Eur J Secur Res (2016) 1:97–114
DOI 10.1007/s41125-016-0004-2

ORIGINAL ARTICLE

Critical Infrastructures Vulnerability and Risk Analysis

Enrico Zio[1,2]

Received: 8 December 2015 / Accepted: 17 February 2016 / Published online: 15 March 2016

Abstract Vulnerability and risk analysis are considered in relation to critical infrastructures protection. The complexity of critical infrastructures is presented as a challenging characteristic, which calls for new approaches of analysis and the integration of different modeling perspectives. The concepts of vulnerability, risk and resilience are discussed in details and analyzed with respect to their characterization in critical infrastructures (CIs) and the challenges therein. Recent new perspectives on these concepts and their interpretations are also discussed in relation to their applicability for analyzing CI vulnerability and risk, in view of decision making for protection. Throughout the paper, reference is made to systems like the (smart) electric power grid and the Internet, to further exemplify the concepts and issues discussed.

Keywords Critical infrastructures · Complex systems · Electric power grids · Smart grids · Vulnerability · Risk · Uncertainty

1 Introduction

Critical infrastructures (CIs) like the energy transmission and distribution networks, the telecommunication networks, the transportation systems, the water and gas distribution systems are complex systems made by many interacting components assembled by design to provide, as a whole, optimal, consistent and reliable operation, and functional safety (Ottino 2004; Rouse 2003). The configuration that

✉ Enrico Zio
enrico.zio@polimi.it; enrico.zio@ecp.fr; enrico.zio@supelec.fr

[1] CentraleSupélec, Chair System Science and the Energy Challenge, Fondation Electricité de France (EDF), CentraleSupélec, Université Paris-Saclay, Grande Voie des Vignes, 92290 Châtenay-Malabry, France

[2] Dipartimento di Energia, Politecnico di Milano, Via La Masa 34, 20156 Milan, Italy

the system structure takes is often organized hierarchically in a way that it could, in principle, be decomposed into parts and reassembled in the whole, while maintaining its function (Ottino 2004; Rouse 2003).

As the system 'lives', its design and engineering updating, modification, improvement and integration with new technologies, and extension of capacity to meet service demands, creates a need for linking the system 'engineering-on-design' with the ever-changing domains of technology, society, economy, legislation and politics, which determine the profiles of service demand and corresponding expected performance.

In this scenario of evolving (and more and more interdependent) critical infrastructures, concerns are arising on their vulnerability to failure and risk of accident, i.e., on the danger that the allocated system capacities may not be adequate to support the anticipated growing demands, in scenarios of greater integration among critical infrastructures and of market deregulation. Then, the safety margins preventively designed may be insufficient to cope with the expected and unexpected stresses arriving onto the systems. Emergent behaviors may arise in these systems in collective ways difficult to predict from the superposition of the behavior of the individual elements and difficult to manage resiliently. Indeed, large uncertainties exist in the characterization of the failure behavior of the elements of a complex system, of their interconnections and interactions, which make predictions difficult to achieve reliably (Zio and Aven 2011). And in the end, critical infrastructures are witnessing more and more system-level breakdowns which emerge from small perturbations followed by cascades of failures, which lead to large-scale consequences that can trespass the borders to propagate from one system to another one, due to (inter-)dependencies.

Then, the problem of ensuring protection and resilience of critical infrastructures is such that vulnerability and technical risk analyses by reductionist methods are likely to fail to capture the heterogeneity and structural and dynamic, or operational, complexities of these systems, and new approaches are needed, capable of offering a holistic viewpoint (Kröger and Zio 2011). The analysis of these systems 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 problem from different perspectives (topological and functional, static and dynamic, etc.), under the existing uncertainties and given the high system complexity.

In the following Sect. 2, we introduce the concept of critical infrastructures and characterize them as engineered complex systems.

In Sect. 3, vulnerability and risk concepts are introduced and discussed with reference to critical infrastructures design and operation. The need for extended modeling is put forward as a way to understanding system behavior and capturing the related risk and vulnerability factors.

In Sect. 4, some perspectives are offered for what regards approaches that may extend the way of looking into the characteristics of the complex systems that make up critical infrastructures, to analyze 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 (Bouchon 2006; Kröger and Zio 2011).

CIs are various by nature, e.g., physical-engineered, cybernetic or organizational, and by environment (geographical, natural) and operational context (political/legal/institutional, economic, etc.).

