JRC Technical Notes

# Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art

**Georgios Giannopoulos**
**Roberto Filippini**
**Muriel Schimmer**


EUR 25286 EN - 2012

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

**Contact information**
Address: Via E. Fermi 2749, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: 00390322786211
Fax: 00390332789576

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/



JRC 70046

EUR 25286 EN
ISBN 978-92-79-23839-0
ISSN 1831-9424
doi:10.2788/22260

Luxembourg: Publications Office of the European Union, 2012



*Printed in ITALY*

# Contents

**1 Risk Assessment Methodologies for Critical Infrastructures. Setting the scene 3**

1.1 Introduction . . . 3

1.2 The policy framework in EU and worldwide . . . 5

1.2.1 The European programme for Critical Infrastructure Protection (EPCIP) . . . 5

1.2.2 The US Critical Infrastructure Protection (CIP) . . . 6

1.2.3 National Strategy and Action Plan for Critical Infrastructure Protection in Canada 7

**2 State of the art of Risk Assessment methodologies in EU and worldwide 8**

2.1 Criteria for methodology assessment . . . 8

2.2 Risk Assessment methodologies: Theoretical Background . . . 9

2.3 Risk Assessment methodologies in EU and worldwide . . . 11

2.3.1 Better Infrastructure Risk and Resilience (BIRR) . . . 11

2.3.2 Protection of Critical Infrastructures - Baseline Protection Concept (BMI) . . . 12

2.3.3 CARVER2 . . . 14

2.3.4 Critical Infrastructure Modelling Simulation (CIMS) . . . 17

2.3.5 Critical Infrastructure Protection Decision Support System (CIPDSS) . . . 18

2.3.6 Critical Infrastructure Protection modelling and Analysis (CIPMA) . . . 19

2.3.7 CommAspen . . . 20

2.3.8 COUNTERACT . . . . . 21

2.3.9 The DECRIS approach . . . . . 23

2.3.10 European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM) . . . . . 24

2.3.11 Fast Analysis Infrastructure Tool (FAIT) . . . . . 25

2.3.12 Multilayer Infrastructure Network (MIN) . . . . . 26

2.3.13 Modular Dynamic Model . . . . . 27

2.3.14 Agent-Based Laboratory for Economics (N-ABLE) . . . . . 28

2.3.15 Net-Centric Effects-based operations MOdel (NEMO) . . . . . 28

2.3.16 Network Security Risk Assessment modelling (NSRAM) . . . . . 29

2.3.17 RAMCAP-Plus . . . . . 30

2.3.18 Risk and Vulnerability analysis (RVA ) . . . . . 31

2.3.19 Sandia Risk Assessment Methodology . . . . . 32

2.3.20 National Infrastructure Protection Plan Risk Management Framework . . . . . 34

2.3.21 Risk Management for Critical Infrastructure Sectors (Canada) . . . . . 35

2.4 Gap analysis . . . . . 36

**References** **41**

**Summary table of risk assessment methodologies** **45**

# 1 Risk Assessment Methodologies for Critical Infrastructures. Setting the scene

## 1.1 Introduction

Effective risk assessment methodologies are the cornerstone of a successful Critical Infrastructure Protection programme. The extensive number of risk assessment methodologies for critical infrastructures clearly supports this argument. Risk assessment is indispensable in order to identify threats, assess vulnerabilities and evaluate the impact on assets, infrastructures or systems taking into account the probability of the occurrence of these threats. This is a critical element that differentiates a risk assessment from a typical impact assessment methodology.

There is a significant number of risk assessment methodologies for critical infrastructures. In general the approach that is used is rather common and linear, consisting of some main elements: Identification and classification of threats, identification of vulnerabilities and evaluation of impact. This is a well known and established approach for evaluating risk and it is the backbone of almost all risk assessment methodologies.

However, there is a huge differentiation of risk assessment methodologies based on the scope of the methodology, the audience to which it is addressed (policy makers, decision makers, research institutes) and their domain of applicability (asset level, infrastructure/system level, system of systems level). These attributes are not mutually exclusive, in the sense that the domain of applicability defines to a certain extent the target group of the methodology. For example, a risk assessment methodology that is applicable to system of systems at national or even supranational level is mostly addressed to policy makers and relevant authorities and less to operators or to asset managers at local level.

Methodologies developed for certain assets are well defined, tested and validated and the vast majority follows the linear approach already mentioned. However, methodologies that aim at assessing risks

at a higher level e.g. networked systems require further refinement. 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 (mostly an operator's approach) leads to unprecedented complexity that is out of the scope for policy and decision makers. This target group requires simplified solutions that can provide results even in real time.

The second important parameter that is entering the stage for the risk assessment methodologies of networked infrastructures is the element of interdependencies. According to the work of Rinaldi et al. [1] four types of interdependencies are identified for critical infrastructures:

- 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. As a concrete example we can mention the high voltage electricity grid that is composed by the interconnected national high-voltage electricity grids.

As mentioned before, the domain of applicability of a risk assessment methodology may be the most important attribute. According to this attribute, CIP risk assessment methodologies can be divided in two major categories: Sectoral methodologies, when each sector is treated separately with its own risks and ranking and systems approach that assess the critical infrastructures as an interconnected network. Methodologies that have been initially conceptualised to fit in the second category are rather limited. The vast majority of the existing work has been sectoral and mostly at asset level. These methodologies

have been then extended to cope with networked systems. This reflects the natural evolution of risk assessment methodologies existing already at organizational level to address issues at sectoral level. These methodologies reveal their limitations when cross-sectoral issues have to be addressed.

## 1.2 The policy framework in EU and worldwide

### 1.2.1 The European programme for Critical Infrastructure Protection (EPCIP)

The European Programme for Critical Infrastructure Protection (EPCIP) is a multi-annual programme that encompasses several instruments for the protection of critical infrastructures in Europe as depicted in Figure 1. The legislative instrument is the Council Directive 2008/114/EC *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (see [2]).

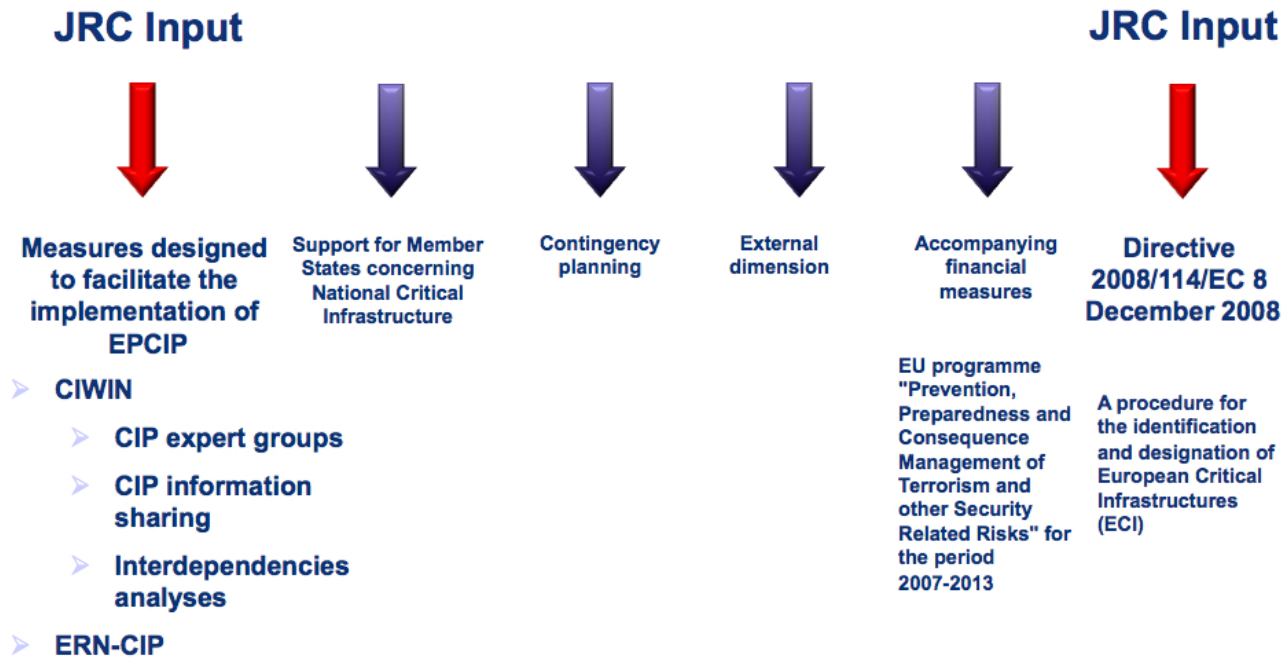


**Figure 1:** *The European programme for Critical Infrastructure Protection (In red JRC involvement)*

The scope of the Directive covers only the energy and the transport sector.

The identification and designation process follows a 4-step procedure that is based on the sectoral and cross-cutting criteria. More information on the identification and designation process can be found in [3]. These criteria have been defined on the basis of numerous impact assessments and studies carried out by JRC and relevant stakeholders and have been the subject of intensive negotiations. However, it is important to stress out that for the definition of the cross-cutting and sectoral criteria no risk assessment work has been carried out . A very good summary of the relevant activities can be found in [4].

The review of the EPCIP Directive has officially started on the $12^{th}$ of January 2012 three years after its adoption. Issues related both to the scope as well as the processes of the Directive will be discussed under the light of the continuous evolvement of critical infrastructures. This evolution has led to more complex systems with the interaction of cyber and physical layers. The boundaries of the sectors are not any more clearly defined thus in several cases it is rather difficult to classify a certain infrastructure within the limits of sectors. This reflects the complexity that has brought in place the interconnectivity of infrastructures for delivering vital societal services.

