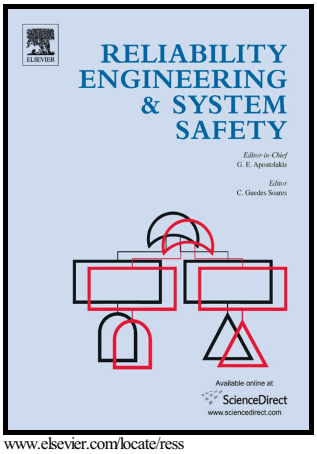
# Challenges in the vulnerability and risk analysis of critical infrastructures

Enrico Zio




www.elsevier.com/locate/ress

PII: S0951-8320(16)00050-8
DOI: http://dx.doi.org/10.1016/j.ress.2016.02.009
Reference: RESS5509

To appear in: *Reliability Engineering and System Safety*

Received date: 12 March 2015
Revised date: 16 February 2016
Accepted date: 22 February 2016

Cite this article as: Enrico Zio, Challenges in the vulnerability and risk analysis o critical infrastructures, *Reliability Engineering and System Safety* http://dx.doi.org/10.1016/j.ress.2016.02.009

# Challenges in the vulnerability and risk analysis of critical infrastructures

Enrico Zio

Ecole Centrale Paris and Supelec, Chair on System Science and the Energetic challenge, European Foundation for New energy – Electricite de France (EDF), Grande Voie des Vignes 92295, Chatenay-Malabry Cedex, France; email: enrico.zio@ecp.fr, enrico.zio@supelec.fr

Dipartimento di Energia, Politecnico di Milano, Via Ponzio 34/3 – 20133 Milano, Italy; email: enrico.zio@polimi.it

## ABSTRACT

The objective of this paper is to provide a systematic view on the problem of vulnerability and risk analysis of critical infrastructures. Reflections are made on the inherent complexities of these systems, related challenges are identified and possible ways forward for their analysis and management are indicated. Specifically: the framework of vulnerability and risk analysis is examined in relation to its application for the protection and resilience of critical infrastructures; it is argued that the complexity of these systems is a challenging characteristic, which calls for the integration of different modeling perspectives and new approaches of analysis; examples of are given in relation to the Internet and, particularly, the electric power grid, as representative of critical infrastructures and the associated complexity; the integration of different types of analyses and methods of system modeling is put forward for capturing the inherent structural and dynamic complexities of critical infrastructures and eventually evaluating their vulnerability and risk characteristics, so that decisions on protections and resilience actions can be taken with the required confidence.

**Keywords:** *critical infrastructures, complex systems, systems of systems, electric power grids, smart grids, vulnerability, risk, resilience, uncertainty*

## 1. INTRODUCTION

In this paper, we consider critical infrastructures (CI) like the energy transmission and distribution networks, the telecommunication networks, the transportation systems, the water and gas distribution systems. These are complex systems made by many interacting components assembled by design to provide optimal performance, reliable operation and functional safety (Rouse 2003; Ottino 2004).

CI are designed to function for long periods of time (several tens of years), through maintenance, updating and integration of new technologies. Extensions of capacity are also often required to meet changing and growing service demands. This leads to the need of injecting flexibility and adaptabiliy to the system engineering design, to respond to the ever-changing domains of technology, society, economy, legislation and politics, which determine the profiles of service demand and the corresponding expected performance.

In this scenario of technologically and structurally evolving (and more and more interdependent) CI, understandable concerns are arising on their vulnerability and risk of failure, i.e. on the danger that:

- the allocated system capacities may not be adequate to support the growing demands in scenarios of greater CI integration and market deregulation;
- the safety margins preventively designed may not be sufficient to cope with the expected and, most of all, unexpected stresses arriving onto the systems.

These issues are difficult to analyze as, due to the complexity of CI, emergent behaviors may arise at system level from the collective response of the elementary components, in ways difficult to predict and manage. As a result, large uncertainties exist in the characterization of scenarios of CI failure (Zio and Aven 2011).

On the practical side of the issue, the matter of fact is that CI are witnessing more and more system-level breakdowns, which emerge from small perturbations that cascade to large-scale consequences. Then, it is not surprising that CI protection and resilience have become a national and international priority, which calls for the analysis of CI vulnerability and the evaluation of their resilient properties, for ensuring their protection and resilience (Rigaud and Guarnieri, 2006).

Here, the problem is that the classical methods of system vulnerability and risk analysis cannot capture the (structural and dynamic), complexities of CI; the analysis of these systems cannot be carried out with classical methods of system decomposition and logic modelling. A framework is needed for the integration of methods capable of viewing the problem from different perspectives (topological and functional, static and dynamic), suitable for coping with the high complexity of the system and the related uncertainties (Kröger and Zio 2011).

Several researchers have addressed this problem, introducing new perspectives and methods of analysis and applying them for the protection and resilience of CI (see for example Wang et al 2011 and Ouyang 2014, for some reviews of methods). In this paper, the complexity of CI is presented as a challenging characteristic, which calls for an integrated framework of different types of analyses and methods of vulnerability and risk assessment, for application to CI protection and resilience. The concepts of vulnerability, risk and resilience are discussed in details and analyzed with respect to their characterization in CI, and the challenges therein. Recent new perspectives on these concepts and their applications are also discussed in relation to their applicability for analyzing CI vulnerability and risk in view of decision making for protection and resilience.

The paper is organized as follows:

- in Section 2, we introduce the concept of critical infrastructures and specify them as engineered complex systems;
- in Section 3, vulnerability and risk concepts are introduced and discussed with reference to critical infrastructures design and operation. Three statements are proposed to advocate the need for extended modeling as a way to understanding system behavior and capturing the related risk and vulnerability factors;
- in Section 4, some perspectives are offered on approaches for looking into the complexity characteristics of CI, for analyzing their vulnerability and risk.

## 2. CRITICAL INFRASTRUCTURES

Infrastructures are large scale, man-made systems that function interdependently to produce and distribute essential goods (such as energy, water and data) and services (such as transportation, banking and health care). An infrastructure is termed critical if its incapacity or destruction has a significant impact on health, safety, security, economics and social well-being (Council Directive 2008/114/EC). A failure in such an infrastructure, or the loss of its service, can be damaging to a single society and its economy, while it could also cascade across boundaries causing failures in multiple infrastructures with potential catastrophic consequences (Carreras 2004, Bouchon 2006).

On these premises, this paper offers some reflections on the challenges that characterize the vulnerability and risk analysis of CI, leading to the argument that there is a

need for new methods and approaches, and a systematic framework for their integration. The structural and dynamic complexities of CI are analyzed, and different modeling perspectives are identified for describing them. Although, inevitably, abundant reference is made to previous works of literature, the paper has no intention to provide a state of the art review on the characteristics of complexity (like in Rouse 2003, Boccaletti et al. 2006, Bouchon 2006, Barthelemy 2011) or on the methods and models for CI analysis (like in Wang et al. 2011, Ouyang 2014).

### *2.1 Characteristics of complexity of critical infrastructures*

CI are various by nature, e.g., physical-engineered, cybernetic or organizational, and by environment (geographical, natural) and operational context (political/legal/institutional, economic, etc.). Examples are those providing services of:

- energy (including generation, transmission, distribution and storage, in regard with electricity, oil and gas supply);
- transportation (including rail, roads, aviation and waterways);
- information and telecommunication (including information systems, industrial control systems (SCADA), Internet, fixed and mobile communications and broadcasting).

CI are complex systems made by many components interacting in a network structure. Most often, the components are physically and functionally heterogeneous, and organized in a hierarchy of subsystems that contributes to the system function. This leads to both structural and dynamic complexity.

#### *2.1.1 Structural complexity*

Structural complexity derives from:

- Heterogeneity of components across different technological domains due to increased integration among systems (Gheorghe and Schlapfer 2006).
- Scale and dimensionality of connectivity through a large number of components (nodes), highly interconnected by (Rinaldi et al. 2001; Bloomfield 2009; Popov 2009; Luiijf 2009; Chou and Tseng 2010; D'Agostino et al. 2010; Fioriti et al. 2010; Barthélemy 2011):
    - dependences, i.e. unidirectional relationships: a component depends on another through a link, but this other one does not depend on the former through the same link, and
    - interdependences, i.e. bidirectional relationships: a component depends on another through some links, and this latter component likewise depends on the former component through the same and /or other links.

The relevance of the issue of interdependency among critical infrastructures is demonstrated, for example, by the fact that it has been prioritized by the European Reference Network for Critical Infrastructure Protection (ERNCIP) and a Thematic Area has been launched to address it systematically, and by the several research works (Brown et al. 2004; Svendsen and Wolthusen 2007; Bobbio et al. 2010; Johansson and Hassel 2010; Utne et al. 2011) and European Union projects on the subject (e.g., Klein et al. 2011).

A common example of structural complexity is that of the Internet. Initiated in 1969 in the United States as a military project (Ryan 2010), the Internet has become pervasive in our lives: it penetrates our offices, houses and public spaces, supported by the increasing use of personal computing devices. Today, the Internet is a global platform for commercial and social interactions, used regularly by 20% of the world's population already in 2008 (OECD 2008). Using widespread and standard engineering services with easy access to information, communication and data sharing, the Internet increases the efficiency of economic activities and considerably increases social interactions (OECD 2008). Its evolution continuously demands creation of new policy frameworks, to "encourage innovation, growth and change,

and develop appropriate governance that does not stifle creativity or affects the openness of the Internet" (OECD 2008). As a backbone and enabler of convergence across multiple fields (engineering, social, economic, finance and policies), the Internet is a good example of a structurally complex engineered system, expanding, evolving and updating with new technology.

Heterogeneity refers to the differences in the elements, their interconnections and roles within the system structure, often with high-connected core elements and low-connected periphery nodes. For example, heterogeneity is strong in current electric power grids, with architectures in the form of hierarchical trees where production facilities are connected by centralized high-voltage transmission systems, to transformation substations linked, in their turn, to final consumers by distribution branches. Notably, Smart grid systems aim at evolving towards more decentralized architectures, with a more homogeneous distribution of heterogeneous production sources of different nature and size, including renewable energies. These will need to penetrate the network at all levels, homogeneously. The arising grid pattern forms a sort of neural or vascular system, manifesting in some conditions structured into self-similarities and adding a layer of communication among the system elements, based on the integration of new, enabling technology (Agnati et al. 2009).

For the concerns of vulnerability and risk, the strong heterogeneity of the elements and the large number of connections in current electricity grids (with an increasing number of virtual connections, while moving towards Smart grids) translates into high sensitivity to direct attacks (Crucitti et al. 2003; Zio 2007a). In principle, this high vulnerability to direct, targeted attacks can be limited by allocating supplemental connections and elements, for a more homogeneously distributed structure, as the tolerance of homogeneous networks is similar for random failures or direct attacks to nodes and connections, independently of the network size (Rosas-Casals et al. 2007).

#### *2.1.2 Dynamic complexity*

Dynamic complexity manifests through the emergence of (even unexpected) system behavior in response to local changes in the environmental and operational conditions of its components.

