓ impact on public order and safety,
- ✓ political implications, psychological implications,
- ✓ damage to cultural assets,
- ✓ other factors considered important which cannot be measured in single units

Political/social impacts will generally refer to a semi-quantitative scale comprising a number of classes

- limited/ insignificant
- minor/ substantial
- moderate/ serious
- significant/ very serious
- catastrophic/ disastrous.

Risk Assessment – Empirical Evidence

- Impact analysis should rely as much as possible on **empirical evidence and experience from past event data or established quantitative models of impact**. It is clear that for quantification purposes, a number of assumptions and estimates will have to be used, some of which may be rather uncertain. These **assumptions and estimates should always be clearly identified and substantiated.**

- The assessment of the probability of an event or hazard should be based, where possible, on the historical frequency of events of similar scale and available statistical data relevant for an analysis of the main drivers.

- However, when considering Cyber-Threat, reliance on historical data may not be enough, especially when considering the most innovative and advance threats (APT, Zero day, etc.). For this reason in this domain the focus of risk assessment has shifted toward continuous monitoring and real-time data gathering/analysis

Metriche dell'impatto

- Vittime
- Impatti economici
- Sicurezza economica
- Sofferenza fisica
- Perturbazione della vita quotidiana
- Fiducia nelle istituzioni
- Salute pubblica
- Sicurezza pubblica
- Impatti psicologici
- Sicurezza dello Stato
- Difesa della Nazione
- Impatto sull'opera delle istituzioni
- Violazione del territorio
- Disordine pubblico e panico
- Perturbazione della democrazia
- Impatto sull'ordine sociale
- Impatto geopolitico
- Morale nazionale
- Impatto ambientale
- Impatto sociopolitico
- Effetti negativi sui marchi e aziende nazionali
- NGH…

COSO ERM : Risk Assessment – Principali fasi del processo

2 Identificazione e valutazione dei rischi

La valutazione del rischio si basa su due dimensioni

IMPATTO

PROBABILITA' DI ACCADIMENTO

In entrambi i casi viene utilizzata una scala di valutazione delle dimensioni del rischio per ordini di grandezza con 5 livelli, dove 5 rappresenta la valutazione massima e 1 la valutazione minima.

COSO ERM : Risk Assessment – Principali fasi del processo

2 Identificazione e valutazione dei rischi

Identificare l'IMPATTO di un rischio vuol dire definire la tipologia di perdita e misurare la grandezza associata al verificarsi del rischio. E' quindi necessario quantificare il danno derivante per la Società sia in termini quantitativi che qualitativi.

I criteri per la valutazione dell'impatto dei rischi sono:

- Economico
- Mercato
- Reputazionale
- Vantaggio competitivo

Cyber-risk managment in CIP

Cyber risk management in CIP:

- ✓ Shift from a reactive approach to a predictive/proactive approach

- ✓ Use of security intelligence techniques and platforms for data gathering, sharing and analysis. (CERT, SOC, ISACS)

- ✓ Use of specific and establish integrated risk management framework for Cyber security:
  - ➢ Cobit
  - ➢ Magerit
  - ➢ ISO 27001
  - ➢ NIST
  - ➢ Framework Nazionale Cyber-Security

Cyber-risk managment in CIP

The traditional method of securing the enterprise is outdated. Defense in Depth alone is not enough. The future is all about *VELOCITY*.

Old Paradigm	New Paradigm
Security Model based on **Defense in Depth (DiD)**	Security Model based on **DiD + Rapid Detection + Rapid Response**
Security Operations **Steady State and Reactive**	Security Operations **Elastic and Agile**
Security Analysis **Manual and Fragmented**	Security Analysis **Analytics and Intelligence**
Governance, Risk & Compliance **IT and Compliance Focused**	Governance, Risk & Compliance **Integrated Risk Management**
Functional Domains **IT, OT, Telecom, Physical Silos**	Functional Domains **Converged**

Risk Assessment – Single & Multiple

- ✓ **Single-risk assessment**: determine the singular risk (i.e. likelihood and consequences) of one particular hazard (e.g. flood) or one particular type of hazard (e.g. flooding) occurring in a particular geographic area during a given period of time.

- ✓ **Multi-risk all-hazard assessment:** determine the total risk from several hazards either occurring at the same time or shortly following each other, because they are dependent from one another or because they are caused by the same triggering event or hazard; or merely threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence.