Within the framework of the EPCIP Directive, support activities such as workshops are taking place at a regular basis (workshops on the implementation and application of the Directive). During the VI Workshop on the implementation and application of the Directive, the Member States asked for a closer look at systems approach for critical infrastructures. Risk assessment methodologies are central in this approach.

### 1.2.2 The US Critical Infrastructure Protection (CIP)

The Homeland Security Presidential Directive (HSPD-7) established U.S. policy for enhancing critical infrastructure protection by establishing a framework for the Department's partners to identify, prioritize, and protect the critical infrastructure in their communities from terrorist attacks. The directive identified 17 critical infrastructure sectors and, for each sector, designated a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programmes and activities. HSPD-7 allows for

the Department of Homeland Security to identify gaps in existing critical infrastructure sectors and establish new sectors to fill these gaps [45]. For each Sector-Specific Agency a sector-specific plan has been developed for the implementation of the National Infrastructure Protection programme (NIPP) in each sector. Clearly the US approach is sectoral and that is similar to the approach that has been implemented in EPCIP. However, in US CIP there is a tendency to focus more on resilience issues. Furthermore in the US CIP there is no formalized procedure in analogy with the EPCIP Directive for the designation of critical infrastructures and assets.

The National Infrastructure Protection programme (NIPP) [6] is the implementation framework of the US CIP. It provides the guidelines for the implementation of the CIP programme. Among others it integrates the efforts for critical infrastructure protection measures in the various sectors, it defines the roles and responsibilities of the several actors at state and federal level and also sets the framework for a risk management framework for critical infrastructures. The latter is further analysed in the present report.

### 1.2.3 National Strategy and Action Plan for Critical Infrastructure Protection in Canada

The National Strategy for Critical Infrastructure ([7]) sets the framework for strengthening the resiliency of critical infrastructure in Canada. Clearly the programme gives emphasis to the resilience aspect of critical infrastructures as the ultimate goal to be achieved. The vehicle to obtain these objectives is through building partnerships, implementing an all-hazards risk management approach and information sharing.

The action plan for critical infrastructures is the implementing element of the national strategy. It sets out the action items in the areas of partnerships, risk management and information sharing that are the building blocks of the action plan. Particularly interesting in this action plan is the distribution of responsibilities among actors, that is federal government, provincial/territorial governments and critical infrastructure operators. Thus it promotes a multi-layer approach that requires the collaboration of

the various actors that is based on information sharing. Furthermore, the distribution of responsibilities clearly demonstrates that resilience stays at the territorial and government levels whereas the main role for operators remains the one of identifying, managing and mitigating the risks associated to their environment. Clearly this stems from the fact that resilience cannot be handled at asset/operator level since it requires the collaboration of various actors, in many cases also involving actors in different sectors. This is something that the national strategy has fully taken on board during the establishment of the plan.

# 2 State of the art of Risk Assessment methodologies in EU and worldwide

## 2.1 Criteria for methodology assessment

The aim of the present report is to obtain a structured review of the existing methodologies at EU and global level, identify gaps and prepare the ground for the proposal of a risk assessment methodology at European level. The aim is not to establish a new methodology from scratch but rather build on existing knowledge in Europe and worldwide so that it will be suitable for European critical infrastructures risk assessment needs. Thus this work is the first of a series of reports that will follow during the process of the Directive review.

Clearly there is an extensive list of methodologies. We only present a selected number of these based on their citation records and their recognition in the scientific community. In order to obtain a structured review, the evaluation of these methodologies took place according to the following criteria:

- Scope of the methodology: Which sector is addressed, to whom it is addressed (Policy makers, researchers, operators etc.).
- Objectives of the methodology.

- Applied techniques and standards.
- Interdependencies coverage.
- Is resilience addressed?
- If cross-sectoral methodology, how are risks compared across sectors?

The report is structured as follows. First we present a theoretical introduction in order to set the scene at research level. Then we present selected methodologies and relevant implementation tools that are assessed according to the above listed criteria. Finally we present a gap analysis on the elements that are still missing at global and mostly at European level.

## 2.2 Risk Assessment methodologies: Theoretical Background

The necessity of a cross-sectoral approach to RA is not a totally new issue. Indeed, RA t is by itself cross sector, if we consider that technical installations, human operators, and organization represent already a rich diversity in any RA problem set up. Nonetheless, a new challenge exists, which is represented by the fact that field of play of complex systems is continuously enlarging. For instance, a power grid is an infrastructure which does not work in isolation anymore. The same holds for the communication networks, Internet, railway transport and so forth. A disruption of service is not confined but instead is propagating rendering the whole network more vulnerable (see [8]).

The modelling scope has changed accordingly, from the concept of complex system to the system of systems (SoS). While complex systems still got boundaries and defined architecture, a system of systems is more blurry in boundaries and may evolve in time. An infrastructure is an instance of a system of systems. Definition and technical issues on systems of systems engineering may be found in the book of [9] and in the work of [10] and [11], just to mention only a few. A research agenda on System of Systems Engineering (SoSE) can be found in [12] in which a number of relevant topics that need to be addressed

are outlined. This work can be compared with the state of the art in CIP modelling that is presented by Yusta et al. [13].

The choice of methodologies is vast, though in several cases the application of the existing approaches is not straightforward. In addition it is not clear whether the needs of emerging disciplines can be satisfied. In many circumstances, there is room for significant innovations. In the literature one can identify three different approaches: application of RA methodologies to infrastructure, structural analysis and behavioural analysis.

Applications of risk assessment to SoS, with the necessary adjustments, can be found in [14], in [15] and [16]. Structural approaches assume the existence of a system of systems topology, which accounts for interdependencies. This field of research is particularly rich of contributions, starting from the classification of interdependencies [1], [17] to their use in vulnerability analysis, see for example [18], [19]. Behavioural analysis aims at unveiling subtle mechanisms of failure propagation, cascading effects that occur as consequence of complex interactions among systems. The majority of this approaches resort to the theory of resilience [20], [21] and the emerging behaviour [22]. But there are also studies on building common platforms for the simulation of networked systems, see for example the IEEE 1516 standard on High Level Architecture [23], which is currently applied from the scientific community, see for example [24]. It is important to say that in all cases presented, the context stretches the application and definition of a traditional RA framework. Moreover, the most promising research contributions suggest a new paradigm which is closer to the domain of control than risk. In this respect, room for innovation is huge. We mention the work of [25] in which this idea of the control paradigm is applied to interdependent systems and the evaluation of resilience.

## 2.3 Risk Assessment methodologies in EU and worldwide

### 2.3.1 Better Infrastructure Risk and 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). Supporting this activity, 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 and commercial office buildings.

The umbrella programme covering these activities is the ECIP (Enhanced Critical Infrastructure Protection). The cornerstone of such methodologies is the collection of reliable data. The necessary data sets have been collected by 93 DHS Protective Security Advisors (PSAs) who are located throughout the US. Argonne has facilitated this procedure by developing statistical and data mining techniques in order to analyse and display the data in a harmonized and structure way. These data sets undergo a quality assurance and control procedure and cover a wide area of security related components and subcomponents. It can be concluded that in terms of data the programme relies on expert opinion.

The methodology developed within the framework of ECIP covers the facilities in 18 critical infrastructure sectors (Energy, critical manufacturing etc.). This methodology has a sectoral approach that goes down to the assets level and gives priority on the protection measures that are applied mainly against terrorist threats. A particularly interesting point of this methodology is the concept of VI (**V**ulnerability **I**ndex), PMI (**P**rotective **M**easures **I**ndex) and RI (**R**esilience **I**ndex). The concept behind the development of VI is to have a common metric and facilitate the comparison across various sectors of infrastructures that are covered by this methodology. The procedure for establishing the VI starts from PMI that is designed to reflect the increase in protection of certain assets as new measures are applied. The

aim is to provide policy makers with tools that can help in the analysis of the various sectors, identify vulnerabilities and prepare risk reports. An important parameter of this methodology is that it relies on operators for the asset assessment through templates that contain what if scenarios. Thus 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.

Although this methodology cannot be characterized as purely cross-sectoral but more as sectoral that is applied to assets of different sectors, the use of the VI to compare critical assets *protection measures* across sectors is remarkable. An additional important characteristic of this methodology is that dependencies are included in the PMI calculation. For each asset that is analysed it is possible to define on which main sectors (electricity, gas, ICT, etc.) its operation relies on and quantify this through the Redundancy, Resilience and Impact indexes.

Resilience is addressed through RI although it is still in a very preliminary phase. The evaluation of the RI is based on the same methodology as the other indexes (similar data collection methods, operator involvement etc.) and it is based on data on the robustness, resourcefulness and recovery of a facility. In Figure 2 a snapshot of the interface that is implemented for this methodology is depicted.

Concluding, this methodology is excellent for being applied to assets of critical infrastructures, it is mainly addressed to operators of assets and infrastructures while tackling key issues such as resilience requires further development. More information can be found in [26].