Self-organization is a specific dynamic feature of a complex system, which amounts to the capability of re-organizing its isolated elements and subsystems into coherent patterns without intervention from external influences or a central authority (Granic and Lamey 2000). Emergence is another dynamic property of complex systems, which appears only at a macro level manifesting itself by the arising of novel and coherent structures, patterns and behavioral properties (Goldstein 1999; Seth 2008). In the case of the Internet, social bookmarking or tagging leads to an emergent effect in which information resources are re-organized according to users priorities. Electric power grids have also shown emergent behavior in the past, where local failures have evolved into unexpected cascade failure patterns with transnational, cross-industry effects. In this view, also Smart grids are expected to present emergent behaviors, depending on the extent and type of the active involvement of users in the energy management process. For example, a situation in which a large amount of information is exchanged within technologies at a period of high electricity demand can lead to a vulnerable condition of the system, similar to Internet networks and information traffic congestion (Chen et al. 2004). This emergent behavior could be driven by small changes in users behavior and result in grid dysfunction.

However, emergence can also offer opportunities to find resilient solutions in the recombination of evolved structures and processes, renewal of system components and new connection trajectories to satisfy demands (Rosas-Casals 2009). For Smart grids, one could imagine using the bookmarking mechanism to make social participation more visible and

involve people in energy infrastructure design and operation by communication of their major expectations and needs, as well as to take into account their feedback during system updates. In this view, an emergence process driven in reasonable proportion between social participation and central authority can make Smart grids more resilient to environmental changes without losing the functional capacity.

Adaptive learning is a different dynamic property of complex systems, which relates to the ability of adjusting the system structure and behavior to respond to external pressures, by using long-term memory experience feedback to anticipate future unfavorable changes in system functioning (NECSI 2005). In complex engineered CIs like the Internet, the adaptive learning process partly relies on the ability of self-organization driven by local changes. Such process can play a fundamental role on the system vulnerability and on the resilience performance (Dalziell and McManus 2004).

In the electric power grid, adaptive learning is a challenge-response property, which results from the trade-off between consumer involvement and control by the central authority in the energy management process:

- on one side, intense consumer involvement can initiate chaotic behavior in the electrical system;
- on the opposite side, strong control by the central authority renders the system rigid, missing opportunities for service efficiency and for exercising system resilience and adaptation capacity.

This raises the question on how much adaptive learning can be expected or should be imparted in the future Smart grids, and on the related feedback mechanisms.

Complex systems are also subject to evolution and growth mechanisms. When the external pressures applied to a system exceed 'critical values' beyond which responding by adaptive learning mechanisms is not sufficient, the system is forced to evolve. In the absence of a central authority governing system changes, the evolutionary process resembles natural selection in biological systems, resulting in the consequent disappearance of elements associated with low adaptive fitness. The Internet, for example, is the product of the evolution of its constitutive software and hardware technologies, information and communication services and applications, and also faces the creation of new ways of use, such as e-commerce. Unlike biological systems, complex engineered systems are exposed also to stresses coming from the growth of user portfolios.

In the example of electric power grids, these systems, restricted by technical constraints and transmission capacity, extend by preferential attachment, whereby highly connected nodes attract new links. This is a typical mechanism of growth of complex networks (Barabasi et al. 2000; Boccaletti et al. 2006). The result of this particular mechanism of growth is that it reinforces the 'scale-free' (inhomogeneous) nature of electrical systems and, as a consequence, makes them vulnerable to direct attacks and propagation of cascading failures. This means that the electricity system growth must be carefully monitored in order to anticipate possible critical decision points at which infrastructure development must be steered in a preferred direction. In this sense, the resilient mechanism for electricity infrastructure growth is likely to be based on the repulsion process between the hubs at all length scales, when the hubs prefer to grow by connections to less-connected nodes (Song et al. 2006). On the other hand, user involvement in the energy management process may cause drastic shifts in the system dynamic evolution, leading to unexpected events and system vulnerabilities.

#### *2.1.3 An example of CI as complex system: the electric power grid*

The electric power grid serves as a good example of CI as complex system (Mei et al., 2011). It is made of a large number of interconnected elements (wires and machines) that link

the electricity generators to the customers, for satisfaction of their needs. Structural complexity in this system comes from:

- heterogeneity of the components across different technological domains (electrical components, information technology components, etc.) due to the increased integration of the electrical power grid with other critical infrastructures, e.g. driven by the pervasive use of computer-based communication and control systems, which is beneficial in many respects but, on the other hand, introduces additional vulnerabilities due to the increased interdependence, which can lead to surprising behaviors in response to perturbations (Dueñas-Osorio et al. 2007; Casalicchio et al. 2011);
- scale of connectivity (interactions among several components) and dimensionality (large number of nodes highly interconnected also with other neighboring power systems, distributed energy sources, storage devices and electrical vehicles, etc.) (Ruzzante et al. 2010).

From the point of view of dynamic complexity, characteristics of dynamic complexity, such as adaptation, self-organization and emergent behavior, are seen originating from:

- the distributed power generation from renewable energy sources (e.g. solar and wind), increasingly connected to the existing network;
- the extent of interconnectedness, the number and variety of power sources and generators, of controls and loads, that make electric power grids among the most complex engineered systems.

These dynamic system properties offer opportunities for extended, improved and more reliable service but also pose vulnerabilities, mostly due to unforeseen and hidden behaviors arising from the integration (Ottino 2004).

With the fast-pace re-conceptualization of the electric power grid for the integration of large shares of electricity produced by harvesting solar and wind energies at the most suitable sites (e.g. desert solar and offshore wind farms), a "smarter" system is sought with:

- decentralized generation;
- smart metering;
- new devices for increased controllability;
- self-healing etc.

Then, extending the considerations on the electric power grids from their current configuration to the foreseen future “smart” development, one must consider the structural and technological evolution from their original development as loosely interconnected networks of local systems to distributed electric power grids, extended on large scales, across regional and national boundaries. As a result, electric power grids are considered among the most important European Critical Infrastructures (ECI) in the European Programme for Critical Infrastructure Protection (EPCIP).

Smart grids are expected to provide a flexible, adaptive infrastructure, operated proactively through three foundational layers:

- power and energy;
- communication;
- IT/computing.

What emerges is the typical construct of a system of systems (SoS), in which the systems forming the collaborative set of the SoS fulfill their purposes and are managed for their own purposes and the purposes of the whole SoS (Eusgeld et al. 2011; Zio and Sansavini 2011). This may lead to new and unexpected hazards and vulnerabilities acros systems. For example, the growing role of ICT in the energy infrastructure requires that cyber-security be considered from the outset in the development of smart grids (Zio and Sansavini 2013). Indeed, recent incidents have shown that ICT systems can be vulnerable to cyber-attacks and that such

attacks can lead to disruption of physical systems and networks (Ten et al. 2008; Amin et al. 2013; Peng et al., 2013; Netkachov et al. 2014a and b).

On top of the technological challenges related to the evolution of such systems (e.g. creation of distribution management through using distributed intelligence and sensing, integration of renewable resources, etc.), a number of other issues are daunting the electric power grid systems and increasing the stress of the environments in which these are to be operated:

- the deregulated energy market, which has resulted in the systems being operated closer to their capacity and limits, i.e., with reduced safety margins, and consequently in the need for new and balanced business strategies;
- the prospected demand for electricity in the next 25-50 years, which results in the need to technically respond by increased capacity and efficiency;
- the sensed increase in the exposure to malevolent attacks that are no longer only hypothetical, which calls for effective protection to a different type of hazard/threat, much more difficult to predict than random failures.

In these scenarios of increased stress onto the electric power grids, concerns are naturally arising on the vulnerabilities and risks associated to their future development and operation.

## 3. VULNERABILITY AND RISK ANALYSIS

CI are exposed to many types of hazards, such as natural hazards, component aging and failure, sharp load demand increase, climatic changes, intentional attacks. For this reason, Critical Infrastructure Protection (CIP) has gained great importance in all nations, with particular focus being placed traditionally on physical protection and asset hardening (Bush 2002; Bush 2003; Clinton 1998; Lewis 2006). To protect CI, it requires modeling their component fragilities under different hazards and, then, analyzing their system-level risk and vulnerability.

In recent years, lessons learned from some catastrophic accidents have extended the focus on the ability of CI to withstand, adapt to and rapidly recover from the effects of a disruptive event and, thus, the concept of resilience (Moteff 2012; Obama 2013; Pursiainen 2009). The outcomes of the 2005 World Conference on Disaster Reduction (WCDR) confirmed the significance of the entrance of the term resilience into disaster discourse and gave birth to a new culture of disaster response (Cimellaro et al. 2010). As a result, systems should not only be reliable but also able to recover from disruptions (Zio 2009). Government policy has also evolved to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation after the occurrence of disruptive events (Moteff 2012). As a consequence, resilience is nowadays considered a fundamental attribute for CI that should be guaranteed by design, operation and management.

### *3.1 The concept of resilience*

Resilience comes from the Latin word “resilio” that literary means “to leap back” and denotes a system attribute characterized by the ability to recover from challenges or disruptive events. The Merriam-Webster dictionary defines resilience as “the ability to recover from or adjust easily to misfortune or change”. The concept of resilience used in practice varies by discipline and application (Najjar and Gaudiot 1990; Henry and Ramirez-Marquez 2012; Ouyang et al. 2012). Resilience can be understood as:

- “the ability of the system to reduce the chances of shock, to absorb a shock if it occurs and to recover quickly after a shock (re-establish normal performance)” and it is characterized by (Bruneau et al. 2003):
  - four properties, i.e.:

        - robustness;
        - redundancy;
        - resourcefulness;
        - rapidity and
    - four interrelated dimensions, i.e.:
        - technical;
        - organizational;
        - social;
        - economic;

- a new paradigm for safety engineering, which proactively integrates the accident preventive tasks of anticipation (imagining what to expect) and monitoring (knowing what to look for), the in-accident tasks of responding (knowing what to do and being capable of doing it) and learning (knowing what has happened), the mitigative tasks of absorbing (damping the negative impact of the adverse effect) and the recovery tasks of adaptation (making intentional adjustment to come through a disruption), restoration (returning to the normal state) (Hollnagel et al. 2006);
- the capacity of a system of surviving to aggressions and shocks by changing its non-essential attributes and rebuilding itself (Manyena 2006);
- "the capacity of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident" (U.S. Department of Homeland Security 2009);
- the "ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks" (Haimes 2009);
- related to the concept of robustness, with the key difference being the initiating event: robustness (and vulnerability) relates to a specific initiating event, whereas resilience relates to any initiating event; in other words, resilience can be interpreted as "the uncertainty about and severity of the consequences of the activity given the occurrence of any type of initiating event (Aven 2011);
- a structural property, i.e., as the ability to resist to internal drifts and cascading failures, and recover back to the initial operation state (Alessandri and Filippini 2013).

A recent definition of resilience is given in the Society for Risk Analysis (SRA) glossary , as the ability of the system to sustain or restore its basic functionality following a risk source or an event (even unknown), the sustainment of system operation and associated uncertainties, following a risk source or an event (even unknown) (SRA 2015).