Single-Risk Assessment

- **Single-risk assessments**:
  - ✓ Single-risk analysis estimates the risk of a singular hazard in isolation from other hazards or risk scenarios. Different natural hazards require very different analyses of their risk, i.e. in establishing the probability of their occurrence and the level of possible impacts.
  - ✓ EU legislation has introduced a number of "single-hazard" risk assessment requirements, such as in the area of flood risks, droughts, risks of accidents with dangerous substances, and risks to European Critical Infrastructures.
- However, for **Critical Infrastructure Protection** a **multi-risk all-hazard** approach is required in order to gain a multi-hazard and a multi-vulnerability perspective.
- Each risk assessment must incorporate **possible amplifications due to the interaction with other hazards**;
- Many single-risk analyses consider to varying degrees the complexity of different origins of a particular hazard. But they often **stop short of bringing together dissimilar hazards and considering adequately infrastructures interdependencies**.

Multi-risk all-hazard risk assessments

Multi-risk assessments determine the total risk from several hazards, taking into account possible hazards and vulnerability interactions:

A. **occurring at the same time or shortly following each other**,
   - ✓ because they are dependent of one another
   - ✓ because they are caused by the same triggering event or hazard;

Also referred to as follow-on events, knock-on effects, domino effects or cascading events

The likelihood of each of the events occurring is of course correlated to the likelihood of occurrence of the other event or the prior triggering event.

B. **threatening the same elements at risk (vulnerable/ exposed elements) without chronological coincidence**

In both cases the assessment of consequences needs to consider the cumulative impacts of all of the various impacts occurring at the same time or shortly following each other.

Multi-Risk Assessment Challenges

- Current Challenges:
  - ✓ Adequately taking into account all possible follow-on effects (also: knock-on effects, domino effects or cascading effects) amongst hazards and infrastructure (Interdependencies)
  - ✓ Co-ordination and interfacing between different specialized authorities and agencies, which each deals with specific hazards or risks without developing a complete overview of the knock-on, domino and cascading effects
  - ✓ Most multi-risk assessment methodology are just an adaptation of single risk-assessment methodology
    - ✓ There are a number of difficulties combining single-risk analyses into more integrated multi-risk analysis:
    - ✓ Available data for different single risks may refer to different time windows, different typologies of impacts are used, etc.,
    - ✓ makes comparisons and rankings difficult if not impossible.

Risk Assessment & Critical Infrastructure Protection

- Risk assessment is the key element in Critical Infrastructure Protection

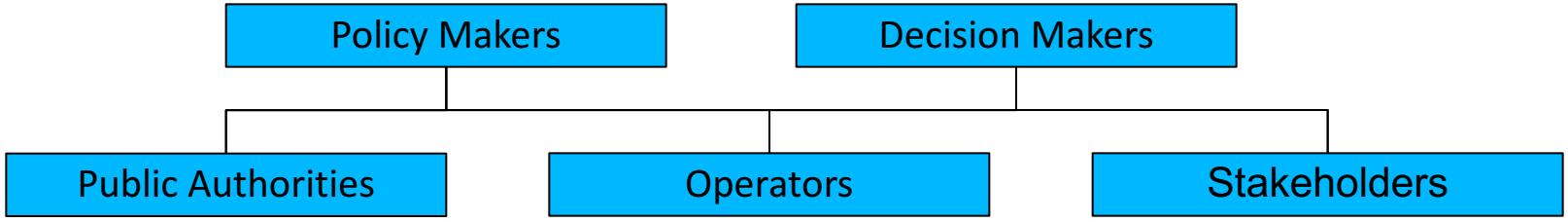
- Risk assessment is indispensable in order to:
  - ✓ Identify **threats/hazard,**
  - ✓ **Assess vulnerabilities**
  - ✓ **Evaluate the impact on assets, infrastructures or systems** taking into account the **probability of the occurrence** of these threats/hazards

- There is a significant number of risk assessment methodologies for critical infrastructures protection.