CIs are complex systems. A system is a group of interacting elements (or subsystems) having an internal structure which links them into a unified whole. The boundary of a system is to be defined, as well as the nature of the internal structure linking its elements (physical, logical, etc.). A complex system is 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, the former being intrinsic in the system design and the latter emerging from the system operation onto its complex architecture.

Structural complexity derives from a number of characteristics, among which:

- Heterogeneity of components of a given technological domain (because of different internal structures and states) and across different technological domains, due to the increased integration among systems (Gheorghe and Schlapfer 2006).
- Scale and dimensionality of connectivity through a large number of components (nodes) highly interconnected by dependences and interdependences (the former are unidirectional relationships, that is a component depends on another through a link, but this other one does not depend on the former through the same link, while the latter represent bidirectional relationships, that is 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) (Rinaldi et al. 2001; Chou and Tseng 2010; D'Agostino et al. 2010; Fioriti et al. 2010). The issue of interdependency among critical infrastructures has been prioritized by the European Reference Network for Critical Infrastructure Protection (ERNCIP) and a Thematic Area has been launched to address it systematically.

A common example of complex system is the Internet. Initiated in 1969 in the United States as a military project, 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. 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. 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 complex engineered system.

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 structuring into self-similarities.

System architecture is, then, the core structural complexity characteristic defining the topological and/or logic structure linking the elements of a system through their interrelations. It provides the backbone for complex systems dynamic features such as adaptive learning, emergence and evolution.

On top of the presence of hierarchical interdependencies in complex engineered systems, the overall structure itself and the wiring of the different elements in it are very complex to model. Various empirical and theoretical approaches have been introduced to analyze the structure of complex networks by graph theory, at different levels of abstraction of the physical system, e.g., unweighted graphs for pure topological characterization, weighed graphs for attributing physical meaning to the connections, planar graphs to account for physical constraints. A taxonomy based on the nodes connectivity distribution distinguishes free-scale (inhomogeneous) networks, and small-world and random (homogeneous) networks (Erdos and Renyi 1960; Watts and Strogatz 1998; Barabasi 2002).

The strong heterogeneity of the elements and connections in current electricity grids, for example, translates into high sensitivity to direct attacks. This high vulnerability to direct targeted attacks of scale-free networks can be limited by allocating supplemental connections and elements for a more homogeneously distributed architecture. Indeed, the tolerance of homogeneous networks is similar for random failures or direct attacks to nodes and connections, independent of the network size.

In view of the above, the architecture of complex systems is quite relevant and needs careful consideration for its influence on system dynamic evolution and adaptation. System architecture not only lays down the topological map of the system structure, but also allows taking into account the differences between its elements and connections, which are heterogeneous physically, functionally and in role.

Two other characteristics related to the structural complexity of CIs are decomposability and self-organization. The former relates to the divisibility of the system structure into subsystems and into further separate elementary elements. Electric power grids, for example, seem to exhibit a structural property of decomposability.

By enabling 'disassembly' of a complex system into its subsystems and their components, decomposability allows understanding and categorization of system elements. In principle, low decomposability implies potential vulnerability as the system is characterized by massive elements with limited capacity for adaptation and evolution in response to newly emerging challenges. On the other hand, high decomposability translates into a large number of components, connections and interrelations, which may make the system difficult to control, and thus vulnerable. Another situation of vulnerability may arise from significant variations of decomposability level across the smart grid, resulting in system stiffness and possible instabilities.

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

Self-organization is a specific dynamic feature of a complex system capable of re-organizing its isolated elements and subsystems into coherent patterns, without intervention from external influences or a central authority (Granic and Lamey 2000). For example, the open system of the Internet, affected by a continuous growth in the number of components and by technologies evolution, tends to self-organize into stable patterns through the creation of particular niches of services or user 'coalitions.' Such flexibility allows the Internet to adapt continuously to changes in the local environment, while maintaining coherence of structure and reliability of service. In this sense, self-organization constitutes mostly an adaptive and evolutionary property of complex dynamic systems, spontaneously emerging from the interactions of the different system components.