Various models, methods and frameworks for analyzing and measuring resilience have been proposed in the literature (Carpenter et al. 2001; Fiksel 2003; Wreathall 2006; Jackson 2007, 2009; Peters et al. 2008; Madni and Jackson 2009), with focus on diverse fields of application such as seismic engineering and structural systems (Cimellaro et al., 2006; 2010; Poljanfisek et al. 2012; Duenas-Osorio and Kwasinski 2012), ecological systems (Holling 1973), economics and financial systems (Starr et al. 2003; Rose et al. 2009; Amini et al. 2013; Baroud et al. 2015), service systems (Todini 2000; Rosenkrantz et al. 2009); telecommunication systems (Omer et al. 2009), urban infrastructures (Jin et al. 2014; Oyuang and Duenas-Osorio 2012; Attoh-Okine et al. 2009), disaster analysis for avoidance and recovery (Bonanno et al. 2007; Tierney and Bruneau 2007; Zobel 2011)

In this paper, vulnerability and risk analysis are considered for their central role in support to decision making for proper CI protection and for guaranteeing CI resilience.

While resilience can be characterized by many system features and attributes, recovery is a vital element of strategies to improve resilience. System recovery and its role in infrastructure system resilience have attracted much previous attention. Some studies have modelled the post-disaster restoration of various infrastructure systems in an effort to estimate the expected restoration time (Ferrario and Zio 2014; Liu et al. 2007; Shinozuka et al. 2004), and several others have compared the performance of different restoration strategies (Buzna et al. 2007), (Çağnan et al. 2006). More works have been done to tackle the problem of post-disaster restoration strategy planning and optimization, for the purpose of restoring system service in a timely and efficient manner. Considering multiple types of systems simultaneously, Kozin and Zhou (Kozin and Zhou 1990) developed a Markov process to describe the process of infrastructure system recovery; then, they used dynamic programming to estimate the repair resources required for each time step and for each system, so as to maximize the expected economic return from system functioning. Noda (Noda 1993) used a neural network to minimize the likelihood of post-earthquake functional loss for a telephone system. Bryson et al. (Bryson et al. 2002) applied a mixed integer programming approach for selecting a set of recovery subplans giving the greatest benefit to business operation. Casari and Wilkie (Casari and Wilkie 2005) discussed restoration when multiple infrastructures, operated by different firms, are involved. Lee et al. (Lee et al. 2007) focused on a case of network restoration that involves selecting the location of temporary arcs (e.g., shunts) needed to completely reestablish network services over a set of interdependent networks. A mixed-integer optimization model was proposed to minimize the operating costs involved in temporary emergency restoration. Xu et al. ( Xu et al. 2007) applied a genetic algorithm to a problem associated with restoring power after an earthquake. The objective of this problem was the minimization of the average time that each customer stays without power (therefore, no prioritization is given to demand to critical points within the infrastructure). Finally, Matisziw et al. (Matisziw et al. 2010) propose an integer programming model to restore networks where the connectivity between pairs of nodes is the driving performance metric associated with the network.

The studies cited above involving the optimization of post-disaster CI restoration apply a variety of modelling approaches and focus on different aspects of the restoration strategy (e.g. the repair order of damaged components, where and how to allocate repair resources, and so on).

For ensuring adequate protection and resilience of CI, vulnerability and risk must be analyzed and assessed in order to prepare to address them by design, operation and management. According to (Zhang and Peeta 2011), the concept of risk is fairly mature whereas that of vulnerability is still evolving. In the following we briefly recall these concepts, as they relate to the context of the present work.

*3.2 The concept of risk*

Risk analysis as a formalized subject has existed for almost four decades, and has reached a wide range of applications with the purpose of revealing and identifying potential failure modes and hazards in our systems and operations, so that they may be corrected before they manifest.

In general terms, and in line with SRA (2015), risk describes the (future) consequences potentially arising from the operation of our systems and from our activities, and the associated uncertainty. Consequences are usually seen in negative, undesirable terms with respect to the planned objectives. Accident scenarios are a relevant part of risk, in that they are those combinations of events potentially leading to the undesired consequences.

The recent definition of risk in the SRA glossary, refers to the consequences of a future activity, e.g. the operation of a CI, where the consequences are with respect to

something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.) and the focus is normally on negative, undesirable consequences. There is always at least one outcome that is considered as negative or undesirable (SRA 2015).

To support decision making for CI protection and resilience, risk needs to be described and possibly measured: the consequences, in terms of losses, damages, injuries etc., and the uncertainties therein, in terms, for example, of probabilities (frequencies). For CI, the term risk may include the frequency of loss of service with its resulting consequences for the people concerned by the service.

In recent years, new perspectives on risk have been proposed, which add the description and/or measurement of the strength of the knowledge that the risk description is based on (Aven and Krohn 2014). For example, the values of probability in two different situations could be the same, but their assignment may be based on quite different knowledge, data and information, and eventually assumptions, which leave quite different room for surprises of unforeseen events and related consequences. The strength of the knowledge supporting the risk assessment is, thus, an element of great relevance for using the risk outcomes in decision making; how to measure it is an open challenge. Besides this professional side of risk, there is a non-technical dimension accounting for aspects of societal and psychological risk experience and perception, which are subject to changes and contextual in nature; knowing and understanding this is fundamental for effective decision making.

*3.3 The concept of vulnerability*

In the SRA glossary, vulnerability of a system is referred to the risk and the degree that the system can be affected by a risk source or agent (SRA 2015). The concept of vulnerability seen as a global system property embeds three other concepts (Kröger and Zio 2011; Wang et al. 2011):

- degree of losses and damages due to the impact of hazards;
- degree of exposure to hazards, i.e.,
  - likelihood of being exposed to hazards of a certain degree
  - susceptibility to suffering losses and damages (this depends on the system robustness, which is the antonym of vulnerability);
- degree of resilience.

In the context of the present paper, vulnerability is:

- seen as a global technical property and
- interpreted as a flaw or weakness (inherent characteristic, including resilience) in the design, implementation, operation and/or management of an infrastructure system, or its elements, that
  - renders it susceptible to destruction or incapacitation when exposed to a hazard or threat, or
  - reduces its capacity to resume new stable conditions.

For example, the vulnerability of the electric power system might be specified in terms of:

- changes of network characteristics following attacks on nodes and the scale (e.g., number of nodes/lines lost) or the duration of the associated loss or
- the frequency of major blackouts (number per year) and the associated severity, measured either in power lost or energy unserved (MW or MWh).

Finally, the spatial scale of CI introduces an additional important aspect to consider in the vulnerability analysis: that of the global impact of spatially local hazards (Wilkinson et al. 2012). Indeed, whereas the spatially local hazards threaten relatively small-scale systems

whose components are located in the hazard influence area, these relatively small-scale systems are usually a part of much larger or national scale systems, and then the impact of localized natural hazards can extend to the large-scale systems they are embedded in. Examples are the vulnerability analysis in (Hong et al. 2015) concerning the Chinese railway system under flood hazards, where the flood hazards only occur at some provinces and their induced component failures are local relative to the system scale, and the seismic vulnerability analysis of the European gas and electricity networks, where the seismic hazards only occur at earthquake-prone regions (Poljansek et al. 2012). Recently, some works on localized failures have been made by scholars in the field of complex networks. Shao et al. (2015) studied network percolation under localized failures, which were modeled by removing a randomly selected node, its nearest neighbors, next nearest neighbors and so on to reach some failure intensity, and should be strictly called as topologically localized failures. Berezin et al. (2015) modeled localized failures in a diluted square lattice by removing all nodes within a certain Euclidean distance from a random location, which is only a simple form of spatially localized failures. Also, these purely topology-based studies usually produce the vulnerability results with weak correlations to those results obtained when the infrastructure system flow properties are considered (Cavalieri and Franchin 2014; Ouyang 2013; Ouyang et al. 2014).

*3.4 Vulnerability and risk analysis of critical infrastructures*

In a system perspective, the goals of vulnerability and risk analysis for informing protection and resilience decision making are (Kröger and Zio 2011):

1. given a system and its planned objectives (positive), identify the set of events and event sequences that can cause damages and loss effects with respect to the planned objectives (negative);
2. identify the relevant set of "initiating events" and evaluate their cascading impact on a subset of elements, or the system as a whole;
3. given a system and its planned objectives, identify the set of events or respective event sequences that would cause this effect. For any real-world situation, the set of possible event sequences can be very large. In practice, the challenges are of:
    a. completeness of the set, and
    b. management of its dimension.

    The analysis must be organized and structured so that:
    - the important event sequences are explicitly identified, and
    - the less important ones are grouped into a finite number of categories.
4. given the set of initiating events, event sequences and observed outcomes, determine and elaborate on:
    a. (inter-)dependencies (within the system and among systems), and
    b. the coupling of different orders.

The ultimate goal for the purposes of CI protection and ensuring resilience is to identify obvious and, most importantly, hidden vulnerabilities in infrastructure systems, to be able to act for managing and reducing them before they manifest as failures (Figure 1). The achievement of these goals relies on the analysis of the system, its parts and their interactions within the system, through dependencies and interdependencies; the analysis must:

- account for the environment which the system lives and operates in, and
- start from the objectives the system is expected to achieve, to look for variations and deviations (Kröger 2008).

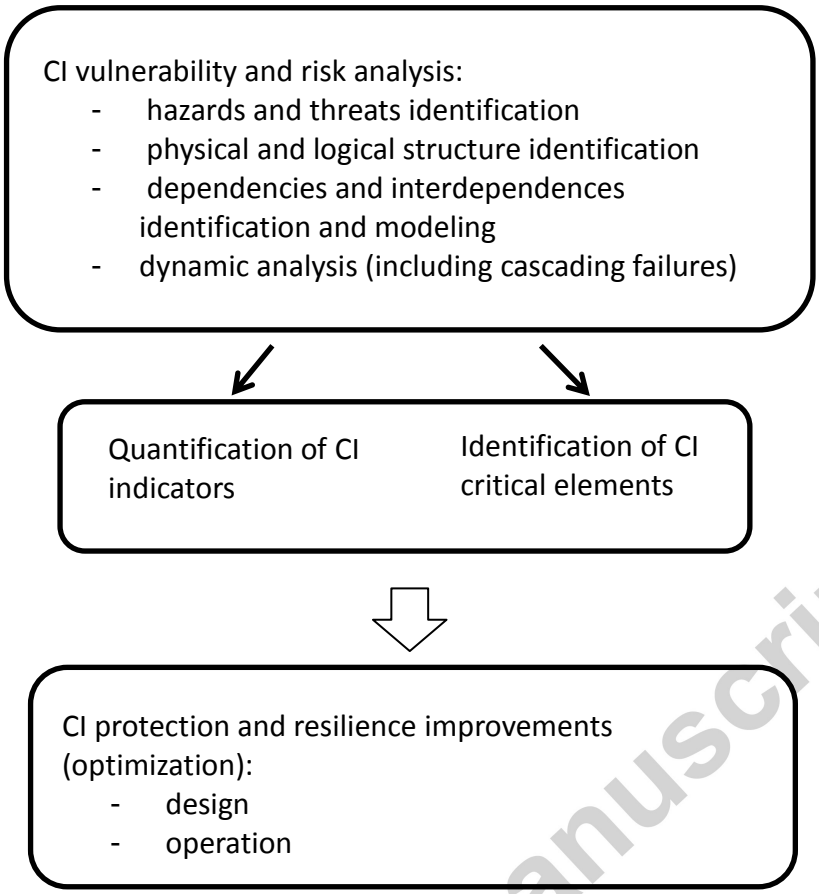



*Figure 1: Schematic structure of CI vulnerability and risk analysis*



*Statement 1: For the Vulnerability and Risk Analysis of Critical Infrastructures, we must model them to know their behavior*

When addressing the vulnerability and risk analysis of a CI with the goals mentioned above, one faces old problems which develop into new challenges due to the complexity of the system, with respect to (Zio 2009):

- the representation and modeling of the system;
- the quantification of the system model;
- the representation, propagation and quantification of the uncertainty in system response.