### 2.3.2 Protection of Critical Infrastructures - Baseline Protection Concept (BMI)

The Federal Ministry of Interior (Germany), the Federal Office for Civil Protection and the Disaster Response and the Federal Criminal Police Office have issued a baseline protection plan. This protection plan is more than a risk assessment methodology. It is a complete protection plan that stresses out the importance of private companies. It sets as basis the cooperation between infrastructures operators and

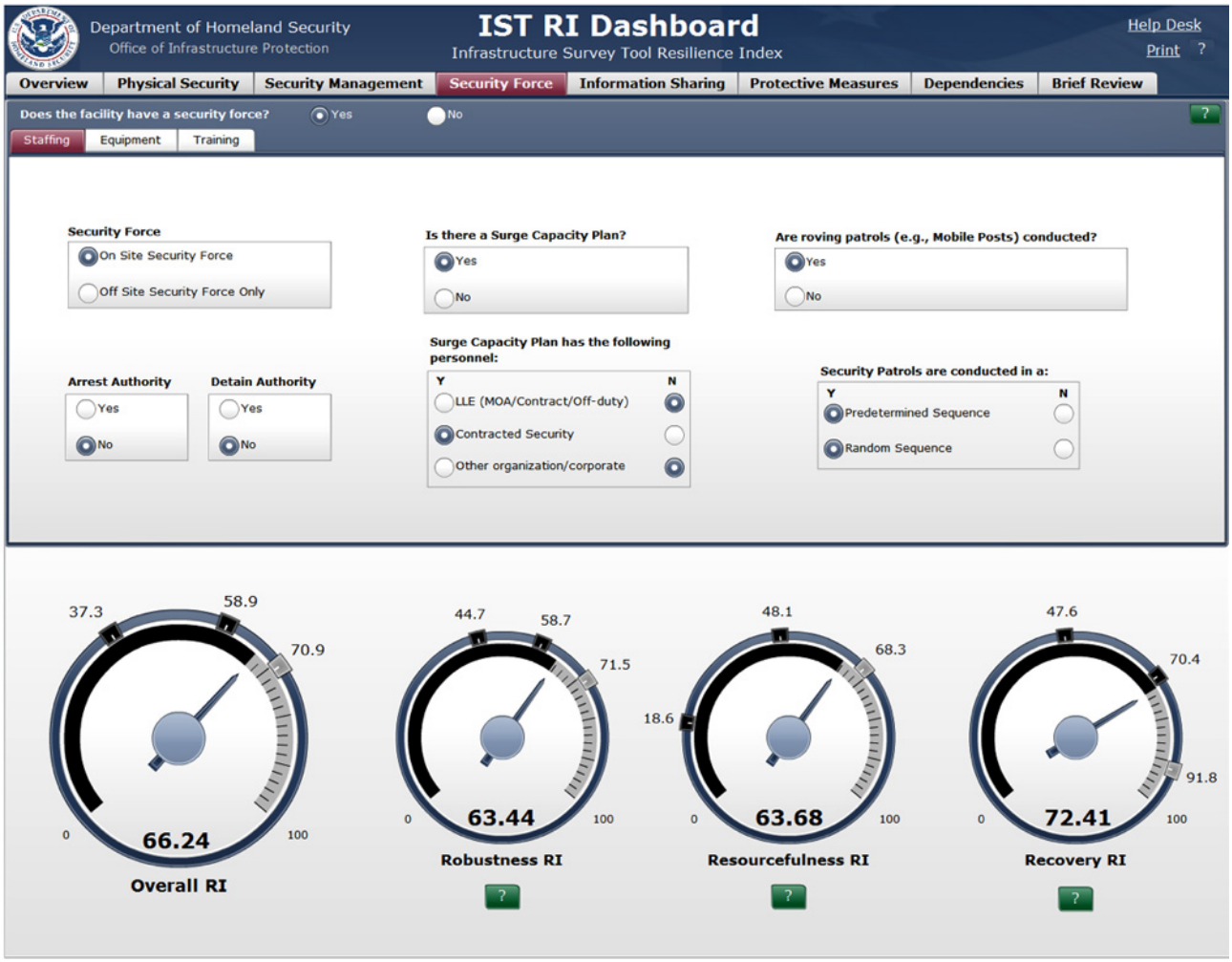


**Figure 2:** *Interface of the Better Infrastructure Risk and Resilience: Resilience assessment page*

state for reassuring the smooth operation of infrastructures with importance to the whole society. It is explicitly mentioned that infrastructure operators are the ones that should implement security measures as they have in-depth knowledge of their infrastructure and the way it operates.

In general it addresses to companies that are doing business in the domain of critical infrastructures with the aim to protect human life. An interesting point is that without being a proper risk assessment methodology, most of the corresponding elements are in place in the form of recommendations. There is a substantial and detailed list of possible threats that expands from natural hazards to terrorism and criminal acts. Then recommendations for the potential vulnerable points are identified for these categories

of threats.

The facilities protection measures are also part of the report. This is the point at which risk assessment is entering the stage. The aim of the risk assessment is focused on the identification of the various hazards. Particularly interesting is the fact that there is a dedicated section on the way to treat issues related to interdependencies or domino effects as they are called in the document. These are treated as secondary effects, or indirect threats that are related to the level of dependency of the infrastructure under concern with respect to an event that is not developed within the confined architecture of this infrastructure. The kind of event is out of concern, the only issue here is whether these indirect effects can indeed endanger the infrastructure under concern and if so through which dependency (geographical dependency for natural hazards are particularly mentioned). Furthermore the study raises the awareness of the operators for the fact that secondary effects can stem from the disruption of supply chains due to events out of the limits of this infrastructure.

Finally certain recommendations can be found in the document concerning risk management, concluding that a certain level of residual risk (after avoiding, minimising and transferring risk) should be recognised. As a consequence a risk officer has to be appointed that will work closely with the personnel within the limits of the company, maintain and update a risk management procedure and interact with the relevant bodies at government level.

To this end, it provides recommendations on the identification of threats, vulnerable points and risk management elements. More information can be found in [27]

### 2.3.3 CARVER2

The $NI^2$ Centre for Infrastructure Expertise is working closely with operators, government, private industry in order to ensure the protection of critical infrastructures in US. CARVER2 is a tool that has been developed in order to serve the needs of critical infrastructure analysis mostly from the

policy maker point of view. CARVER stands for **C**riticality **A**ccessibility **R**ecoverability **V**ulnerability **E**spyability **R**edundancy. NI[2] states that it is a non-technical method for comparing and ranking critical infrastructure and key resources and also claims CARVER2 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.

Figure 3 depicts clearly how this methodology is implemented. In fact there are six different criteria for which an asset or an infrastructure is assessed. The criticality is in fact the impact assessment part of the methodology. It is remarkable that is in good agreement with the cross-cutting criteria of the EPCIP Directive in terms of impact categories (users affected, direct economic loss and cost to rebuild, potential casualties). Accessibility refers to the possibility that terrorists can enter the infrastructure to provoke destruction, it is thus mostly an assessment of the vulnerability of the infrastructure in terms of physical security. The recoverability in fact partially covers resilience since it refers to the bouncing back capability of the infrastructure after failure. The vulnerability covers part of the potential infrastructure vulnerabilities, the ones related to terrorist attacks and more specifically to explosions and chemical/biological threats. Clearly at this point the claimed all hazards approach is not evident. The Espyability criterion refers to the function of an infrastructure as an icon (e.g. cultural site) with indirect impact. However, the implementation to quantify this is not thoroughly explained. Finally the Redundancy refers to the alternatives that exit for the asset in consideration.

Particularly interesting is the way that interdependencies are assessed. The user has a list of sectors that are affected by the loss of an asset. Thus for assets that belong to the same sector (e.g. transport) it may be the case that different sectors are affected. What needs to be further clarified is at which level the interdependencies have been defined. Most probably the links between the various assets of different sectors have been predefined. In addition it is not clear what kind of interdependencies are included in tool (cyber, physical, functional, geographical).

The user receives reports in various forms as well as a score for the classification of the asset. This scoring enables to perform *apples with oranges* comparison and it is a feature that indeed provides a cross-sectoral harmonized metric for the assessment of the importance of different infrastructures.

What has to be stressed out though is that it is a methodology goes down to asset level assessments. A higher level or systems approach is missing. Resilience is only partially considered. More details can be found in [28].