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). Mainly due to self-organization processes, emergent behavior appears more evident in complex dynamic systems without a clear central authority, where some even small local changes evolve into unpredictable forms of high-level organization and behavior. 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. Social networks are not only used for networking with friends, but are also exploited for gathering and communicating relevant users information, or coordinating system-wide actions of entire segments of population. 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 sense, smart grids are also expected to be characterized by an emergent behavior, also in connection to the above mentioned self-organization mechanisms of complex systems and depending on the extent and type of the active involvement of users in the energy management process of future “smart grids”.

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. 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 the dynamic property of complex systems which allows it to adjust its architecture and behavior into a stable coherent pattern under external pressures, using long-term memory experience feedback to anticipate future unfavorable changes in system functioning (NECSI 2005). This adaptation process is made possible by a set of internal mechanisms, named detectors and effectors. The system collects the information on acting external pressures through the detectors. Then, effectors, such as locomotion, communication, manipulation and expulsion, actively change the state of certain components, subsystems and/or their interrelations to keep the system in equilibrium under the acting external forces. Feedback mechanisms play an indispensable role for the anticipation of future changes in support of system equilibrium. The dynamic feedback and learning process provide changes in time to the system components and their interrelations through the successive consideration and evaluation of external and internal factors. In complex engineered CIs like the Internet, the adaptive learning process partly relies on the ability of self-organization driven by local changes.

In the electric power grid, for example, 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 uncertainty regarding the extent of adaptive learning in future smart grids, as well as on the suitable functioning of its mechanism.

Complex systems are also dynamically subject to evolution and growth mechanisms. When the external pressures applied to a system exceed ‘critical values’ beyond which adaptive learning mechanisms are inefficient, 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 constant 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' 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.

We can, then, unarguably state that the engineered, physically networked CIs (often called also lifeline systems) that support national and international social development, economy, quality of life and security in our societies are complex systems; examples (some of which already mentioned) 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 (e.g. the Supervisory Control And Data Acquisition, SCADA, system), Internet, fixed and mobile communications and broadcasting).

Taking the electric power grids as example, these systems are pervasive in our everyday's life as they reach virtually every home, school, hospital, office, factory and institution in developed countries, and are quickly penetrating in developing ones. They are made of a large number of interconnected elements (wires and machines), which link the electricity generators to the customers for satisfaction of their diverse needs. Structural complexity arises in these systems 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 and electrical vehicles, etc.) (Ruzzante et al. 2010).

Extending the considerations on the electric power grids from their current configuration to the foreseen future "smart" developments in response to the challenges posed ahead for the vital service they provide, one must consider the evolution from their original development as loosely interconnected networks of local systems, to 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)]. Recently, distributed resources, mostly small power generators driven by renewable sources (e.g. solar and wind), are being increasingly connected to the existing backbone. The extent of the interconnectedness, the number and variety of power sources and generators, of controls and loads, make electric power grids among the most complex engineered systems. In virtue of this evolution, the originally complicated engineered systems become complex with hallmarks of dynamic complexity such as adaptation, self-organization and emergent behavior, which offer opportunities for extended, improved and more reliable service but also pose vulnerabilities, mostly due to unforeseen and hidden complications added during the integration process (Ottino 2004). Emergent behaviors may arise in these systems in collective ways difficult to predict from the superposition of the behavior of the individual elements. This has been seen in system-level breakdowns triggered by small perturbations followed by accelerating cascades and large-scale, border-crossing consequences, due to (inter-) dependencies.

While the re-conceptualization of the electric power grid is fast-occurring to allow 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., which will convert the existing power grid from a static infrastructure to be operated as designed into a flexible, adaptive infrastructure operated proactively through three foundational layers: power and energy, communication, IT/computer. What emerges is the typical construct of 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. For example, the growing role of ICT in the energy infrastructure requires that cyber-security be considered in the development of smart grids from the outset (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.

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

CIs vulnerability and risk must be analyzed and assessed in order to prepare to address them by design, operation and management. Risk analysis as a formalized subject has existed for about three decades, and has reached a wide range of applications with the purpose of revealing and identifying potential failure modes and hazards in our systems so that they may be corrected before they manifest.

In general terms, risk includes two dimensions to describe 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; their characterization is uncertain due to the imperfect knowledge on the conditions under which they actually develop during an accident. Accident scenarios are a relevant part of risk, in that they are those combinations of events potentially leading to the undesired consequences; their uncertainty is quantitatively expressed in terms of frequencies and probabilities of occurrence of the involved events.