Given the nature and role of the CI, the modeling must expand to consider:

- physical attributes {structure, dynamics, dependencies and interdependencies …};
- operation and management attributes {communication, control, human and organizational factors, logistics …};
- performance and safety attributes {reliability, availability, maintainability, risk, vulnerability …};
- economic attributes {life-cycle costs, costs-benefits, market drivers …};
- social attributes {supply-demand, active players …};
- environmental attributes {pollution, sustainability …}.

*3.5 Framework for modeling and analysis of critical infrastructures*

Modeling and analysis by reductionist methods are likely to fail to capture the behavior of the complex systems that make up the CI, and new approaches are needed that look into these systems from a holistic viewpoint to provide reliable predictions of their behavior for their safe control (Kröger and Zio 2011). Furthermore, large uncertainties exist in the characterization of the failure behavior of the elements of a complex system, of their interconnections and interactions (Zio and Aven 2011).

*Statement 2: To model the (engineered) complex systems (of systems) which make our CI, there is not one single modeling approach that "captures it all"*

The analysis of CIs cannot be carried out only with classical methods of system decomposition and logic analysis; a framework is needed to integrate a number of methods capable of viewing the complexity problem from different perspectives (topological and functional, static and dynamic, Figure 2), under the existing uncertainties (Ouyang et al. 2009; Reed et al. 2009; Ouyang 2014):

- structural/topological methods based on system analysis, graph theory, statistical physics, etc.; these methods are capable of describing the connectivity of a complex system and analyzing its effects on the system functionality, on the cascade propagation of a failure and on its recovery (resilience), as well as identifying the elements of the system which must be most robustly controlled because of their central role in the system connectivity (Newman et al. 2005; Lee et al. 2007; Zio and Sansavini 2011; Fang and Zio 2013; Alipour et al. 2014);
- logical methods based on system analysis, hierarchical logic trees, etc.; these methods are capable of capturing the logic of the functioning/dysfunctioning of a complex system, and of identifying the combinations of failures of elements (hardware, software and human) which lead to the loss of the system function (Apostolakis and Lemon 2005; Bobbio et al. 2010);
- phenomenological/functional methods, based on transfer functions, state dynamic modeling, input-output modeling and control theory, agent-based modeling etc.; these methods are capable of capturing the dynamics of interrelated operation between elements (hardware, software and human) of a complex system and with the environment, from which the dynamic operation of the system itself emerges (Trucco et al. 2012; Alessandri and Filippini 2013);
- flow methods, based on detailed, mechanistic models (and computer codes) of the processes occurring in the system; these methods are capable of describing the physics of system operation, its monitoring and control (Sansavini et al. 2014).

The integration of these methods is expected to enable capturing the different relevant aspects of the complex CI. Methods of multi-hazard analysis and risk aggregation, such as those under development in the nuclear risk field, may provide valuable guidelines.

For electric power grids, comparisons between structural/topological and power flow methods have been made. Some studies (Baldick et al. 2008; LaRocca et al. 2013; Sun and Han 2005; Correa et al. 2013) have provided qualitative comparisons between complex network theory models and power flow models, identifying similarities and differences, and evaluating advantages and disadvantages. Also, by extensive comparative simulation, (Cupac et al. 2013) has shown that a network-centric model exhibits ensemble properties which are consistent with the more realistic optimal power flow model. Most recently, (Matisziw et al. 2010) conclude on the appropriateness of graph theory techniques for the assessment of electric network vulnerability by comparison to physical power flow models. This is confirmed in (Fang et al. 2014), where the problem of searching for the most favorable pattern of link capacities allocation that makes a power transmission network resilient to cascading failures

with limited investment costs is formulated within a combinatorial multi-objective optimization framework and tackled by evolutionary algorithms. Two different models of increasing complexity are used to simulate cascading failures and to quantify resilience: a complex network model, and a more detailed and computationally demanding power flow model. Both models are tested and compared on a case study involving the 400kV French power transmission network. The results show that the optimal solutions obtained using the two different models exhibit consistent characteristics in terms of phase transitions in the Pareto fronts and link capacity allocation patterns.

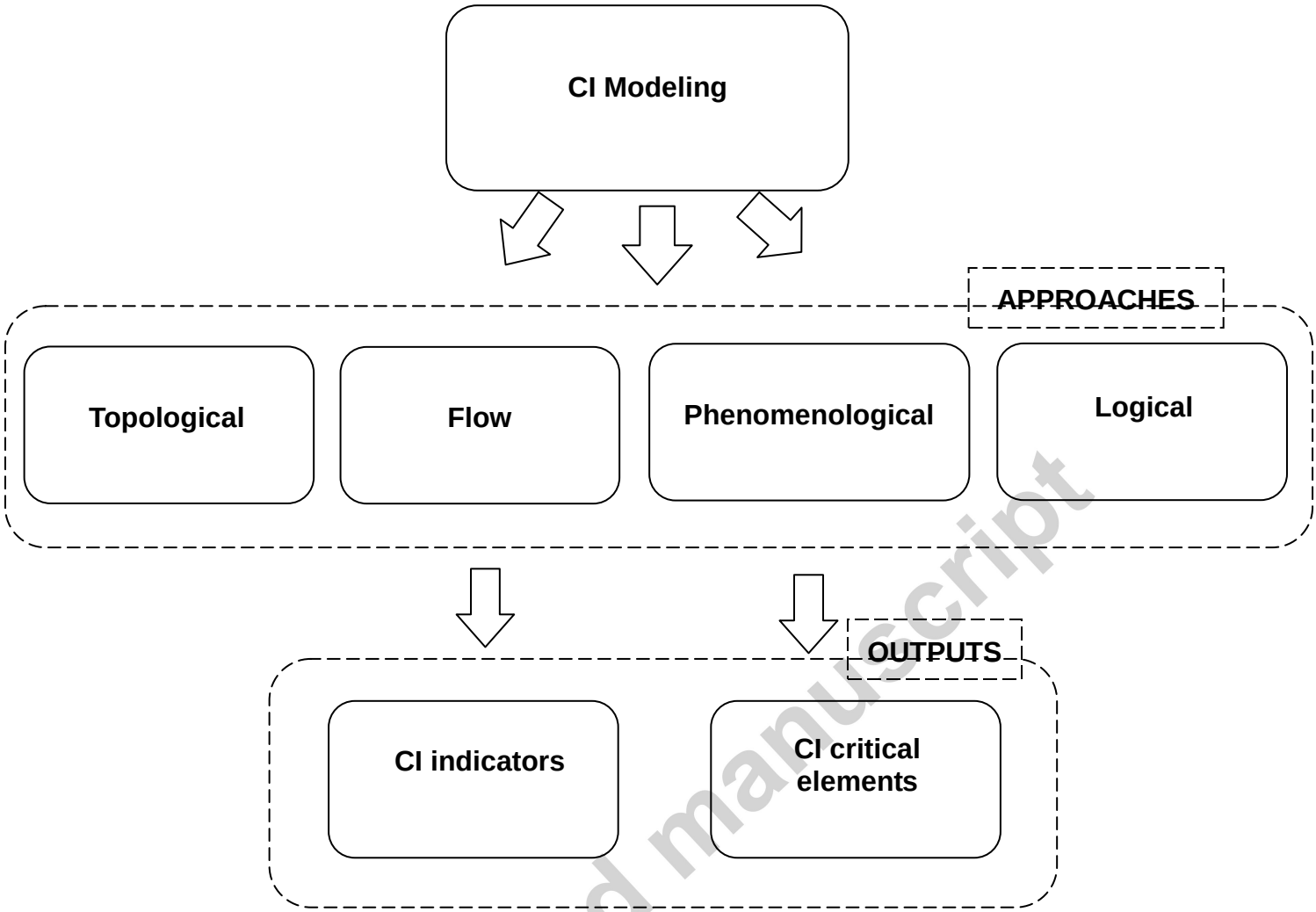



*Figure 2: CI modeling and analysis approaches*

*3.6 Extended modeling and analysis of critical infrastructures*

*Statement 3: The framework of vulnerability and risk analysis must be extended beyond the causal, event-chain description of accidents and the probabilistic quantification of their likelihood of occurrence*

On one side, the above methods must be expanded and complemented with methods for probing surprising events which can potentially emerge from the CI complexity, once triggered by an initiating event. Many types of traditional risk assessment methods address the issue of what can happen, for example HAZOP, HazId, fault tree and event tree analysis (Zio 2007b). Using these methods, hazardous events and scenarios are identified.

Another revealing framework capable of explaining how the fundamental interrelationships among the functions in a complex system may lead to adverse outcomes is the Functional Resonance Accident Model (FRAM), which provides a way to examine individual system functions and determine their interrelationships (Hollnagel 2004 and 2012). FRAM is a method that allows modelling the functions of a complex socio-technical system, which are needed for successful everyday performance. On this basis, it is possible to show how some functions are coupled and how the variability in everyday performance may sometimes lead to unexpected outcomes. Being a method rather than a model, FRAM makes no assumptions about how the system under investigation is structured or organized, nor about possible causes and cause-effect relations. Instead of searching for failures and malfunctions, FRAM looks at how functions become coupled and how everyday performance variability may resonate into unexpected outcomes. In this view, failure is seen as due to the inability to anticipate, timely recognise and react to risks and critical situations that arise due to multiple malfunctions that unexpectedly combine in resonance, which makes these situations developing in a dynamic fashion rather than as a simple combination of causal links. Hence, it is the identification of the system functions, the study of their possible variability and potential for resonance, and of the (damping) protective and resilience barriers installed in the system that can offer a way through for understanding accident progression and adequately adding protection and resilience into the system.

With an increased focus on surprises and black swan types of events and scenarios, there is a need to complement these methods with others offering the necessary, different perspectives. Some ideas are developing in this direction (Aven 2013), e.g. the so-called anticipatory failure determination (AFD) method based on I-TRIZ, a form of the Theory of Inventive Problem Solving, which enables viewing the identification of failure scenarios fundamentally as a creative act carried out systematically, exhaustively, and with diligence (Kaplan et al. 1999). Traditional failure analysis addresses the questions:

- "How did this failure happen?"
- "How can this failure happen?".

The AFD and TRIZ go one step further and pose the question:

- "If I wanted to create this particular failure, how could I do it?"

The power of the technique comes from the process of deliberately "inventing" failure events and scenarios.