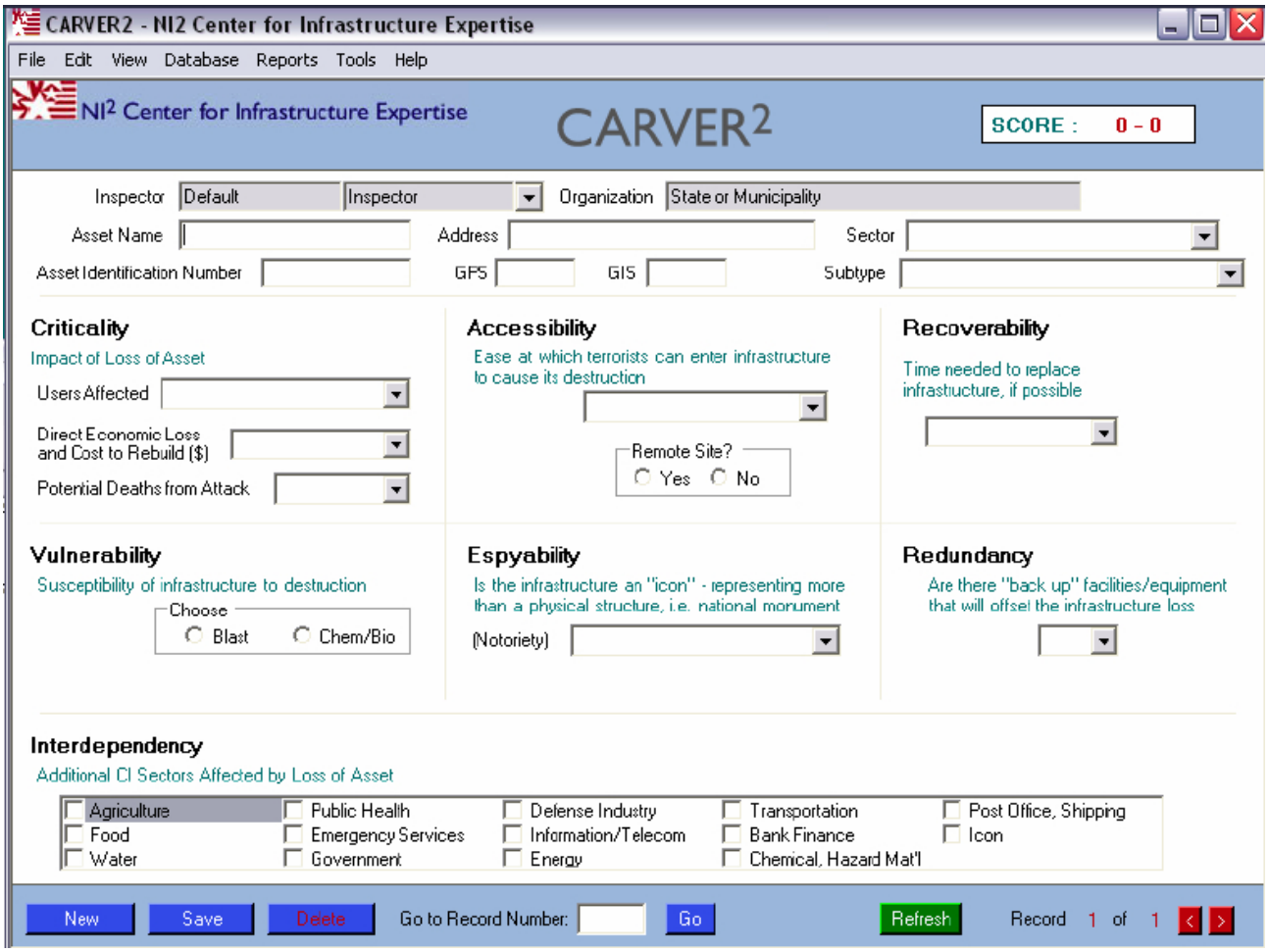


**Figure 3:** *Implementation of the CARVER2 tool*

### 2.3.4 Critical Infrastructure Modelling Simulation (CIMS)

An interesting approach for simulating critical infrastructure disruption has been adopted by Idaho National Laboratory supported by the U.S. Department of Energy. The software tool that has been developed back in 2005 aims at providing to policy makers and mostly decision makers with a tool to take quick decisions to face threats and mostly natural disasters. It is important to mention that hurricane Katrina provided the incentive to develop this tool.

The main features of this tool is that it visually portrays the interoperability of numerous infrastructure sectors and it provides the possibility to create models on the fly from open source information. Thus it is possible in case of a destructive event to capture the dynamics of the cascading effects and the way this affects the operation of emergency teams.

The construction of the models is based on simple maps or aerial photos using high level aggregated information, thus the model development does not require detailed engineering data. This gives an advantage for rapid model development and also for real time updating of the model on the basis of available information from the evolution of the event.

The system is intended to be used at the level of cities or counties mostly for the prioritization of emergency response on the basis of the number of people that are affected. Clearly it is a methodology that is purely cross-sectoral with focus on the interdependencies of infrastructures at high level of abstraction, but it cannot be classified as a pure risk assessment methodology but rather as an impact assessment and interdependencies assessment one. Resilience is not considered in its full extent but rather implicitly at the recovery phase with the prioritization of emergency measures. In addition it is not the resilience of a certain infrastructure that is implicitly assessed but rather the resilience of the society by optimizing the emergency measures. More information can be found in [29].

### 2.3.5 Critical Infrastructure Protection Decision Support System (CIPDSS)

CIPDSS is a tool for information and decision support for the protection of critical infrastructures. It is a pure risk assessment tool that accounts the probability of a threat, vulnerabilities and impact for all hazards and different types of infrastructures. It is applicable to almost all kind of infrastructures. The main audience for this methodology/tool are decision makers that have to decide upon different mitigation measures and operational tactics and prioritize the resources for protecting critical infrastructures. This is taking place by performing simulation of the event considering uncertainties in the input (threat, vulnerabilities) which provides also an estimation of the uncertainty for the output, in other words on the impact of the event.

An important feature of this methodology is that it accounts for interdependencies (first order) between 17 critical infrastructure sectors. Being a pure risk assessment tool, the resilience is out of the scope. It is only implicitly consider by using the risk assessment results for prioritization of the resources for intervention, thus only the recovery aspect of resilience is somehow present in this methodology.

The major highlight of this methodology is the risk informed decision making process. Different options (e.g. mitigation measures or doing nothing) are evaluated according to the certain decision metrics (fatalities, economic loss, etc.). Thus the evaluation of the impact through these common metrics overcomes the problem of comparing risks among sectors. In fact the impact is aggregated for the various sectors into the final value of one of the common metrics. Finally it is a methodology that is applied at high level systems of infrastructures (e.g. national). In Figure 4 the framework of this methodology is presented.

More information can be found in [30].

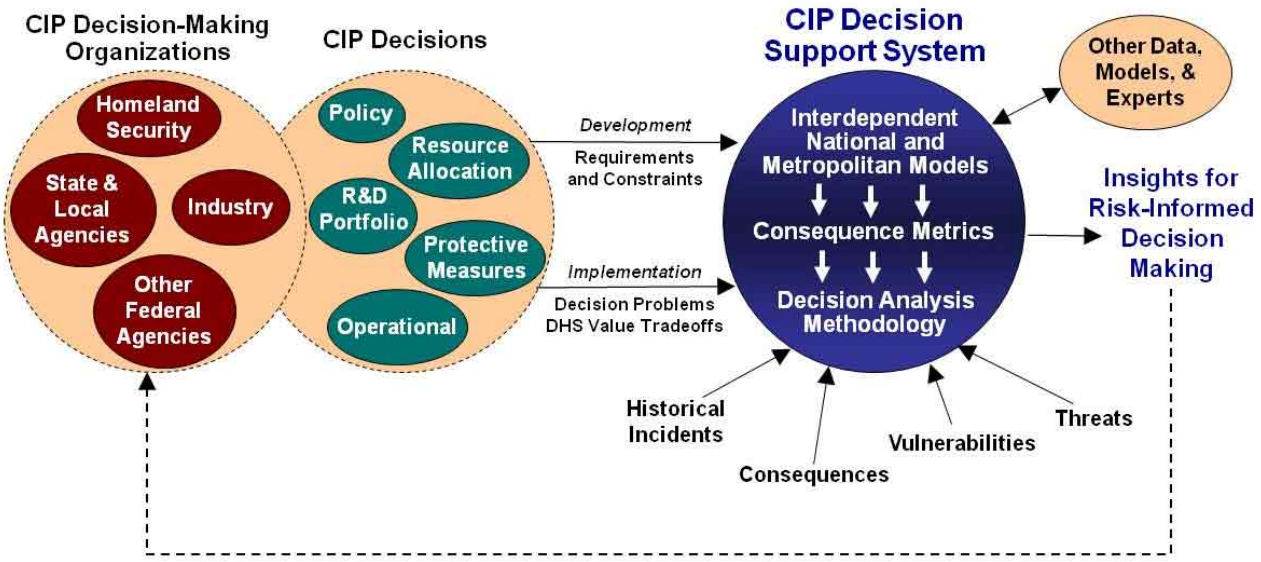


**Figure 4:** *Framework of the Critical Infrastructure Protection Decision Support System (CIPDSS)*

### 2.3.6 Critical Infrastructure Protection modelling and Analysis (CIPMA)

The CIPMA project is a major security initiative launched by the Australian Government in order to build the capacities for the protection of nation's critical infrastructures. The outcome of this programme (it seems to have some similarities with the EPCIP) is a software tool that combines simulation models, databases, GIS and economic models. The target group for this tool are policy makers and industry in order to evaluate different scenarios of critical infrastructure disruption.

It is particularly interesting to mention that CIPMA is restricted to a rather limited range of critical infrastructure sectors, namely Energy, Telecommunications, Banking and Finance. A key element of this tool is that GIS functionality is at the core of this system. GIS is used for data gathering, modelling and visualisation of the results. This methodology is focused on four main areas:

- CI failure consequences: Economy and population consequences with GIS visualization of the results, duration of failure, dynamics of critical infrastructure systems
- Single points of failure: Identification of particularly vulnerable points that can trigger important

cascading effects

- Risks: Elaboration of risk maps
- Investment and mitigation strategies

Interdependencies on the previously mentioned priority sectors are taken into account. Decision makers at national level are the potential users of this tool, thus it must be applicable to high level systems of infrastructures rather than detailed assets. Resilience has not been among the main targets of the project, however, it is implicitly included mainly through the investment to mitigation strategies. Although this is mainly for risk reduction, if applied measures aim at reducing the impact of the threat (not the probability of occurrence) then one can assume that resilience is implicitly accounted for in this methodology. Furthermore, according to the developers of this tool, the aim is to assist also recovery thus resilience is indeed partially assessed.

Finally the methodology is based on an all-hazards approach (natural and man-made threats are explicitly mentioned). More details in [31].

### 2.3.7 CommAspen

CommAspen in the evolution of the first version of an agent-based tool that has been developed in the 90's in order to model the interdependencies between electric power systems and other infrastructures that are essential for the US economy. This last version has been developed in order to include the interdependencies of the telecommunications sector and other infrastructures.