For purposes of decision making, it is necessary to provide a quantification of risk, i.e., of the consequences of the accident scenarios, e.g. measured in terms of losses, damages, injuries etc., and of their likelihood of occurrence quantified by some measure of uncertainty, e.g. in terms of probabilities (frequencies). For CIs, 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 developed, which add the dimension of knowledge to the risk description (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 uncertainty and 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 results in decision making; how to measure it, is an open challenge.

Besides this quantitative 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.

While the concept of risk is fairly mature, the concept of vulnerability is still evolving and not yet fully established (Aven 2011; Zhang and Peeta 2011). The term vulnerability has been introduced as the hazard-centric perception of disasters for which the representation in terms of risk appears too limited. A hazard of low intensity could have severe consequences on a system, while a hazard of high intensity could have negligible consequences: the level of vulnerability of the system makes the difference.

A recent definition is given in the glossary of the specialty group on "Foundations of Risk Analysis" of the Society for Risk Analysis, whereby vulnerability of a system refers to risk and the degree that the system can be affected by it (Glossary 2014).

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 and susceptibility to suffering losses and damages (this depends on the system robustness, which is the antonym of vulnerability);
- degree of resilience, i.e., a measure of the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of hazards.

In the context of the present paper, vulnerability is seen as a global technical property and is 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 it can be expressed in terms of the frequency of major blackouts (number per year) and the associated severity, measured either in power lost or energy unserved (MW or MWh).

Another interpretation qualifies directly system components, i.e., a component is a vulnerability of a system if its failure causes large negative consequences to that system (Johansson and Hassel 2010).

Given the above, the goals of vulnerability and risk analysis 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 completeness of the set and of management of its dimension, by organizing and structuring it so that the important event sequences are explicitly identified, and the less important ones grouped into a finite number of categories.
4. Given the set of initiating events, event sequences and observed outcomes, determine and elaborate on (inter-) dependencies (within the system and among systems), and on coupling of different orders.

The ultimate goal is to identify obvious and, most importantly, hidden vulnerabilities and, also, non-resilience issues, in infrastructure systems, to be able to act and manage them before they manifest as failures. 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).

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 system response and its uncertainty.
- Given the nature and role of the CIs, 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, resilience…}.
- Economic attributes {life-cycle costs, costs-benefits, market drivers, business continuity, asset integrity…}.
- Social attributes {supply–demand, active players…}.
- Environmental attributes {pollution, sustainability…}.

Modeling and analysis by reductionist methods are likely to fail to capture the behavior of the complex systems that make up the CIs, 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).

The analysis of these systems 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 problem from different perspectives (topological and functional, static and dynamic, etc.), 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; Alipour et al. 2014; Fang and Zio 2013).
- 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).

On one side, the above methods must be expanded and complemented with methods for probing surprising events which can potentially emerge from the CIs 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 2007). Using these methods, hazardous events and scenarios are identified.

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, 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?" or "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 CIs 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).

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 interrelationship (Hollnagel 2004). FRAM is based on the idea that failure is 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. The thorough identification of the system functions, the study of their possible variability and potential for resonance, and the damping barriers installed in the system offer a way for understanding accident progression.

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, 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 Monte Carlo simulation and design of experiment techniques (Zio 2013; Turati et al. 2015) 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 (Kundzewicz et al. 2005). 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 Guttmann 1983), Accident Sequence Evaluation Program (ASEP) (Swain 1987) and Human Cognition Reliability (HCR) (Hannaman et al. 1984, 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 modeled. 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. 1996).

Given all the above, it seems clear that the traditional risk-based approaches that incorporate risk and vulnerability analyses, 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.

4 Conclusion

The protection of critical infrastructures has become a national and international priority. To be effective, vulnerability and risk analyses must be undertaken based on new, extended paradigms. The high degree of inter- and intra-connectedness that critical infrastructures reach, can make these systems 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 (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.

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).

Acknowledgments The author wishes to thank Dr. Yiping Fang of ETHZ and Dr. Elizaveta Kutnetsova of PS2E for the valuable and insightful analyses that they have contributed as part of their thesis research. Deep thanks go also to Xing Liu of CentraleSupélec, Paris, for her contribution in the preparation of the manuscript.