A different perspective is also offered by the advocated shift in paradigm from the reactive safety management focus on adverse outcomes, looking at the manifestations of the absence of safety for responding to what goes wrong or what is identified as a risk, to a proactive form of safety management whereby focus is on what goes right rather than on what goes wrong, for ensuring that everything goes right under the varying operating conditions which the system experiences (Hollnagel 2014).

These methods can be supported by different types of analysis frameworks. One of particular interest for CI analysis might be Actor Network Theory (ANT), which seeks to understand the dynamics of a complex system by following its elements/actors – it asks how the world looks through the eyes of the actor doing the function (Latour 2005; Masys 2012).

On the other side, the integration must be systematic and structured. In this respect, the paradigms of control theory, with its underpinning concepts of observability and controllability, seem promising with respect to a view of accidents as deviations/variations resulting from a lack of appropriate constraints (control actions) on system design, or from inadequate enforcement of constraints (control actions) in system operation (Leveson 2004; Levenson 2011; Cowlagi and Saleh 2013; Liu et al. 2013). This can be a way to implement the concepts of predictability and unpredictability, with respect to "common-cause variations" (predictable in view of historical experience and knowledge) and "special-cause variations" (unpredictable because beyond experience and knowledge) (Deming 2000; Bergman 2009).

Advanced simulation techniques for scenario analysis can add a valuable input to this, tailored to the "creation" of scenarios of potential future conditions and events. In this case, the aim of simulation is neither of completeness nor of accuracy of estimation, as in traditional risk analysis, but rather of enabling the generation of "surprising" scenarios that may provide useful insights about what could happen. Methods of "adjoint" simulation may be of particular interest for generating deductive (anticipatory, backwards) scenarios, where we start from a future imagined event/state of the total system and question what is needed for this to occur. Interpretation of these scenarios by system thinking, to see the holes and interconnections, is critical if one is to identify black swans (Aven 2013; Aven and Krohn 2014). On the contrary, using for example an event tree to reveal scenarios has strong limitations, as the analysis is based on a linear inductive thinking on the chain of events resulting from an accident initiator (Kaplan et al. 1999).

Furthermore, the human factor should not be underestimated in the vulnerability and risk analysis of critical infrastructures, especially as far as cascading effects are concerned. Indeed, first, the human behaviour may be the very cause of the initiation of a cascading failure or some major factor in the chain of events along the accident, either directly or indirectly, as seen in practice (e.g. the nuclear accidents of Three Mile Island and Chernobyl). Second, even if not the very cause of an accident human behaviour may aggravate or diminish the impact of its consequences. In this context, the early methods of Human Reliability Analysis (HRA), the so-called 'first generation' ones like Technique for Human Error Rate Prediction (THERP) (Swain and Guttman 1983), Accident Sequence Evaluation Program (ASEP) (Swain 1987) and Human Cognition Reliability (HCR) (Hannaman et al. 1984; Hannaman et al. 1985), are built around the pivotal concept of human error: because of the inherent deficiencies of humans, they naturally fail to perform tasks just like mechanical, electrical, structural components do. In this view, it makes sense to assign a probability of failure of a human operator in performing a task of given characteristics. Thus, the quantity Human Error Probability (HEP) can be defined with respect to a given task and appropriately modified in consideration of the actual environmental conditions under which it is performed. The factors representing the effects of the environment on the human performance of a task are called Performance Shaping Factors (PSFs) or Performance Influencing Factors (PIFs). The point of view of 'first generation' methods with respect to failure of a human performing a given task is thus clear: the task characteristics, captured quantitatively in the HEP assignment, are regarded as the most influential factors for the estimation of the probability of human failure whereas the environment in which the task is performed, which is represented by the PSFs and PIFs, is considered as a minor, corrective factor.

On the other hand, experimental results from extensive studies of human performance in accidents have shown that the importance of the contextual conditions in which the task is

performed is actually greater than the characteristics of the task itself. This has led to a change in the focus of human failure analysis: if the context is the major factor affecting human performance failure, the relation between the context and the probability of human failure should be modelled. This is the underlying principle of the so-called 'second generation' methods of HRA like the Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel 1998) and A Technique for Human Error Analysis (ATHEANA) (Cooper et al. 1994).

Given the above, it seems clear that the traditional risk-based approaches that incorporate risk and vulnerability analyses commonly seen in textbooks and practice today, need to be extended to a broader scope than the standard analysis for the identification of hazards and the probabilistic quantification of their occurrence. The extension must be driven by the need for more confidence in the treatment of risk of surprises and black swans through improved understanding of systems and processes, and the aim of improving the ability to predict what may be coming, including "special-cause variations". For this, methods of analysis, assessment and management are sought that soundly account also for the knowledge dimension supporting the risk evaluation, for reliably supporting the decision making.

In this view, the risk assessment goal is that of describing and characterizing knowledge and lack of knowledge, with uncertainty being a key element of risk (see for example, ISO 31000 definition of risk (ISO 2009), the definition of risk by the Petroleum Safety Authority (PSA-N 2015) and the recommendation given by the SRA glossary (SRA 2015)). In line with such risk conceptualizations, more focus is placed on knowledge and lack of knowledge descriptions and characterizations, compared to more traditional perspectives. Some early work on this has been conducted, see, e.g. Aven and Heide (2009), Aven (2011) and Hansson and Aven (2014), with the aim of systematically and explicitly addressing the difference between the risk as characterized by the analysts and the risk to be considered by the decision makers. The point made is that eventually the decision makers need to address unconditional risk and not only conditional risk as described by the risk analysts and experts. To illustrate this, let P be a probability of an accident scenario A computed by a risk analyst using models and expert judgment. This probability expresses judgments made by the analyst on the basis of a background knowledge K, which covers many assumptions. Hence, we could write explicitly $P = P(A|K)$ to underline that the risk description is conditional on K. The knowledge K may conceal important aspects of the risk associated to the accident scenario A: for example, an assumption undertaken by the analyst may turn out to be wrong. The knowledge K can be weak and surprises may occur relative to this knowledge. On the other hand, the decision maker must consider all risks for making his/her decisions based on unconditional risk.

The current descriptions of risk and the related frameworks for its assessment need to be extended for a proper characterization of the knowledge which they are built on and of the lack of knowledge which limits them. This should enable to characterize the gap between the conditional risk resulting from the assessment and the unconditional risk that the decision maker needs to consider for managing risk properly. In this view, the probability metric used within a classical description of uncertainty does not provide information on the quality of the assessment, i.e., the quality and strength of knowledge which support the assumptions made for the assessment itself and this could conceal important aspects which affect the consequent predictive capability of the risk model.

By characterizing the strength of knowledge that supports the assumptions underpinning the risk model and leading to the conditional risk results, the decision maker should be made aware of the gap with the unconditional risk and the fact that surprises may occur relative to what is captured in the model based on the analyst knowledge, and would thus be more or less cautious in the decisions.

Approaches for the assessment and visualization of uncertainty in probability-consequence diagrams (PCDS) have been reviewed in (Goerlandt and Reniers 2016). After justifying why uncertainty needs to be considered in such diagrams, a relatively recently proposed uncertainty-based risk perspective is adopted as the basis for considering the issue of uncertainty visualization. A review of existing proposals for representing uncertainty in PCDS is made, including the family of ‘‘risk curves” approach, uncertainty boxes, bubble diagrams and PCDS with prediction intervals and strength-of-evidence assessments (PCD-PISEA). A discussion on the elements found in these proposals has revealed a number of strengths and weaknesses of these. Overall, the PCDS-PISEA approach was found most favorable. However, due to some inconsistencies in the strength-of-evidence rating and the lack of inclusion of the potential for surprises, some modifications to this approach have been suggested. The new approaches focus directly on the strength-of-evidence, which is treated separately for different evidence types. This is done to alleviate the inconsistencies in earlier proposals, and especially to provide more direct insight in the types of evidence supporting the quantitative uncertainty assessments of probabilities and consequences. In another proposal, an assumption deviation risk assessment is visualized along with a segmented strength-of-evidence assessment.

In (Aven 2013), two methods are presented for describing the strength of knowledge that supports the risk assessment. The first one is a direct grading of the strength of knowledge, in line with the scoring proposed in Flage and Aven (2009), which looks at the knowledge, data and expertise related to the risk setting of interest.. The second one is based on the analysis of the main assumptions on which the risk assessment is constructed and their sensitivity evaluation as uncertainty factors with respect to an “assumption deviation risk” concept. For each relevant assumption, one assesses the deviations from the conditions/states defined and assigns a risk score for each deviation, which reflects

- magnitude of the deviation
- probability of this magnitude to occur
- the effect of the change on the consequences,

using score categories such as high, medium or low.

This “assumption deviation risk” score, which is to be seen as measure of criticality or importance of the assumption, captures the basic components of the risk description of the extended risk perspectives, i.e., here i) the deviation from the assumptions made with associated consequences, ii) a measure of uncertainty of this deviation and consequences, and iii) the knowledge that these are based on..

Based on these evaluations, one can draw conclusions about the overall strength of the knowledge that supports the probabilistic analysis: for example, if we have a low number of assumptions with high criticality/risk score, we would classify the strength of knowledge as high. If, however, there are many assumptions with high criticality/risk scores, we would conclude that the strength of knowledge is poor.

This risk/criticality scoring can also be used as a guideline for where to place the focus to improve the risk assessment. The assumptions with the high score should be examined to see if they can be dealt with in some way and removed from the highest risk/criticality category.

The strength of knowledge, then, becomes an additional dimension of the risk assessed, that alerts and makes aware the decision maker of the quality of the risk assessment and the confidence that can be placed in its results.

Another aspect to be included in the extended risk perspective relates to the identification of possible surprises relative to the knowledge that is used in the assessment to produce the (conditional) risk results (the black swans of type II in Aven 2013). In Aven 2013, a procedure

is proposed which considers the events having low risk by reference to probability, consequences and strength of knowledge and reviews of all knowledge and evidence related to these events. This analysis is carried out by experts different from those that have performed the risk assessment, to allow for different perspectives. The results of the analysis complete the risk assessment results.

## 4. CONCLUSION

The social and economic stability of the World has become strongly dependent on the reliable supply of essential goods and services that are transported and distributed across large technological networked infrastructure systems. These critical infrastructures are challenged by potential disruptive factors coming from the hazardous, natural and man-made, environments they are operated in, e.g. global warming, disease outbreaks, food (distribution) shortages, financial crashes, heavy solar storms, organized (cyber-) crime, or cyber warfare. Also, the infrastructure systems have been growing independently and very fast, in a somewhat uncontrollable manner, creating underlying pathways along which dangerous hazards and damaging events can spread rapidly and globally throughout the system: this has increased the exposure to systemic risk, characterized by cascades of failures which can have significant impacts at the global system scale.

Indeed, large-scale disruptions have been experienced, which have led the protection and resilience of critical infrastructures to become a national and international priority. For example, in 2009, a framework for European Union (EU) cooperation on disaster prevention across all types of natural and man-made hazards was agreed upon by the EU Member States in Council conclusions.