The tool is focusing on telecommunications, electricity and finance. It is a highly technical tool that requires a certain level of expertise in order to be used. This is mainly due to the modelling techniques that have been adopted (agent-based) as well as on the setup of the input file in order to proceed with the analysis. This tool cannot be classified as a risk assessment tool but rather as an impact assessment tool

since it models the behaviour of the interdependent system of infrastructures once there is a decision or an event in the telecommunications sector. It is important to mention at this point that no dependencies of the communications sector on other infrastructures are considered.

The network system that supports infrastructures for financial transactions is modelled using a dedicated agent. The idea behind this modelling technique is to be able to model network outage impact on dependent infrastructures. What is particularly interesting in this approach is that the communications infrastructure (in fact ICT) is not assessed as a separate sector/infrastructure but rather as an underlying layer tightly integrated with the infrastructure for which the impact is assessed. This can be considered as an example on how ICT sector can be integrated in critical infrastructures at European level since the EPCIP Directive does not cover this sector for the moment. In addition, implementing such an approach it is possible to avoid the inherent problem of defining what is ICT infrastructure and defining the limits of this sector.

Resilience is not addressed by this methodology. More information on this methodology can be found in [32].

### 2.3.8 COUNTERACT

This approach is closer to an organisational risk assessment methodology containing all the relevant items. Counteract (Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities) has been an FP6 funded project. This project is focused on the transport and energy sectors and it is focused on terrorist threats. Thus a priori this methodology is sectoral and covers a certain part of the threats spectrum. According to this consortium, security measures in the transport sector are applied in a non-structured and inconsistent manner, mostly on a case-by-case basis. In order to remediate this, the consortium proposed to adopt a security risk assessment methodology as the first and most important step towards securing transport infrastructure in a consistent way.

The risk assessment methodology presented in this project is focused on assets and operators of any size, thus excluding an approach at the systems level. The security risk assessment is divided in two parts, the risk analysis and the vulnerability assessment. The risk analysis focuses on the probability of an event and the impact it may have, while the vulnerability assessment evaluates the safeguards in place for the corresponding risks for the various assets. It is a rather different approach as to what is risk assessment with respect to what is widely acceptable.

The probability of realisation of a threat (terrorist threat) is classified according to a 5 degree scale (very high, high, possible, low, very unlikely). It is important to mention that the classification of a threat according to this scheme mostly resides on past events within the limits of this company or within the limits of similar companies in other areas of the world. It thus mainly relies on past experience.

The impact/severity assessment follows a similar approach and it is classified in escalating categories (Disastrous, Critical, Marginal, Uncritical). The combination of probability of threat realisation with the impact provides the risk categories (20 categories, although both threat probability and impact categories can be modified and adapted according to the needs of the assessment).

The vulnerability assessment follows the probability assessment of a threat and the impact assessment. It is applied to detect gaps and weak points in the prevention and mitigation of threats and incidents as well as diagnosing potential for optimising the safeguards in place. Basically the vulnerability assessment evaluates additional potential measures against the risks that have been diagnosed during the risk analysis process. These measures are analysed considering the following parameters:

- costs
- Effectiveness
- Time for implementation
- Insurance impact

- Impact on the daily basis operation

This part of the methodology can be classified within the limits of risk mitigation and risk management and less within the limits of a traditional risk assessment. More information can be found in [33].

### 2.3.9 The DECRIS approach

The DECRIS approach 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. The main issue of these risk assessment methodologies, which is common at global level, is exactly the sectorial approach and the assessment of each sector independently. Thus DECRIS project aims to 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. The target group for this methodology is policy and decision makers.

The DECRIS methodology is based on a four-step procedure:

- Establishment of event taxonomies and risk dimensions.
- Simplified Risk and Vulnerability Analysis for the identified events.
- Selection of events to be further analysed.
- Detailed analysis of selected events.

Clearly it is a methodology that is not highly differentiated with respect to a typical risk assessment one. However, a refinement mechanism has been incorporated in order to narrow down the list of

events that have to be assessed. This selection process is maybe the highlight of this methodology. The selection process is taking place on the basis of the importance of the risk, of the amount of impacted infrastructures and also on the communication difficulties of this event to the public. However, the issue of the comparability of the consequences of one event on different infrastructures still remains open.

A proof of concept of this methodology has been setup for the city of Oslo. For each of the four categories of infrastructures that have been considered (Electricity, Water, Transport, ICT) a number of events have been identified. For each of these events, the above mentioned criteria are applied and a short list of scenarios to be further assessed is established. In principle this methodology fosters the collaboration between the various stakeholders in the different sectors in order to widen their understanding on the interdependencies across sectors.

Resilience is not directly assessed in this methodology. More information can be found in [34].

### 2.3.10 European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM)

EURACOM has been a $7^{th}$ Framework programme funded project. The aim of this project was to develop a holistic risk assessment methodology that covers all hazards for all sectors although the name of the project may be misleading. In fact it is not a methodology with developed supporting tools but rather a methodological framework. The implementation tools have still to be developed. Within the framework of this project a risk assessment methodologies state of the art study has been conducted focusing mainly on risk assessment methodologies at European level.

The methodology consists of seven well defined steps:

1. Set up an holistic team with an holistic view
2. Define the holistic scope

3. Define risk assessment scales
4. Understand the assets
5. Understand the threat context
6. Review security/Identify vulnerabilities
7. Evaluate and rank the risks

Clearly it is a very wide framework with several interconnected elements. At this point it is important to mention that the scope of the methodology exceeds the limits of assets and it is suitable to be used for risk assessment at higher level (CI sector, countries). Furthermore, the methodology is extended to risk management by assigning responsibilities over all levels reassuring that all risks are considered.

The target group of this methodology is policy and decision makers. Resilience is not addressed. More information can be found in [35].

### 2.3.11 Fast Analysis Infrastructure Tool (FAIT)

National Infrastructure Simulation and Analysis Centre developed the Fast Analysis Infrastructure Tool (FAIT) in order to support DHS by determining the significance and the interdependencies of US critical infrastructures. Obviously this tool is addressed to policy makers and decision makers. Interdependencies are a first priority of this methodology and implementing tool.

FAIT is a synthesis of infrastructure data and expert knowledge. This tool consists of 4 main elements, namely interdependency assessment, co-location of critical infrastructures, information association and economic impact. Interdependencies are treated based on expert knowledge that is coded in a rule-based experts system software language that is used to express the relationships between the various infrastructures. A wide range of interdependencies are considered, however, geographical interdependencies seem to be treated in a different way as this is part of the second major element of this

methodology (co-location). This element retrieves the geographical dependencies of assets based on the relevant geospatial data.

Particularly important is the element of economic impact. This element is designed in order to evaluate the economic impact of asset disruption on a specified region. Data on the disruption duration and recovery are used in order to obtain the economic impact using I/O modelling techniques.

FAIT is not a typical risk assessment tool but rather an impact assessment tool, as the probability of an event is not considered. In addition the aim of the tool is mostly on the functioning of assets and infrastructures and their interdependencies.

Clearly the tool is not addressing resilience. However, it is a very interesting example that can be very well adapted to European reality. More information can be found in [36].

### 2.3.12 Multilayer Infrastructure Network (MIN)

Multilayer Infrastructure Network is a methodology that has been developed by the Purdue School of Civil Engineering. The objective is to generalize the paradigm of transportation network to infrastructures, and apply optimisation. In fact all types of infrastructures can be assessed. The approach of this methodology seems to be totally different with respect to the rest of the methodologies assessed in the present report in terms of theoretical background. This is based on game theory and optimisation under multiple constraints, in addition to concepts of network reliability. Interdependencies are addressed by capturing the flow dynamics as input-output (Leontief model-like) across sectors. The model includes heterogeneous interdependencies in the same framework (inspired by Rinaldi's work on interdependencies). It is important to mention at this point that additional interdependencies with respect to Rinaldi's work are included in the framework.

The analysis is performed by agent based modelling and simulation. The outcome is the flow of quantities at the steady state, which makes possible to obtain an optimal allocation of resources. However,

this methodology requires a high level of expertise and technical knowledge in order to be used. This obviously reduces its area of applicability. In addition it is not a pure risk assessment methodology but it is restricted to impact assessment. Finally resilience remains out of the scope of this methodology.More information can be found in [37].

### 2.3.13 Modular Dynamic Model

Sandia National Laboratories are involved in an important number of projects related to critical infrastructure protection. The Modular Dynamic Model is the outcome of one of these projects and it has been developed based on the issue of interdependencies. All sectors and infrastructures are falling within the scope of this methodology. The objective is to analyse the risk by modelling infrastructure interdependencies. The analysis outcome is the estimate of the consequences due to an applied perturbation.

The theoretical background is based on agent-based modelling and dynamic systems modelling. This methodology follows a kind of hierarchical modelling approach in the sense that it provides a first screening that can be followed by a more detailed analysis if the identified risks require such action. However, the whole approach is rather complicated and requires substantial effort from the end user to obtain accurate and reliable results. In addition a huge data set is necessary that further complicates the analysis process.

The target group of this methodology is primarily CI operators and decision makers but with a certain level of expertise. Resilience is not explicitly addressed.

More information can be found in [38].

### 2.3.14 Agent-Based Laboratory for Economics (N-ABLE)

This tool has been developed by NISAC (National Infrastructure Simulation and Analysis Centre). It is an agent-based microeconomic framework that aims at analysing the interdependencies between firms and the infrastructures they use. The scope of the methodology is to identify which economic sectors are most vulnerable to the disruption of infrastructures. What is particularly interesting is that this methodology can be used for the assessment of supply chain impact due to infrastructure disruption. This is feasible since the economic sector concept can be used for the representation of supply chains (such as the chemicals supply chain).