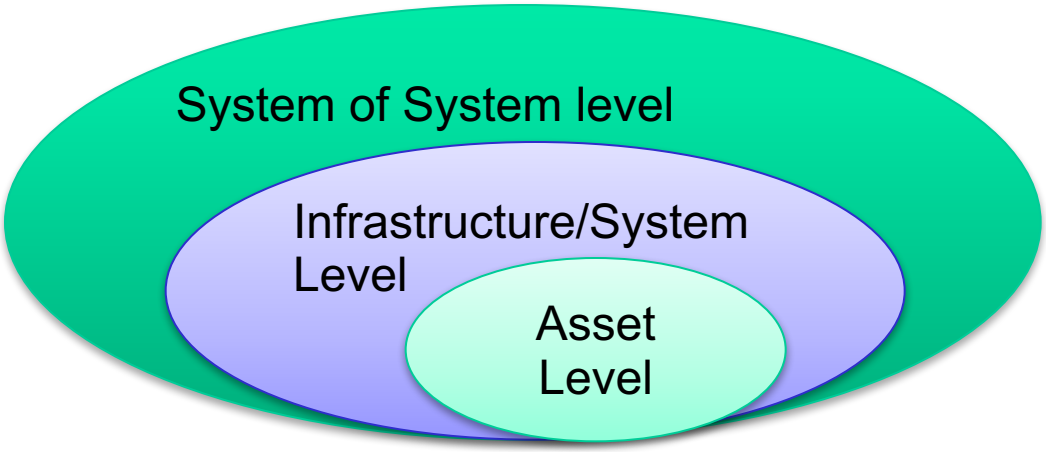
- Critical Infrastructure risk assessment methodologies differ in scope, audience to which they are addressed and their domain of applicability.

Risk Assessment Metodologies for Critical Infrastructure Protection

Risk assessment methodologies audience



Risk assessment methodologies domain of applicability:



Risk Assessment Metodologies for Critical Infrastructure Protection

Risk Assessment Methodologies for Critical Infrastructure Protection

- Sectoral Methodologies
  - Each sector is treated separately with its own risks and ranking
- System Approach Methodologies
  - Assess critical infrastructures as an interconnected network

Risk Assessment Metodologies for Critical Infrastructure Protection

The following are the Methodologies that will be presented:

- **Better Infrastructure Risk Resilience (BIRR)**
- **DECRIS Project**
- **CARVER2 - NI2**
- **Critical Infrastructure Protection Decision Support System**
- **RAMCAP-Plus**

Risk Assessment Methodologies for Critical Infrastructure Protection
Argonne National Laboratory – Better Infrastructure Risk Resilience (BIRR)

- **Argonne National Laboratory** is one of the U.S. Department of Energy's oldest and largest national laboratories conducting research in a wide range of fields
- One of the main domains is national security. **Protection of critical infrastructures** is part of this field.
- Research conducted in this direction is mainly oriented to the policy needs of the Department of Homeland Security (DHS).
- Argonne develops methodologies for assessing infrastructure risk and resilience to a variety of natural and man made hazards for various infrastructures including :

  - ✓ **Energy facilities**
  - ✓ **Transportation**
  - ✓ **Water treatment plants**
  - ✓ **Financial institutions**
  - ✓ **Commercial office buildings**

Risk Assessment Methodologies for Critical Infrastructure Protection
Argonne National Laboratory – Better Infrastructure Risk Resilience (BIRR)

- Enhanced Critical Infrastructure Protection (ECIP) : umbrella program covering Critical Infrastructure Protection activities.
- The BIRR methodology is developed within the framework of ECIP and covers the facilities in 18 critical infrastructure sectors :
  - ✓ **Approach**: sectoral approach that goes down to the assets level and gives priority on the protection measures that are applied mainly against terrorist threats
  - ✓ **Aim:** to provide policy makers with tools that can help in the analysis of the various sectors, identify vulnerabilities and prepare risk reports
  - ✓ **Target audience:** Policy maker

Risk Assessment Methodologies for Critical Infrastructure Protection
Argonne National Laboratory – Better Infrastructure Risk Resilience (BIRR)

Strengths of the methodology

- ✓ It is possible for the operator to assess the security of its assets with respect to certain scenarios and also to compare their security level with respect to that of similar sectors/subsectors.
- ✓ The use of a common metric (VI) to compare critical assets protection measures across sectors is remarkable
- ✓ Cross-sectoral and Intra-sectoral dependences are considered (PMI)

Weaknesses of the methodology

- ✓ Sectoral approach
- ✓ Gives priority on the protection measures that are applied mainly against terrorist threats
- ✓ Resilience index concept need further development and consideration

Detailed information available here:
http://www.anl.gov/articles/better-infrastructure-risk-and-resilience

Risk Assessment Methodologies for Critical Infrastructure Protection
DECRIS Project / Approach

- The DECRIS approach was develop by SINTEF within the SAMRISK research programme
- SAMRISK is a program of the Research Council of Norway that aims at increasing the knowledge about threats, dangers and vulnerability, about how unwanted events can be prevented and crises management be strengthened, whilst respecting basic human rights and privacy.
- The project is the result of intensive research from SINTEF in the domain of hazard/risk assessment for critical infrastructures
- The DECRIS project/approach builds on the existing capacities in the sectoral risk assessment methodologies that existed already in Norway