For adequate protection and resilience of a critical infrastructure, a number of questions must be addressed: What is its inherent vulnerability? Which are its critical components that if they fail cause large consequences? What is the mechanism of propagation of failures across the critical infrastructure, which makes a local initiating event develop into a cascade of failures with global, system-level consequences? How will the critical infrastructure react to unexpected events and how large can the consequences become? Are there particular properties that allow the critical infrastructure to resist to systemic failures? How to evaluate the resilience of the critical infrastructure? How to find an ‘optimal’ strategy for the critical infrastructure to effectively recover from disruption?

To answer these questions, vulnerability and risk analyses must be undertaken based on new, extended paradigms. Indeed, a fundamental building block of the just mentioned EU cooperation framework for critical infrastructure protection and resilience is vulnerability and risk assessment, which constitute the basis for a successful disaster risk management strategy. As a practical action of initiation, in 2011 the Council asked the Commission to develop an overview of natural and man-made disaster risks the EU may face in the future, based on national risk assessments (NRAs). The overview focuses primarily on those risks which are ‘shared’, i.e. whose impacts are likely to cross borders and be experienced by more than one Member State. National risk assessments have been considered and compared focusing on risk characteristics of probability/likelihood of occurrence, magnitude of the impact, cross-border dimension. The potential risk of losing a CI was identified in 7 out of the 18 NRAs provided, also as a cascade effect of other identified natural and malicious risks.

The findings of these NRAs and other studies confirm that high degree of inter- and intra-connectedness that critical infrastructures have, can make them vulnerable to global disruption, when exposed to hazards of various nature, from random mechanical/physical/material failures to natural events, software failures, intentional

malevolent attacks, human and organization errors. It is widely recognized that this broader spectrum of hazards and threats, calls for an all-hazards approach for the understanding of the failure behavior of such systems, for their effective protection and for ensuring resilience (Zio et al. 2011).

Given the complexity of these systems, the characterization of the hazardous events and the evaluation of their consequences and probabilities, call for an integrated framework capable of including a variety of methods of analysis for capturing the problem from the different characteristic perspectives related to their topological, functional, logic and dynamic properties.

Further, as CI are interdependent and can extend well beyond the geographical and jurisdiction limits of a single State, achieving a harmonized, holistic, system-of-systems approach to risk assessment and management is necessary for providing adequate protection and resilience. Indeed, due to the inter-dependences of essential services, the disruption of one part of a critical infrastructure may trigger a domino effect causing the loss of functionality of other key services, as seen in various recent accidents. For this reason, the EU Commission is encouraging a system-of-systems approach where critical infrastructures are treated as an interconnected framework and the European Programme for Critical Infrastructure Protection (EPCIP) is contributing extensively to collaboratively involving the EU member States towards this objective, lately with a much pragmatic push to the implementation of elements of risk assessment on real case studies of infrastructures of European dimension.

Advanced modelling, simulation, analysis and optimization methods are needed for the protection and resilience of critical infrastructures against systemic failures. Modeling, simulation and analysis can provide the tools for the quantification of the resilience of critical infrastructures, and allow the evaluation and comparison of the effectiveness of different protection and recovery strategies that are proposed to avoid and reduce the adverse consequences of disruptive events.

A promising way seems that of conceptualizing a control framework for risk and vulnerability analysis, whereby accidents are seen to occur due to process variations beyond the designed and operated safety barriers. Concepts of “common-cause variation” and “special-cause variation”, and the continuous focus on learning and updating for improvement in observability and controllability, could be introduced to capture “normal” system variations, and the “unusual” variations and surprises (black swans). Accidents can be seen as resulting from inadequate control or insufficient enforcement of safety-related constraints on the development, design, and operation of the system, leading to their violation and subsequently to accidents. Then, in this view, the notions of controllability and observability can be related to accident causation and prevention, by the ability of a system to be brought back to its “safety zone” through control inputs and the idea that an accident sequence can be interrupted through appropriate control inputs.

Vulnerability and risk assessment, and risk management drive a majority of the core activities associated with critical infrastructure protection and resilience, including executive and managerial decision-making for prioritization of programs and investments. Risk qualitative measures and quantitative metrics also support the design, deployment and employment of protection and resilience management strategies, by measuring their effectiveness and efficiency.

Vulnerability and risk assessment, and risk management are both foundational concepts and analytic disciplines solidly rooted on a structured and systematic approach, which should be deeply ingrained in the practical application of critical infrastructure protection and resilience. The reason for their application is straightforward, as by identifying and understanding hazards and vulnerabilities of a critical infrastructure one is able to identify

the proper measures to implement for its protection and resilience. However, in practice, the complexity of the critical infrastructures brings significant difficulty in the analysis of the vulnerabilities and the assessment of the risks, in a confident and comprehensive way; this is where the intuitive simplicity of risk management crashes with the practical complexity of vulnerability analysis and risk assessment for critical infrastructures: much research is still needed in this direction.

**Acknowledgments:**
The author thanks the ten anonymous referees and the handling editors for their critical comments that have helped improve the paper in the different stages of its development. Especially the criticisms by one patient referee have been instrumental for resiliently revising the work, helping to finally shape it in a much improved form. The author also acknowledges the contribution of Dr. Elisa FERRARIO in the constructive and expert check of the paper.

**REFERENCES**

Agnati, L. F., Baluska, F., Barlow, P. W., and Guidolin, D. (2009). "Three explanatory instruments in biology." *Communicative and Integrative Biology*, 2(6), 552-563.

Alessandri, A., and Filippini, R. (2013). "Evaluation of Resilience of Interconnected Systems Based on Stability Analysis." Critical Information Infrastructures Security - 7th International Workshop, CRITIS 2012, B. M. Hämmerli, N. K. Svendsen, and J. Lopez, eds., Springer Berlin Heidelberg, 180-190.

Alipour, Z., Monfared, M. A. S., and Zio, E. (2014). "Comparing topological and reliability-based vulnerability analysis of Iran power transmission network." *Proceedings of the Institution of Mechanical Engineers Part O-Journal of Risk and Reliability*, 228(2), 139-151.

Amini, H., Cont, R., and Minca, A. (2013). "Resilience to contagion in financial networks." *Mathematical Finance*.

Apostolakis, G. E., and Lemon, D. M. (2005). "A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism." *Risk Analysis*, 25(2), 361-376.

Attoh-Okine, N. O., Cooper, A. T., and Mensah, S. A. (2009). "Formulation of Resilience Index of Urban Infrastructure Using Belief Functions." *Systems Journal, IEEE*, 3(2), 147-153.

Aven, T. (2011). "On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience Response." *Risk Analysis*, 31(5), 693-697.

Aven, T. (2013). "A conceptual foundation for assessing and managing risk, surprises and black swans." Paper presented at the Network Safety Conference, Toulouse 21-23 November.

Aven, T., and Heide, B. (2009). "Reliability and validity of risk analysis." *Reliability Engineering & System Safety*, 94(11), 1862-1868.

Aven, T., and Krohn, B. S. (2014). "A new perspective on how to understand, assess and manage risk and the unforeseen." *Reliability Engineering & System Safety*, 121, 1-10.

Baldick, R., Chowdhury, B., Dobson, I., Zhaoyang, D., Bei, G., Hawkins, D., Huang, H., Manho, J., Kirschen, D., Fangxing, L., Juan, L., Zuyi, L., Chen-Ching, L., Mili, L., Miller, S., Podmore, R., Schneider, K., Kai, S., Wang, D., Zhigang, W., Pei, Z., Wenjie, Z., and Xiaoping, Z. (2008). "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures." *Power*

*and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 1-8.

Barabasi, A. L., Albert, R., and Jeong, H. (2000). "Scale-free characteristics of random networks: the topology of the World-Wide Web." *Physica A*, 281(1-4), 69-77.

Baroud, H., Barker, K., Ramirez-Marquez, J. E., and Rocco, C. M. (2015). "Inherent Costs and Interdependent Impacts of Infrastructure Network Resilience." *Risk Analysis*, 35(4), 642-662.

Barthélemy, M. (2011). "Spatial networks." *Physics Reports*, 499(1), 1-86.

Bergman, B. (2009). "Conceptualistic Pragmatism: A framework for Bayesian analysis?" *IIE Transactions*, 41(1), 86-93.

Berezin Y., Bashan A., Danziger M.M., Li D. and Havlin S. (2015) Localized attacks on spatially embedded networks with dependencies. Scientific reports, 5: 8934.

Bloomfield, R., Chozos, N., and Nobles, P. (2009). *Infrastructure interdependency analysis: introductory research review*, Adelard, London.

Bobbio, A., Bonanni, G., Ciancamerla, E., Clemente, R., Iacomini, A., Minichino, M., Scarlatti, A., Terruggia, R., and Zendri, E. (2010). "Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network." *Reliability Engineering & System Safety*, 95(12), 1345-1357.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwang, D. U. (2006). "Complex networks: Structure and dynamics." *Physics Reports-Review Section of Physics Letters*, 424(4-5), 175-308.

Bonanno, G. A., Galea, S., Bucciarelli, A., and Vlahov, D. (2007). "What predicts psychological resilience after disaster? The role of demographics, resources, and life stress." *J Consult Clin Psychol*, 75(5), 671-82.

Bouchon, S. (2006). "The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art." European Commission, Directorate-General Joint Research Centre, Institute for the Protection and Security of the Citizen, Ispra, Italy.

Brown, T., Beyeler, W., and Barton, D. (2004). "Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems." *International Journal of Critical Infrastructures*, 1(1), 108-117.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., and von Winterfeldt, D. (2003). "A framework to quantitatively assess and enhance the seismic resilience of communities." *Earthquake Spectra*, 19(4), 733-752.

Bryson, K.-M., Millar, H., Joseph, A., and Mobolurin, A. (2002). "Using formal MS/OR modeling to support disaster recovery planning." *European Journal of Operational Research*, 141(3), 679-688.

Bush, G.W. (2002). "Homeland Security Presidential Directive-3 (HSPD-3)," Washington, D.C.

Bush, G.W. (2003). "Homeland Security Presidential Directive-7 (HSPD-7)," Washington, D.C.

Buzna, L., Peters, K., Ammoser, H., Kühnert, C., and Helbing, D. (2007). "Efficient response to cascading disaster spreading." *Physical Review E*, 75(5), 056107.

Çağnan, Z., Davidson, R. A., and Guikema, S. D. (2006). "Post-Earthquake Restoration Planning for Los Angeles Electric Power." *Earthquake Spectra*, 22(3), 589-608.

Carpenter, S., Walker, B., Anderies, J. M., and Abel, N. (2001). "From Metaphor to Measurement: Resilience of What to What?" *Ecosystems*, 4(8), 765-781.

Carreras, B. A., Newman, D. E., Dobson, I., and Poole, A. B. (2004). "Evidence for self-organized criticality in a time series of electric power system blackouts." *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 51(9), 1733-1740.

Casalicchio, E., Bologna, S., Brasca, L., Buschi, S., Ciapessoni, E., D'Agostino, G., Fioriti, V., and Morabito, F. (2011). "Inter-dependency Assessment in the ICT-PS Network: The MIA Project Results." Critical Information Infrastructures Security, C. Xenakis and S. Wolthusen, eds., Springer Berlin Heidelberg, 1-12.