The theoretical background is on the theory of complex networks (Barabasi, [39]) and agent based modelling (for simulation). The tool is mathematically sophisticated and requires experienced users in order to render reliable results.

The target group of this methodology is mainly researchers and scientists working in the field. CI operators and policy makers may benefit from this methodology but this depends on their level of expertise.

N-ABLE cannot be characterised as a pure risk assessment methodology but rather as an impact and interdependencies assessment methodology. However, if there is one issue to highlight this is the capability to model impact on supply chain due to infrastructure disruption.

Resilience is not in the scope. More information can be found in [40].

### 2.3.15 Net-Centric Effects-based operations MOdel (NEMO)

This methodology may seem irrelevant to be included in this report. A first reading of the methodology would confirm this statement. In fact this methodology has been developed for military operations to be used as a real-time operations assessment tool. The main element of this methodology is that it treats

the opponent's infrastructure as a system of interconnected networks thus it covers all sectors. Here the identification of the interdependencies does not aim at reducing the impact but rather identify the critical elements of the network that can maximize the impact through cascading effects. Thus is the other side of the coin using the same principles as for infrastructure protection.

The theoretical background is based on similar tools for supporting military strategy, e.g. against sabotage, and for assessing vulnerabilities across domains. The analysis provides consequence management (what if analysis) with respect to closer effect, and with second order effects (spread throughout the infrastructure). Results are mapped in GIS.

Obviously the tool is addressed to military authorities. However, CI operators and decision makers can benefit from this as it is possible to identify the vulnerable points of assets and infrastructures by observing the issue of protecting infrastructures from a different angle.

At this point it is important to mention that the tool leaves the freedom of defining what a dependency is, so also functional on/off dependencies are possible. An ideal line of command is postulated like in the military context, which should apply the best strategies to the diverse players, i.e. net centric. Though, this is hardly the case in heterogeneous infrastructures.

Resilience is implicitly within the scope of the methodology through the protection and recovery measures. More information can be found in [41].

### 2.3.16 Network Security Risk Assessment modelling (NSRAM)

The NSRAM methodology has been developed by the Institute for Infrastructure and Information Assurance at James Madison University. The methodology covers all interconnected infrastructures and the objective is to determine how the systems respond and interact to various kinds of accidents and attacks.

The theoretical background is agent modelling simulation in stochastic environment. Besides failure events, the model also includes repair capability that models the effects of repair personnel or part scarcity, communication requirements and uncertainty. This is an element that has not been encountered in any other methodology presented in this report. Among other advantages, this repair element can be used for the modelling of human behaviour in case of system damage. The NSRAM emphasizes interactivity and interconnectedness among the infrastructures simultaneously.

The analysis of the models returns the system service performance, with security and risk metrics over time. It also identifies the most serious failure modes, implementing cost-effective countermeasures and planning for reconstitution. The target group of the methodology is CI operators and decision makers.

Apparently resilience is addressed in this methodology mainly through the recovery process. More info can be found in [42].

### 2.3.17 RAMCAP-Plus

The RAMCAP-Plus methodology has been developed by ASME (American Society of Mechanical Engineers) as an all hazards risk and resilience assessment methodology. The scope of the methodology covers all infrastructures, with the objective of addressing protection of nations critical infrastructures (avoiding hazardous events or their consequences) and resilience (rapid return to full function after disruptive events).

The methodology is based on a seven step approach namely:

1. Asset characterisation
2. Threat characterisation
3. Consequence analysis

4. Vulnerability analysis

5. Threat assessment

6. Risk and Resilience assessment

7. Risk and Resilience Management

The methodology is particularly interesting as it incorporates a number of important features for risk assessment of infrastructures. The first element is that the methodology avoids unnecessary detail by focusing on the most critical assets at a facility. The second important element is that the developers of the methodology have identified the necessity for cross-sectoral risk comparisons which is rarely offered by the existing risk assessment methodologies. Finally the methodology has a simplified approach and it is based on existing risk assessment techniques but the high-level approach is pronounced.

The target group of this methodology are CI operators and decision makers.

Resilience is addressed in this methodology. In fact it constitutes a central element of the methodology, a feature that is not developed at this level by any other methodology analysed in the present report. More info can be found in [43].

### 2.3.18 Risk and Vulnerability analysis (RVA )

This methodology has been developed by the Danish Emergency Management Agency (DEMA). The scope of the methodology is all sectors with the objective of assessing threats, risks and vulnerabilities in relation to those functions that are particularly critical for the effective functioning of society, including during major accidents or catastrophes.

The methodology consists of 4 discrete steps:

1. Purpose and scope of the analysis

2. Scenario development

3. Assessment of risks and vulnerabilities

4. Graphical representation of risk and vulnerability profile

The theoretical background is based on qualitative risk assessment. The risk and vulnerability analyses are conducted for a general purpose rather than at detail level. The focus is on *critical functions*, which denote those activities, goods and services that comprise the basis for the ability of society to function and, therefore, must be upheld and continued during major accidents or catastrophes. The RVA model is primarily based on the use of qualitative rather than quantitative data. All assessments are conducted using the index method, in which a level for probability, consequences and vulnerabilities is stated on a scale from 1 to 5, where 1 is best and 5 is worst.

The target group are primarily government authorities and secondarily other interested parties with preparedness responsibility, both public and private entities. Resilience is not addressed.

More details can be found in [44].

### 2.3.19 Sandia Risk Assessment Methodology

Sandia National Laboratories presented back in 2000 a risk assessment methodology for the protection of physical critical infrastructures. This work has been performed on behalf of an agency of the US Government, thus it has a clear orientation towards policy makers at national level.

What is particularly interesting is that in the abstract of the report there is a clear link between critical infrastructure and services and also continuation of service even after anthropogenic threats. This translated to modern critical infrastructure jargon would be *increase the resilience of critical infrastructures against terrorist and man-made threats*. Clearly resilience is within the objectives of the methodology although it is not explicitly mentioned.

The methodology comprises seven distinct steps:

- Characterise facility
- Identify undesired events ad critical assets
- determine consequences of undesired events
- define threats to the facility
- analyse protection system effectiveness
- estimate risks
- suggest ad evaluate upgrades to the system

Fault tree analysis is the main tool of this methodology to identify the vulnerabilities. This implies that the user of the methodology is in the position to master this methodology and apply it to assets of critical infrastructures. It is important to mention that fault tree analysis is mostly adapted for use in selected assets rather than complex networks, although this is also feasible by adapting the fault tree methodology. By applying fault tree analysis it is possible to identify failure scenarios and critical elements for the functioning of the asset.

A thorough investigation of the propose process demonstrates that this risk assessment methodology follows a path that this rather different with respect to a traditional methodology (i.e. threat, vulnerability, risks). At threat level the methodology starts from the undesired events and the relevant consequences in order to narrow down the number of possible threats only to those that can lead to these undesired events. Then for these prioritised threats a quasi-typical risk assessment methodology takes place with the addition of the protection system effectiveness that is expressed in terms of reducing the probability that a threat is successful. Thus the final risk value takes into account the effectiveness of the protection measures.

The final step of the methodology is to evaluate whether the risk is acceptable or not. In case the risk is unacceptable, it is necessary to evaluate again all assumptions and then proceed to the improvement of the protection measures. At this point it is necessary to evaluate the trade-off between increasing the security and putting additional burden to the operations of the infrastructure.

The issue of interdependencies as well as cross-sectoral risks is not explicitly mentioned in this methodology mainly due to its orientation versus assets protection from terrorist attacks. Finally as previously mentioned, resilience is only implicitly described in this methodology.

### 2.3.20 National Infrastructure Protection Plan Risk Management Framework

As a last section of this report concerning the various methodologies we have intentionally put the Risk Management Framework of the National Infrastructure Protection Plan (NIPP) developed by the Department of Homeland Security and the corresponding Risk Management framework in Canada (see next section). As a proof of concept of the importance of risk assessment for effective critical infrastructure protection we quote the following phrase that provides an overview of the scope of this framework: *The cornerstone of the NIPP is its risk management framework that establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.*

The scope of the methodology covers all sectors. The objective is to provide a framework that, given national priorities, goals, requirements for critical infrastructure, makes it possible to allocate protection resources effectively in order to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents.

The theoretical background is a classic risk assessment framework, with the specificity of responding to all CI sectors identified in Homeland Security Presidential Directive-7 (HSPD-7), and addresses the physical, cyber, and human considerations required for effective implementation of comprehensive

programmes. The framework has got six steps from goals definition, threat identification, assessment and prioritization of risk, to the validation of protective actions and measures for risk reduction.

The analysis returns the estimate of risk, and validation of protective measures that contribute to reduce the risk. These latter translate into plans with the key initiatives, milestones, and metrics required to achieve the desired risk reduction.

The users are the decision makers at Department of Homeland Security (DHS), Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, and private sector security partners.

Resilience is not explicitly addressed. We have chosen to include in this report Figure 5 that depicts in an excellent way the elements that risk management framework or critical infrastructures has to include. More information in [45].