Risk Assessment Methodologies for Critical Infrastructure Protection
DECRIS Project / Approach

- The methodology is an "all hazard" approach, to be used by authorities and companies. Part of the project is to study how risk related to critical infrastructure is communicated to the public, to gain knowledge of decision processes, and of the society's perception of risk.
  - **Approach:** Cross-sectoral / interconnected system approach
  - **Aim:** bridge the gap between the methodologies that exist in various sectors and propose an all-hazard generic Risk and Vulnerability Assessment methodology for cross-sector infrastructure analysis
  - **Target audience**: policy and decision makers

Risk Assessment Methodologies for Critical Infrastructure Protection
DECRIS Project / Approach

Strengths of the methodology

- ✓ A refinement mechanism to narrow down the list of events that have to be assessed
- ✓ Fosters the collaboration between the various stakeholders in the different sectors in order to widen their understanding on the interdependencies across sectors
- ✓ Cross-sectoral risk assessment approach
- ✓ Cross-sectoral and Intra-sectoral dependences are considered

Weaknesses of the methodology

- ✓ Resilience is not directly assessed in this methodology
- ✓ The methodology is not highly differentiated with respect to a typical risk assessment one
- ✓ The issue of the comparability of the consequences of one event on different infrastructures still remains

Detailed information available here:
https://www.sintef.no/projectweb/samrisk/decris/

Risk Assessment Methodologies for Critical Infrastructure Protection
CARVER2 - NI2

- Developed by NI2 Centre for Infrastructure Expertise an non-profit, non-partisan applied research organisation funded by the U.S. Department of Commerce National Institute for Standard and Technology
- **CARVER** stands for **C**riticality **A**ccessibility **R**ecoverability **V**ulnerability **E**spyability **R**edundancy
- NI2 states that CRAVER is a non-technical method for comparing and ranking critical infrastructure and key resources
- Claims to be the only assessment tool that ranks critical infrastructure across sectors
- A stand-alone PC tool and a server/client version (CARVER2Web) have been developed for the implementation of this methodology
- The methodology is supposed to cover both terrorist threats as well as natural disasters, thus implementing an all-hazards approach
- it is available free of charge to federal, state, and local government officials and agencies

Risk Assessment Methodologies for Critical Infrastructure Protection
CARVER2 - NI2

CARVER2 is a tool that has been developed in order to serve the needs of critical infrastructure protection:

- **Approach:** Cross-sectoral approach
- **Aim:** to serve the needs of critical infrastructure analysis mostly from the policy maker point of view
- **Target audience**: Policy makers

Risk Assessment Methodologies for Critical Infrastructure Protection
CARVER2 - NI2

Strengths of the methodology

- ✓ Cross-sectoral risk assessment approach
- ✓ Cross-sectoral and Intra-sectoral dependences are considered
- ✓ Predefined interdependencies
- ✓ Provides a cross-sectoral harmonized metric for the assessment of the importance of different infrastructures

Weaknesses of the methodology

- ✓ A systems approach is missing
- ✓ Not clear at which level the interdependencies have been defined
- ✓ Not clear what kind of interdependencies are included in tool

Detailed information available here:
https://web.archive.org/web/20111208113119/http://www.ni2cie.org/CARVER2.asp

Risk Assessment Methodologies for Critical Infrastructure Protection
Critical Infrastructure Protection Decision Support System

- The Critical Infrastructure Protection Decision Support System (CIPDSS) has been developed by the Los Alamos National Laboratory in the context of the National Infrastructure Simulation and Analysis Center (NISAC)
- The NISAC models, simulates, and analyzes the Nation's critical infrastructure and key resources (CIKR) to assess the technical, economic, and national security implications of infrastructure protection, mitigation, response, and recovery options.
- NISAC leverages LANL's well-established expertise in the modeling and simulation of complex systems. They provides advanced modeling, simulation, and analysis capabilities focused on studying critical national infrastructures, their interdependencies, vulnerabilities, and complexities.
- NISAC is comprised of Department of Homeland Security program management and outreach personnel in Washington, D.C., and technical analytical staff at Los Alamos and Sandia national laboratories. Congress mandated that NISAC serve as a "source of national expertise to address critical infrastructure protection" research and analysis.