Casari, M., and Wilkie, S. J. (2005). "Sequencing Lifeline Repairs After an Earthquake: An Economic Approach." *Journal of Regulatory Economics*, 27(1), 47-65.

Cavalieri F. and Franchin P. (2014) Models for seismic vulnerability analysis of power networks: comparative assessment. Computer-aided civil and infrastructure engineering, 29: 590-607.

Chen, L., Wang, X. F., and Han, Z. Z. (2004). "Controlling chaos in Internet congestion control model." *Chaos Solitons & Fractals*, 21(1), 81-91.

Chou, C. C., and Tseng, S. M. (2010). "Collection and Analysis of Critical Infrastructure Interdependency Relationships." *Journal of Computing in Civil Engineering*, 24(6), 539-547.

Cimellaro, G. P., Reinhorn, A. M., and Bruneau, M. (2006). "Quantification of seismic resilience." Proceedings of the 8th U.S. National Conference on Earthquake Engineering San Francisco, California, USA.

Cimellaro, G. P., Reinhorn, A. M., and Bruneau, M. (2010). "Framework for analytical quantification of disaster resilience." *Engineering Structures*, 32(11), 3639-3649.

Clinton, W. (1998). "Presidential Decision Directive PDD-63, Protecting America's Critical Infrastructures," Washington, D.C.

Cooper, S. E., Ramey-Smith, A. M., Wreathall, J., Parry, G. W., Bley, D. C., Luckas, W. J., Taylor, J. H., and Barriere, M. T. (1994). "A technique for Human Error Analysis (ATHEANA)." NUREG/CR-6093, USNRC, Washington DC.

Correa, G. J., and Yusta, J. M. (2013). "Grid vulnerability analysis based on scale-free graphs versus power flow models." *Electric Power Systems Research*, 101, 71-79.

Cowlagi, R. V., and Saleh, J. H. (2013). "Coordinability and Consistency in Accident Causation and Prevention: Formal System Theoretic Concepts for Safety in Multilevel Systems." *Risk Analysis*, 33(3), 420-433.

Cupac, V., Lizier, J. T., and Prokopenko, M. (2013). "Comparing dynamics of cascading failures between network-centric and power flow models." *International Journal of Electrical Power & Energy Systems*, 49, 369-379.

Crucitti, P., Latora, V., Marchiori, M., and Rapisarda, A. (2003). "Efficiency of scale-free networks: error and attack tolerance." *Physica a-Statistical Mechanics and Its Applications*, 320, 622-642.

D'Agostino, G., Bologna, S., Fioriti, V., Casalicchio, E., Brasca, L., Ciapessoni, E., and Buschi, S. (2010). "Methodologies for inter-dependency assessment." Critical Infrastructure (CRIS), 2010 5th International Conference on, 1-7.

Dalziell EP, McManus ST (2004). Resilience, Vulnerability, Adaptive Capacity: Implications for System Performance. Proceedings of the International Forum for Engineering Decision Making (IFED), Stoos.

Deming, W. E. (2000). *The New Economics*, 2nd ed. MIT CAES, Cambridge, MA.

Dueñas-Osorio, L., Craig, J. I., Goodno, B. J., and Bostrom, A. (2007). "Interdependent Response of Networked Systems." *Journal of Infrastructure Systems*, 13(3), 185-194.

Dueñas-Osorio, L., and Kwasinski, A. (2012). "Quantification of Lifeline System Interdependencies after the 27 February 2010 Mw 8.8 Offshore Maule, Chile, Earthquake." *Earthquake Spectra*, 28(S1), S581-S603.

EPCIP. "European Programme for Critical Infrastructure Protection." http://europa.eu/legislation_summaries/justice_freedom/fight_against_terrorism/133260_en.htm.

Eusgeld, I., Nan, C., and Dietz, S. (2011). "System-of-systems" approach for interdependent critical infrastructures." *Reliability Engineering & System Safety*, 96(6), 679-686.

Fang, Y. P., Pedroni, N., and Zio, E. (2014). "Comparing Network-Centric and Power Flow Models for the Optimal Allocation of Link Capacities in a Cascade-Resilient Power Transmission Network." *Systems Journal, IEEE*, PP(99), 1-12.

Fang, Y., and Zio, E. (2013). "Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems." *American Journal of Operations Research*, 3(1A), 101-112.

Ferrario, E., and Zio, E. (2014). "Assessing nuclear power plant safety and recovery from earthquakes using a system-of-systems approach." *Reliability Engineering & System Safety*, 125, 103-116.

Fiksel, J. (2003). "Designing resilient, sustainable systems." *Environ Sci Technol*, 37(23), 5330-9.

Fioriti, V., D'Agostino, G., and Bologna, S. (2010). "On Modeling and Measuring Inter-dependencies among Critical Infrastructures." *2010 Complexity in Engineering: Compeng 2010, Proceedings*, 85-87.

Flage, R., and Aven, T. (2009). "Expressing and communicating uncertainty in relation to quantitative risk analysis." *Reliability & Risk Analysis: Theory & Application*, 2(13), 9-18.

Gheorghe, A. V., and Schlapfer, M. (2006). "Ubiquity of digitalization and risks of interdependent critical infrastructures." *2006 IEEE International Conference on Systems, Man, and Cybernetics, Vols 1-6, Proceedings*, 580-584.

Goerlandt, F. and Reniers, G. (2016). "On the assessment of uncertainty in risk diagrams". Safety Science, Volume 84, 67-77.

Goldstein, J. (1999). "Emergence as a Construct: History and Issues." *Emergence*, 1(1), 49-72.

Granic, I., and Lamey, A. V. (2000). "The self-organization of the Internet and changing modes of thought." *New Ideas in Psychology*, 18(1), 93-107.

Haimes, Y. Y. (2009). "On the Definition of Resilience in Systems." *Risk Analysis*, 29(4), 498-501.

Hannaman, G., Spurgin, A., and Lukic, Y. (1984). "Human cognitive reliability model for PRA analysis." Electric Power Research Institute, Technical report NUS-4531, Palo Alto California

Hannaman, G., Spurgin, A., and Lukic, Y. (1985). "A model for assessing Human Cognitive Reliability in PRA studies." IEEE Third Conference on Human Factors in Nuclear Power Plants, Monterey, California.

Henry, D., and Ramirez-Marquez, J. E. (2012). "Generic metrics and quantitative approaches for system resilience as a function of time." *Reliability Engineering & System Safety*, 99, 114-122.

Holling, C. S. (1973). "Resilience and Stability of Ecological Systems." *Annual Review of Ecology and Systematics*, 4(1), 1-23.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*, Elsevier Science Ltd.

Hollnagel, E. (2004). *Barriers and accident prevention*, Ashgate, Aldershot, UK.

Hollnagel, E (2012). FRAM: The Functional Resonance Analysis Method: Modeling Complex Socio-Technical Systems. Farnham, UK: Ashgate Publishing.

Hollnagel, E. (2014). *Safety I and Safety II*, Ashgate, Farnham, UK.

Hollnagel, E., Woods, D. D., and Levenson, N. (2006). *Resilience engineering: concepts and precepts*, Ashgate Publishing Limited, Abingdon, Oxon, GBR.

Hong L., Ouyang M., Peeta S., He X.Z. and Yan Y. (2015) Vulnerability assessment and mitigation for the Chinese railway system under floods. Reliability Engineering and System Safety, 137, 58-68.

ISO (2009). ISO 31000:2009, Risk management - Principles and guidelines. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170

Jackson, S. (2007). "6.1.3 System Resilience: Capabilities, Culture and Infrastructure." *INCOSE International Symposium*, 17(1), 885-899.

Jackson, S. (2009). *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions*, John Wiley & Sons, Inc.

Jin, J. G., Tang, L. C., Sun, L., and Lee, D.-H. (2014). "Enhancing metro network resilience via localized integration with bus services." *Transportation Research Part E: Logistics and Transportation Review*, 63, 17-30.

Johansson, J., and Hassel, H. (2010). "An approach for modelling interdependent infrastructures in the context of vulnerability analysis." *Reliability Engineering & System Safety*, 95(12), 1335-1344.

Kaplan, S., Visnepolschi, S., Zlotin, B., and Zusman, A. (1999). *New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*, Ideation International Inc, Southfield, MI.

Klein, R. (2011). "The EU FP6 Integrated Project IRRIIS on Dependent Critical Infrastructures - Summary and Conclusions." 5th International Workshop, CRITIS 2010, C. Xenakis and S. D. Wolthusen, eds., Springer, Athens, Greece, 26-42.

Kozin, F., and Zhou, H. (1990). "System Study of Urban Response and Reconstruction due to Earthquake." *Journal of Engineering Mechanics*, 116(9), 1959-1972.

Kröger, W. (2008). "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools." *Reliability Engineering & System Safety*, 93(12), 1781-1787.

Kröger, W., and Zio, E. (2011). *Vulnerable Systems*, Springer, London.

LaRocca, S., Johansson, J., Hassel, H., and Guikema, S. (2014). "Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems." *Risk Analysis*.

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor Network Theory*, Oxford University Press, Oxford, UK.

Lee, E. E., Mitchell, J. E., and Wallace, W. A. (2007). "Restoration of services in interdependent infrastructure systems: A network flows approach." *IEEE Transactions on Systems Man and Cybernetics Part C-Applications and Reviews*, 37(6), 1303-1317.

Levenson, N. (2011). *Engineering a Safer World*, The MIT Press, Cambridge, UK.

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

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, Wiley.

Liu, H., Davidson, R. A., and Apanasovich, T. (2007). "Statistical Forecasting of Electric Power Restoration Times in Hurricanes and Ice Storms." *Power Systems, IEEE Transactions on*, 22(4), 2270-2279.

Liu, Y. Y., Slotine, J. J., and Barabasi, A. L. (2013). "Observability of complex systems." *Proceedings of the National Academy of Sciences of the United States of America*, 110(7), 2460-2465.

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., and Cruz, E. (2009). "Empirical Findings on Critical Infrastructure Dependencies in Europe." Critical Information Infrastructure Security, R. Setola and S. Geretshuber, eds., Springer Berlin Heidelberg, 302-310.

Madni, A. M., and Jackson, S. (2009). "Towards a Conceptual Framework for Resilience Engineering." *Systems Journal, IEEE*, 3(2), 181-191.

Manyena, S. B. (2006). "The Concept of Resilience Revisited." *Disasters*, 30(4), 434-450.

Masys, A. J. (2012). "Black swans to grey swans: revealing the uncertainty." *Disaster Prevention and Management: An International Journal*, 21(3), 320-335.

Matisziw, T., Murray, A., and Grubesic, T. (2010). "Strategic Network Restoration." *Networks and Spatial Economics*, 10(3), 345-361

Mei, S., Zhang, X., and Cao, M. (2011). *Power Grid Complexity*, Springer-Verlag Berlin Heidelberg.

Moteff, J. D. (2012). "Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress." Congressional Research Service.

Najjar, W., and Gaudiot, J. L. (1990). "Network resilience: a measure of network fault tolerance." *Computers, IEEE Transactions on*, 39(2), 174-181.