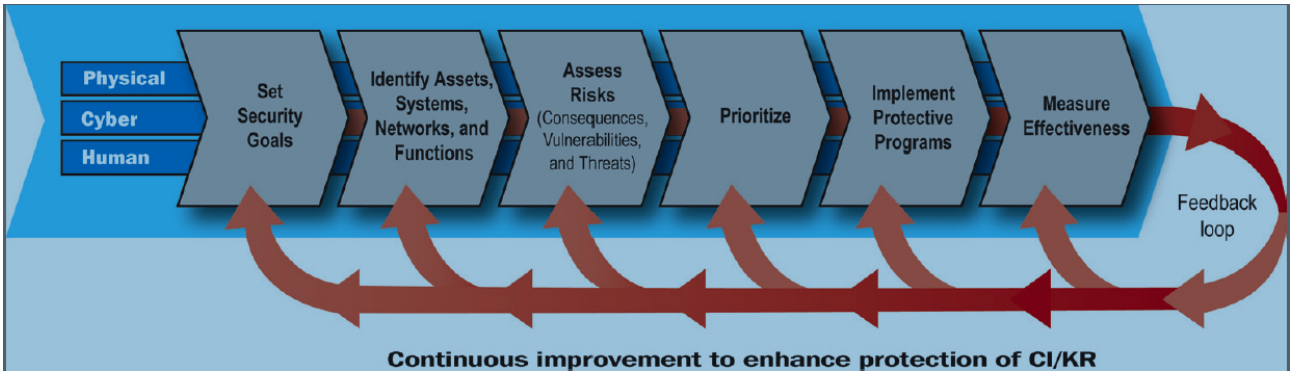


**Figure 5:** *National Infrastructure Protection Plan Risk Management Framework*

### 2.3.21 Risk Management for Critical Infrastructure Sectors (Canada)

One of the main elements of the action plan of the national strategy for critical infrastructure protection in Canada is the risk management framework that is mostly addressed to the operators and jurisdictions. Although the whole strategy and programme fosters collaborative actions in order to improve resilience of critical infrastructures this particular element (risk management) is addressed to operators and local governments.

The risk management framework is based on three pillars:

- Sector risk profiles at national level
- Risk assessments
- Risk management tools and guidance

Concerning risk assessment, the framework sets out some guidelines for the elements of the methodologies but does not indicate which methodology should be implemented. Although interdependencies should be considered, at the same time sector specific methodologies have to be considered which seems to be a contradiction. However, this is not the case as the interdependencies are considered firstly within sectors between the assets/infrastructures of the same sector and then at a second phase between sectors. Thus there is some kind of aggregation of information from sectoral level to cross-sectoral level. Thus cross-sectoral risk should somehow be included in the relevant risk assessment methodologies.

Resilience is not directly tackled at this level but it is part of the national strategy for critical infrastructure protection. The risk management framework and the relevant risk assessment methodologies are the foundation for improving resilience of critical infrastructures.

More information can be found in [46].

## 2.4 Gap analysis

The number of available methodologies in risk assessment for CI is large and only a partial - though significant - sample is presented in this report. 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. As a consequence, these methodologies are tailored to the particular needs of this organization and biased to consider only part of relevant threats. In such context, the application

is facilitated by the knowledge of architecture and functioning principles, which are the preconditions for modelling and subsequent simulation. This precondition is not always met when the risk assessment methodology exceeds the limits of the organization and aims at the assessment of systems of systems, such as interconnected infrastructure, for which the knowledge on architecture and functioning principles is fuzzy. This is the true challenge for upscaling any risk assessment methodology to complex systems.

Policy makers, decision makers and infrastructure operators are aware of this deficiency, and actually ask system analysts to develop effective approaches for assessment of complex infrastructures and lately system of systems. The effectiveness stands in the compromise between the time (and data) necessary to develop a model, and its expressiveness to cope with risk (and resilience), at the level in which the analysis outcome has to feed the decision process. The first step towards this direction has been the development of methodologies that are tailored for the assessment of critical sectors (as these are defined by the policy makers) and for a variety of hazards, e.g. terrorism, natural disasters, man-made threats, etc. The criticality is established along the dimension of interdependency, which is the main challenge for these methodologies. The identification of interdependencies would permit 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*. Most of the risk assessment methodologies considered in this report cope with this issue up to a certain extent. Two main approaches have been identified: aggregated impact and scoring.

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 inter alia to evaluate different disruption scenarios including cascading effects across sectors and evaluate costs and benefits of mitigation measures. A complete risk assessment is possible if the impact is combined with the likelihood of the scenario. If this information is not available then the analysis is just an impact assessment and cannot be used for prioritization of risk mitigation measures especially for HILF (High Impact Low Probability) events.

Scoring approach has inspired a few methodologies. It resembles a multi criteria decision analysis in the fact that the final score produced is the weighted mean of several scores. This approach is qualitative and mostly useful for prioritization of mitigation measures e.g. give priority to a certain sector instead of another one because it can lead to more severe effects. However, this approach is not applicable for cost-benefit evaluation of mitigation measures.

In all available methodologies, resilience seems to be the missing element, or in the best option it is only implicitly addressed. Operators, asset managers, policy makers tend to identify threats and vulnerabilities within their domain of responsibility. This means that the overall picture in which they interact with other actors is never complete. A consequence is the tendency to protect themselves from risk relevant to their domain of responsibility, often by considering worst case scenarios, and thus applying disproportional risk mitigation measures. From the risk assessment point of view this approach is effective but it narrows down the possibilities for a cost-effective risk mitigation.

If the issue would be taken from a resilience point of view, more alternatives to mitigate risks would exist. A resilience analysis requires assessing the infrastructure from a holistic point of view, enhancing coordination and timely response throughout the interdependencies. For example the mitigation of risk for the networked system due to the potential failure of a critical node, besides the avoidance that such an event may develop, can also be tackled by increasing the capacity of the dependent nodes to withstand the perturbation. In order to apply this *resilience paradigm* a higher level of communication and coordination among the operators of the various networked infrastructures is required. This approach is missing from the methodologies that have been presented in this report and to the knowledge of the authors there is no methodology today that incorporates the resilience paradigm, with prevention, resistance to disturbance and failure recovery measures.

The risk assessment methodologies at European level do not match the maturity, in term of effectiveness and completeness of their counterparts in US. This is not surprising considering the fragmentation of several European infrastructures into several countries with different security measures and

security culture, which developed to meet local protection issues. A challenging goal for risk assessment methodologies is to fill the previously mentioned gaps and finally converge into a harmonized framework at European level. This framework should be able to accurately capture interdependencies across different infrastructures, cross-sector and cross borders (unique requirement applicable only to EU) with a focus on resilience. In addition an agreement has to be obtained on a common metric for risk across sectors e.g. economic impact could be one.

In conclusion, risk assessment for critical infrastructures must be considered as an integral part of a wider framework in which the principal tool is the resilience analysis. The continuation of the present work will be the proposition of a resilience assessment framework for critical infrastructures where risk assessment will be a subset and it will aim to bridge the gaps identified in the present work.

# References

[1] Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, pp. 11-25

[2] 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, Official Journal of the European Union, L345/75

[3] Sara Bouchon, Carmelo Di Mauro, Christiaan Logtmeijer, Jean-Pierre Nordvik, Russell Pride, Bastiaan Schupp, Michael Thornton, Non-Binding Guidelines for the application of the Council Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, EUR 23665, 2008

[4] M. Christou, M. Masera, J.P. Nordvik, G. Schumacher, Administrative Arrangement No. 30670-2007-07. Towards the identification and assessment of European Critical Infrastructures, European Commission, JRC56384

[5] http://www.dhs.gov/files/programs/gc_1189168948944.shtm, last accessed 10/03/2012

[6] National Infrastructure Protection Plan, 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[7] http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx, last accessed 29/02/2012

[8] W. Kroeger, E. Zio, (2011) Vulnerable Systems, Springer.

[9] M. Jamshidi editor (2010), System of systems engineering, Innovations for the 21st century,Wiley.

[10] A. Sousa-Poza, S. Kovacic, C. Keating, (2008) System of Systems Engineering: an Emerging Multidiscipline, International Journal of System of Systems Engineering, Vol 1, pp. 1-17.

[11] Alex Gorod, Brian Sauser, and John Boardman, System-of-Systems Engineering Management: A Review of Modern History and a Path Forward IEEE SYSTEMS JOURNAL, VOL. 2, NO. 4, DECEMBER 2008.

[12] Valerdi R, and others (2008), A Research Agenda for System of Systems Engineering, Int. J. System of Systems Engineering, Inderscience Publisher, Vol. 1, pp. 171-188.

[13] Jose M.Yusta, Gabriel J.Correa, Roberto Lacal-Arantegui, Methodologies and applications for critical infrastructure protection: State-of-the-art, Energy Policy 39(2011) 6100-6119.

[14] Yacov Y. Haimes, Models for risk management of systems of systems, Int. J. System of Systems Engineering, Vol. 1, Nos. 1/2, 2008 Copyright 2008 Inderscience Enterprises Ltd.

[15] N. Leveson (2004), A new accident model for engineering safer systems. Safety Science 42(4), 237-270.

[16] Anna-Karin Lindberg, Sven Ove Hansson, Carl Rollenhagen, Learning from accidents - What more do we need to know?, Safety Science 48 (2010) 714-721

[17] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, INL, INL/EXT-06-11464, 2006.

[18] Enrico Zio, and Giovanni Sansavini, Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins Interdependency, IEEE Transactions on Reliability, vol. 60, no. 1, March 2011.

[19] Robin Bloomfield, Lubos Buzna, Peter Popov, Kizito Salako, and David Wright, Stochastic Modeling of the Effects of Interdependencies between Critical Infrastructure, E. Rome and R. Bloomfield (Eds.): CRITIS 2009, LNCS 6027, pp. 201-212, 2010, Springer-Verlag Berlin Heidelberg 2010

[20] E. Hollnagel, D. W. Woods, N. Leveson (Editors) (2006) Resilience Engineering: Concepts And Precepts. Ashgate.