Risk Assessment Methodologies for Critical Infrastructure Protection
Critical Infrastructure Protection Decision Support System

- The Critical Infrastructure Protection Decision Support System (CIPDSS) provides information and decision support for the protection of critical infrastructures based on an assessment of risks appropriately accounting for the likelihood of threat, vulnerabilities, and uncertain consequences associated with terrorist activities, natural disasters, and accidents.
  - **Approach:** Cross-sectoral / System of systems approach
  - **Aim:** information and decision support for the protection of critical infrastructures
  - **Target audience**: decision makers that have to decide upon different mitigation measures and operational tactics and prioritize the resources for protecting critical infrastructures

Risk Assessment Methodologies for Critical Infrastructure Protection
Critical Infrastructure Protection Decision Support System

Strengths of the methodology

- ✓ Cross-sectoral / System of System risk assessment approach
- ✓ Evaluation of the impact through common decision process metrics overcomes the problem of comparing risks among sectors
- ✓ Predefined interdependencies among 17 different sectors
- ✓ Provides a common metric for the prioritization of mitigation measures, operational tactics and resources for protecting critical infrastructures

Weaknesses of the methodology

- ✓ Complexity of the model
- ✓ Needs constant update and validation

Detailed information available here:
http://www.lanl.gov/programs/nisac/index.shtml

Risk Assessment Methodologies for Critical Infrastructure Protection
American Society of Mechanical Engineers (ASME)- RAMCAP-Plus

- ASME aims at helping the global engineering community develop solutions to real world challenges
- Founded in 1880, ASME is a not-for-profit professional organization that enables collaboration, knowledge sharing and skill development across all engineering disciplines, while promoting the vital role of the engineer in society.
- RAMCAP-Plus was developed by ASME (American Society of Mechanical Engineers) as an all hazards risk and resilience assessment methodology
    - **Approach:** Cross-sectoral approach
    - **Aim:** to provide an objective, consistent and efficient method for assessing and reducing infrastructure risks in terms directly comparable among the assets of a given sector and across sectors
    - **Target audience**: Critical Infrastructure operators and decision makers

Risk Assessment Methodologies for Critical Infrastructure Protection
RAMCAP-Plus

Strengths of the methodology

- ✓ Cross-sectoral / System of System risk assessment approach
- ✓ Resilience is addressed and constitutes a central element of the methodology.
- ✓ Cross-sectoral interdependences are considered
- ✓ Focus on the most critical assets
- ✓ Has both high and sector specific application
- ✓ Offer cross-sectoral risk comparisons method

Weaknesses of the methodology

- ✓ Adapts existing risk assessment techniques to a system of system approach

Detailed information available here:
https://www.asme.org/products/books/itiramc-allhazards-risk-resilience-prioritizing

Risk Assessment Metodologies for Critical Infrastructure protection
Existing metodologies shortcoming

- Methodologies developed at sectoral and assets level are well defined, tested, validated and the vast majority follows a linear risk assessment approach.
- Existing sectoral and assets methodologies have been extended to cope with critical infrastructure interdependencies.
    - This reflects the natural evolution of risk assessment methodologies existing already at organizational level
    - These methodologies reveal their limitations when cross-sectoral issues have to be addressed.
    - Detailed risk assessment is not applicable any more and a certain level of abstraction is necessary.
- Representing all assets of a networked system at the highest level of detail can leads to unprecedented complexity that is out of the scope for policy and decision makers.

Conclusion

- In many cases, the risk assessment methodologies for CI are an adaptation of methodologies that have been used for assessing risks within the confined environment of an organization.
- The identification of a common methodology for cross-sectoral interdependencies evaluation would allow to assess cascading effects and return a common cross-sector risk figure so that comparison of sectors does not end up to a comparison of apples vs oranges.
- In order to define a common approach for interdependencies assessment further cooperation is required among government authorities, CI operators and stakeholders.
- Impact of infrastructure disruption is usually expressed in terms of aggregated figures that account for the economic losses. This is a straightforward choice that enables policy makers to evaluate different disruption scenarios including cascading effects across sectors and evaluate costs and benefits of mitigation measures.
- The true challenge for upscaling any risk assessment methodology to complex systems is to develop effective approaches for the assessment of system of systems interdependences

Grazie per l‘attenzione

for any further information

AIIC
Ing. Luisa Franchina
Presidente AIIC / Partner Hermes Bay
E-Mail address
blustarcacina@gmail.com

AIIC
Dr.Michele Kidane Mariam
Senior Analyst / Consultant
E-Mail address
michele_kidane@hotmail.com