NECSI. (2005). "Visualizing Complex Systems Science (CSS)." New England Complex Systems Institute, www.necsi.org/projects/mclemens/viscss.html, Accessed: 30-Nov-2010.

Netkachov, O., Popov, P., and Salako, K. (2014a). "Model-based Evaluation of the Resilience of Critical Infrastructures under Cyber Attacks." 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), Limassol, Cyprus.

Netkachov, O., Popov, P., and Salako, K. (2014b). "Quantification of the Impact of Cyber Attack in Critical Infrastructures." Computer Safety, Reliability, and Security, A. Bondavalli, A. Ceccarelli, and F. Ortmeier, eds., Springer International Publishing, 316-327.

Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E., and Gradney, P. (2005). "Risk Assessment in Complex Interacting Infrastructure Systems." System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on.

Noda, S. (1993). "Optimum post-earthquake restoration of a telephone system using neural networks." *Journal of natural disaster science*, 15(1), 91-111.

Obama, B. (2013). "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," Washington, D.C.

OECD. (2008). "The future of the internet economy." Organisation for Economic Co-operation and Development, Policy Brief.

Omer, M., Nilchiani, R., and Mostashari, A. (2009). "Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System." *Systems Journal, IEEE*, 3(3), 295-303.

Ottino, J. M. (2004). "Engineering complex systems." *Nature*, 427(6973), 399-399.

Ouyang, M. (2014). "Review on modeling and simulation of interdependent critical infrastructure systems." *Reliability Engineering & System Safety*, 121, 43-60.

Ouyang Min. (2013) Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos, 23: 023114.

Ouyang Min, Zhao Lijing, Hong Liu, Pan Zhezhe. (2014) Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliability Engineering and System Safety, 123: 38-46.

Ouyang, M., and Dueñas-Osorio, L. (2012). "Time-dependent resilience assessment and improvement of urban infrastructure systems." *Chaos*, 22(3), 033122.

Ouyang, M., Duenas-Osorio, L., and Min, X. (2012). "A three-stage resilience analysis framework for urban infrastructure systems." *Structural Safety*, 36-37, 23-31.

Ouyang, M., Hong, L., Mao, Z.-J., Yu, M.-H., and Qi, F. (2009). "A methodological approach to analyze vulnerability of interdependent infrastructures." *Simulation Modelling Practice and Theory*, 17(5), 817-828.

Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X. and Xie, F., *"Cyber-physical system risk assessment"*, In Proceedings of Ninth International Conference on Intelligent Information Hiding and Mulitmedia Signal Processing, IEEE Computer Society, 442-447.

Peters, K., Buzna, L., and Helbing, D. (2008). "Modelling of cascading effects and efficient response to disaster spreading in complex networks." *IJCIS*, 4(1-2), 46-62.

Poljanšek, K., Bono, F., and Gutiérrez, E. (2012). "Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks." *Earthquake Engineering & Structural Dynamics*, 41(1), 61-79.

Popov, P. (2009). "PIA:FARA (Probabilistic Interdependency Analysis: framework, data analysis and on-line risk assessment)." http://www.city.ac.uk/centre-for-software-reliability/research/research-projects/piafara-probabilistic-interdependency-analysis-framework,-data-analysis-and-on-line-risk-assessment, City University London.

PSA-N (2015). Petroleum safety authority Risk and risk understanding, http://www.psa.no/risk-and-risk-management/category897.html

Pursiainen, C. (2009). "The Challenges for European Critical Infrastructure Protection." *Journal of European Integration*, 31(6), 721-739.

Reed, D. A., Kapur, K. C., and Christie, R. D. (2009). "Methodology for Assessing the Resilience of Networked Infrastructure." *IEEE Systems Journal*, 3(2), 174-180.

Rigaud, E. and Guarnieri, F. (2006), "Proposition of a conceptual and a methodological modeling framework for resilience engineering", 2nd Symposium on Resilience Engineering, Nov 2006, Juan-les-Pins, France.

Rinaldi, S. A., Peerenboom, J. P., and Kelly, T. K. (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE Control Systems Magazine*, 21(6), 11-25.

Rosas-Casals, M. (2009). "Topological complexity of the electricity transmission network. Implications in the sustainability paradigm," Universitat Politècnica de Catalunya.

Rosas-Casals, M., Valverde, S., and Solé, R. V. (2007). "Topological vulnerability of the european power grid under errors and attacks." *International Journal of Bifurcation and Chaos*, 17(7), 2465-2475.

Rose, A. Z., Oladosu, G., Lee, B., and Asay, G. B. (2009). "The Economic Impacts of the September 11 Terrorist Attacks: A Computable General Equilibrium Analysis." *Peace Economics, Peace Science, and Public Policy*, 15(5), 1-31.

Rosenkrantz, D. J., Goel, S., Ravi, S. S., and Gangolly, J. (2009). "Resilience Metrics for Service-Oriented Networks: A Service Allocation Approach." *Services Computing, IEEE Transactions on*, 2(3), 183-196.

Rouse, W. B. (2003). "Engineering complex systems: Implications for research in systems engineering." *IEEE Transactions on Systems Man and Cybernetics Part C-Applications and Reviews*, 33(2), 154-156.

Ruzzante, S., Castorini, E., Marchei, E., and Fioriti, V. (2010). "A Metric for Measuring the Strength of Inter-dependencies." *Computer Safety, Reliability, and Security*, 6351, 291-302.

Ryan, J. (2010). *A History of the Internet and the Digital Future*, Reaktion Books.

Sansavini, G., Piccinelli, R., Golea, L. R., and Zio, E. (2014). "A stochastic framework for uncertainty analysis in electric power transmission systems with wind generation." *Renewable Energy*, 64, 71-81.

Shao S., Huang X., Stanley H.E. and Havlin S. (2015) Percolation of localized attack on complex networks. New Journal of Physics, 17, 023049.

Shinozuka, M., Chang, S. E., Cheng, T.-C., Feng, M., O'rourke, T. D., Saadeghvaziri, M. A., Dong, X., Jin, X., Wang, Y., and Shi, P. (2004). *Resilience of integrated power and water systems*, Multidisciplinary Center for Earthquake Engineering Research, Buffalo, NY.

Seth, A. (2008). "Measuring emergence via nonlinear Granger causality." *Artificial Life XI: Proceedings of the Eleventh International Conference on the Simulation and Synthesis of Living Systems*, 545-552.

Song, C. M., Havlin, S., and Makse, H. A. (2006). "Origins of fractality in the growth of complex networks." *Nature Physics*, 2(4), 275-281.

SRA (2015). Society of Risk Analysis, "Glossary of the specialty group on Foundations of Risk Analysis." http://www.sra.org/news/sra-develops-glossary-risk-related-terms

Starr, R., Newfrock, J., and Delurey, M. (2003). "Enterprise resilience: managing risk in the networked economy." Enterprise Resilience: Risk and Security in the Networked World, R. Rothenberg, ed., Booz Allen Hamilton Inc.

Sun, K., and Han, Z.-X. (2005). "Analysis and Comparison on Several Kinds of Models of Cascading Failure in Power System." *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 1-7.

Svendsen, N. K., and Wolthusen, S. D. (2007). "Connectivity models of interdependency in mixed-type critical infrastructure networks." *Inf. Secur. Tech. Rep.*, 12(1), 44-55.

Swain, A. D. (1987). "Accident sequence evaluation program human reliability analysis procedure." NUREG/CR-4772.

Swain, A. D., and Guttman, H. E. (1983). "Handbook of human reliability analysis with emphasis on nuclear power plant applications." NUREG/CR-1278.

Ten, C.-W., Liu, C.-C., and Manimaran, G. (2008). "Vulnerability Assessment of Cybersecurity for SCADA Systems." *Power Systems, IEEE Transactions on*, 23(4), 1836-1846.

Tierney, K., and Bruneau, M. (2007). "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction." *TR News*, 250.

Todini, E. (2000). "Looped water distribution networks design using a resilience index based heuristic approach." *Urban Water*, 2(2), 115-122.

Trucco, P., Cagno, E., and De Ambroggi, M. (2012). "Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures." *Reliability Engineering & System Safety*, 105, 51-63.

U.S. Department of Homeland Security. (2009). "National infrastructure protection plan - Partnering to enhance protection and resiliency."

Utne, I. B., Hokstad, P., and Vatn, J. (2011). "A method for risk modeling of interdependencies in critical infrastructures." *Reliability Engineering & System Safety*, 96(6), 671-678.

Wang, S., Hong, L., Chen, X., Zhang, J., and Yan, Y. (2011). "Review of interdependent infrastructure systems vulnerability analysis." Intelligent Control and Information Processing (ICICIP), 2nd International Conference on, 446-451.

West, M. (2004). *Real Process Improvement Using the CMMI*, Auerbach, Boston, MA, USA.

Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., and Vaziri, K. (2007). "Optimizing scheduling of post-earthquake electric power restoration tasks." *Earthquake Engineering & Structural Dynamics*, 36(2), 265-284.

Wilkinson, S., Dunn, S., and Ma, S. (2012). "The vulnerability of the European air traffic network to spatial hazards." *Natural Hazards*, 60(3), 1027-1036.

Wreathall, J. (2006). "Properties of Resilient Organizations: An Initial View." Resilience Engineering: Concepts And Precepts, E. Hollnagel, D. Woods, and N. Leveson, eds., Ashgate Publishing, 275-285.

Zhang, P. C., and Peeta, S. (2011). "A generalized modeling framework to analyze interdependencies among infrastructure systems." *Transportation Research Part B-Methodological*, 45(3), 553-579.

Zio, E. (2007a). "From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures." *International Journal of Critical Infrastructures*, 3(3/4), 488-508.

Zio, E. (2007b). *An Introduction to the Basics of Reliability and Risk Analysis*, World Scientific Publishing Co. Pte. Ltd.

Zio, E. (2009). "Reliability engineering: Old problems and new challenges." *Reliability Engineering & System Safety*, 94(2), 125-141.

Zio, E., and Aven, T. (2011). "Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?" *Energy Policy*, 39(10), 6308-6320.

Zio, E., Piccinelli, R., and Sansavini, G. (2011). "An all-hazard approach for the vulnerability analysis of critical infrastructures." Proceedings of the European Safety and Reliability Conference (ESREL) 2011, Advances in Safety, Reliability and Risk Management, C. G. Soares, ed., CRC Press 2011, London, UK, 2451-2458.

Zio, E., and Sansavini, G. (2011). "Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins." *IEEE Transactions on Reliability*, 60(1), 94-101.

Zio, E., and Sansavini, G. (2013). "Vulnerability of Smart Grids With Variable Generation and Consumption: A System of Systems Perspective." *IEEE Transactions on Systems Man Cybernetics-Systems*, 43(3), 477-487.

Zobel, C. W. (2011). "Representing perceived tradeoffs in defining disaster resilience." *Decision Support Systems*, 50(2), 394-403.

**Highlights**

- The problem of the protection and resilience of CIs is the focus of the work
- The vulnerability and risk analysis framework for this is critically examined
- The complexity of CIs is presented as a challenge for system modeling and analysis
- The integration of different modeling perspectives of analysis is put forward as a solution
- The extension of the analysis framework to new methods for dealing with surprises and black swans is advocated