[21] J. P. G. Sterbenz, D. Hutchison, E. K. etinkaya, A. Jabbar, J. P. Rohrer, M. Schoeler et al., (2010) Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks, Vol 54, pp. 1245-1265.

[22] I.A. Herrera, R.Woltjer, Comparing a multi linear (STEP) and systemic (FRAM) method for accident analysis, Reliability Engineering and System Safety 95 (2010) 1269-1275.

[23] IEEE 1516 (2010), Standard for Modeling and Simulation High Level Architecture.

[24] C. Nan, I. Eusgeld (2011), Adopting HLA standard for interdependency study, Resilience Engineering and System Safety, Volume 96, Issue 1, January 2011, Pages 149-159.

[25] R. Filippini, A. Silva, (2011) Modeling language for the resilience assessment of networked systems of systems, Proceeding of the conference ESREL 2011, Troyes 18-22 Sept 2011.

[26] http://www.dis.anl.gov/projects/ri.html, last accessed 23/02/2012

[27] , http://www.bmi.bund.de, last accessed 03/03/2012

[28] http://www.ni2cie.org/downloads/CARVER2demo.pdf, last accessed 23/02/2012

[29] https://inlportal.inl.gov/portal/server.pt/community/national_and_homeland_security/273 /modeling_and_simulation/1707, last accessed 03/03/2012

[30] http://www.lanl.gov/programs/nisac/cipdss.shtml, last accessed 29/02/2012

[31] http://www.csiro.au/Organisation-Structure/Divisions/Mathematics-Informatics-and-Statistics/CIPMA.aspx , last accessed 29/02/2012

[32] Dianne C. Barton, Eric D. Eidson, David A. Schoenwald, Roger G. Cox, Rhonda K. Reinert, *Simulating Economic Effects of Disruptions in the Telecommunications Sector*, SAND2004-0101, January 2004

[33] http://www.transport-research.info/web/projects/project_details.cfm?id=36152

[34] I.B. Utne, P. Hokstad, G. Kjølle, J. Vatn, I.A. Tøndel, D. Bertelsen, H. Fridheim, J. Røstrum, *Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS approach*

[35] http://www.eos-eu.com, last accessed 02/03/2012

[36] http://www.sandia.gov/nisac/fait.htm, last accessed 23/02/2012

[37] http://www.ivt.ethz.ch/news/archive/20030810_IATBR/peeta.pdf, last accessed 23/02/2012

[38] http://www.Sandia.gov/nisac/docs/CRIS_paper_final.doc, last accessed 28/02/2012

[39] , R. Albert, A.L. Barabasi, Statistical mechanics of complex networks, Reviews of Modern Physics, vol. 74, no. 1, pp. 47-97, 2002

[40] http://www.sandia.gov/nisac/docs/ieee-ehlen-scholand.pdf, last accessed 29/02/2012

[41] http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf, last accessed 03/03/2012

[42] http://www.jmu.edu/iiia/wm_library/NSRAM_Application_to_Municipal_Electric.pdf, last accessed 03/03/2012

[43] http://www.asme-iti.org/RAMCAP/RAMCAP_Plus_2.cfm, last accessed 03/03/2012

[44] http://brs.dk/eng/inspection/contingency_planning/rva_model/Pages/rva_model.aspx

[45] http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf, last accessed 03/03/2012

[46] http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx, last accessed 03/03/2012

| Methodology | Sector/Hazards | Users | Objectives | Interdependencies | Cross-sectoral risk | Resilience |
|---|---|---|---|---|---|---|
| **Better Infrastructure Risk and Resilience**<br><br>http://www.dis.anl.gov/projects/ri.html | All sectors/All Hazards | Operators, asset managers, policy makers | Vulnerabilities assessment, risk reporting | Yes | Yes | Yes |
| **BMI**<br><br>http://www.bmi.bund.de | All Sectors/All Hazards | Private companies, CI operators, Policy makers | Vulnerabilities and risk assessment, Foster collaboration between policy makers and private sector | Yes (Recommendations) | No | No |
| **CARVER 2**<br><br>http://www.ni2cie.org/CARVER2.asp | All sectors/All Hazards | Policy makers | Risk evaluation, evaluation of alternatives, allocation of protective measures | Yes | Yes | Yes (partially) |
| **CIMS (Critical Infrastructure Modeling Simulation)**<br><br>https://inlportal.inl.gov/portal/server.pt/community/national_and_homeland_security/273/modeling_and_simulation/ | All sectors/All hazards | Policy, decision makers | Rapid decision making, prioritization of emergency operations | Yes | No | Yes (implicitly) |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1707 | | | | | | |
| **CIPDSS (Critical Infrastructure Protection Decision Support System)**<br><br>http://www.lanl.gov/programs/nisac/cipdss.shtml | All sectors/All hazards | Policy makers | Risk informed design | Yes | Yes | No |
| **CIPMA (Critical Infrastructure Protection Modeling and Analysis)**<br><br>http://www.csiro.au/Organisation-Structure/Divisions/Mathematics-Informatics-and-Statistics/CIPMA.aspx | Energy, Communications, banking and finance/All hazards | Policy makers, industry | Prevention, preparedness | Yes | Yes | Yes (implicitly) |
| **COMM-ASPEN**<br><br>https://cfwebprod.Sandia National Laboratory.gov/cfdocs/CCIM/docs/04-0101_Simulating_Economic_Effects_of_Disruption.pdf | Telecommunications, electricity, finance/ | Policy makers | Impact assessment of ICT disruption | Yes | No | No |
| **Counteract (**Generic Guidelines for Conducting Risk Assessment in Public Transport Networks)<br><br>http://www.uitp.org/knowledge/projects-details.cfm?id=433 | Transport, Energy/ Terrorist threats | Operators, asset managers | Risk reporting, protection measures effectiveness evaluation | No | No | No |
| **DECRIS**<br><br>http://www.sintef.no/project/SAMRISK | All sectors/ All hazards | Policy makers, | Risk and vulnerabilities assessment, | Yes | No | Yes (partially) |

| | | | | | | |
|---|---|---|---|---|---|---|
| /DECRIS/Documents/DECRIS_paper_SAMRISK_final%20080808.pdf | | operators | prioritization of scenarios | | | |
| **EURACOM**<br><br>http://www.eos-eu.com | All sectors/ All hazards | Policy and Decision makers | Holistic, cross sectoral risk assessment | Yes | Yes | No |
| **FAIT (Fast Analysis Infrastructure Tool)**<br><br>http://www.Sandia National Laboratory.gov/nisac/fait.html | All sectors/ All hazards | Policy and decision makers | Interdependencies assessment and disruption impact | Yes | Partial (economic impact) | No |
| **MIN (Multilayer Infrastructure Network)**<br><br>http://www.ivt.ethz.ch/news/archive/20030810_IATBR/peeta.pdf | Transport/ Technical hazards | CI operators and decision makers | Optimal allocation of resources for CIP | Yes | Partial<br><br>(consequences) | No |
| **Modular Dynamic Model**<br><br>http://www.Sandia.gov/nisac/docs/CRIS_paper_final.doc | All sectors/technical hazards | CI operators and decision makers | Failure propagation effects by simulation | Yes | Partial<br><br>(consequences) | No |
| **N-ABLE (Next-generation agent-based economic laboratory)**<br><br>http://www.sandia.gov/nisac/docs/ieee-ehlen-scholand.pdf | All sectors/technical, economic hazard | CI analyst, researchers | failure propagation effects in term of economy losses by simulation | Yes | Partial<br><br>(consequences) | No |
| **NEMO (Net-Centric Effects-based** | All sectors/technical | CI operators | What if | Yes | Partial | Yes |

| | | | | | | |
|---|---|---|---|---|---|---|
| **operations MOdel)**<br><br>http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf | hazards | and decision makers | analysis under malicious attacks | | (consequences) | |
| **NSRAM (Network Security Risk Assessment Modeling)**<br><br>http://www.jmu.edu/iiia/wm_library/NSRAM_Application_to_Municipal_Electric.pdf | All sectors/ Technical hazards | CI operators and decision makers | What if analysis under malicious attacks | Yes | Partial<br><br>(consequences) | Yes |
| **RAMCAP Plus**<br><br>http://www.asme-iti.org/RAMCAP/RAMCAP_Plus_2.cfm | All sectors/ Technical hazards | CI operators and decision makers | Risk assessment and mitigation, multi-level, cross-sector | Yes | Yes | Yes |
| **RVA (risk and vulnerability analysis)**<br><br>http://brs.dk/eng/inspection/contingency_planning/rva_model/Pages/rva_model.aspx | All sectors/ Technical, socio-technical hazards | CI Decision makers | Risk assessment, qualitative | Not explicitly addressed | Yes | No |
| **Sandia Risk Assessment Methodology** | All Sectors/Terrorism, man-made | CI policy makers | Risk Assessment and | Not explicitly addressed | No | Implicitly |

European Commission

**EUR 25286 EN - Joint Research Centre – Institute for the Protection and Security of the Citizen**
Title: **Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art**
Author(s): Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer
Luxembourg: Publications Office of the European Union
2012 – 70 pp. – 210 x 297 cm
EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)
ISBN 978-92-79-23839-0
doi:10.2788/22260

**Abstract**
Effective risk assessment methodologies are the cornerstone of a successful Critical Infrastructure Protection program. The extensive number of risk assessment methodologies for critical infrastructures clearly supports this argument. Risk assessment is indispensable in order to identify threats, assess vulnerabilities and evaluate the impact on assets, infrastructures or systems taking into account the probability of the occurrence of these threats. This report aims at providing an overview of the relevant methodologies at global level.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-25286-EN-N

ISBN 978-92-79-23839-0

Publications Office