References

Alessandri A, Filippini R (2013) Evaluation of resilience of interconnected systems based on stability analysis. Critical information infrastructures security. Springer, Berlin, pp 180–190

Alipour Z, Monfared MAS, Zio E (2014) Comparing topological and reliability-based vulnerability analysis of Iran power transmission network. Proc Inst Mech Eng Part O J Risk Reliab 228(2):139–151

Apostolakis GE, Lemon DM (2005) A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 25(2):361–376

Aven T (2011) On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Anal 31(4):515–522

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

Aven T, Krohn BS (2014) A new perspective on how to understand, assess and manage risk and the unforeseen. Reliab Eng Syst Saf 121:1–10

Barabasi AL (2002) Linked: the new science of networks. Perseus Publishing, Cambridge

Barabasi AL, Albert R, Jeong H (2000) Scale-free characteristics of random networks: the topology of the World-Wide Web. Phys A 281(1–4):69–77

Bergman B (2009) Conceptualistic pragmatism: a framework for Bayesian analysis? IIE Trans 41:86–93

Bobbio A, Bonanni G, Ciancamerla E, Clemente R, Iacomini A, Minichino M, Scarlatti A, Terruggia R, Zendri E (2010) Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. Reliab Eng Syst Saf 95(12):1345–1357

Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang DU (2006) Complex networks: structure and dynamics. Phys Rep Rev Sect Phys Lett 424(4–5):175–308

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

Casalicchio E, Bologna S, Brasca L, Buschi S, Ciapessoni E, D'Agostino G, Fioriti V, Morabito F (2011) Inter-dependency assessment in the ICT-PS network: the MIA project results. Critical Information Infrastructures Security. Springer, Berlin, pp 1–12

Chen L, Wang XF, Han ZZ (2004) Controlling chaos in internet congestion control model. Chaos Solitons Fractals 21(1):81–91

Chou CC, Tseng SM (2010) Collection and analysis of critical infrastructure interdependency relationships. J Comput Civil Eng 24(6):539–547

Cooper SE, Wreathall J, Thompson C, Drouin M, Bley D (1996) Knowledge-base for the new human reliability analysis method: a technique for human error analysis (ATHEANA). In: International topical meeting on probabilistic safety assessmentmoving toward risk based regulation, Park City, UT (US)

Cowlagi RV, Saleh JH (2013) Coordinability and consistency in accident causation and prevention: formal system theoretic concepts for safety in multilevel systems. Risk Anal 33(3):420–433

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

Deming WE (2000) The new economics, 2nd edn. MIT CAES, Cambridge

Dueñas-Osorio L, Craig JI, Goodno BJ, Bostrom A (2007) Interdependent response of networked systems. J Infrastruct Syst 13(3):185–194

Erdos P, Renyi A (1960) On the evolution of random graphs. Publ Math Inst Hung Acad Sci 5:17–60

Eusgeld I, Nan C, Dietz S (2011) "System-of-systems" approach for interdependent critical infrastructures. Reliab Eng Syst Saf 96(6):679–686

Fang YP, Zio E (2013) Hierarchical modeling by recursive unsupervised spectral clustering and network extended importance measures to analyze the reliability characteristics of complex network systems. Am J Oper Res 3:101–112

Fioriti V, D'Agostino G, Bologna S (2010) On modeling and measuring inter-dependencies among critical infrastructures. In: Proceedings of 2010 Complexity in Engineering 85–87

Gheorghe AV, Schlapfer M (2006) Ubiquity of digitalization and risks of interdependent critical infrastructures. In: Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on, 1: 580–584

Glossary (2014) Glossary of the specialty group on foundations of risk analysis. Society for risk analysis. http://sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf. Accessed 01 Dec 2015

Goldstein J (1999) Emergence as a construct: history and issues. Emergence 1(1):49–72

Granic I, Lamey AV (2000) The self-organization of the Internet and changing modes of thought. New Ideas Psychol 18(1):93–107

Hannaman GW, Spurgin AJ, Lukic Y (1984) Human cognitive reliability model for PRA analysis. NUS-4531

Hannaman GW, Spurgin AJ, Lukic Y (1985) A model for assessing human cognitive reliability in PRA studies. In Conference record for 1985 IEEE third conference on human factors and nuclear safety

Hollnagel E (1998) Cognitive reliability and error analysis method (CREAM). Elsevier, Oxford

Hollnagel E (2004) Barriers and accident prevention. Ashgate Publishing Limited, Aldershot

Hollnagel E (2014) Safety I and safety II. Ashgate Publishing Limited, Farnham

Johansson J, Hassel H (2010) An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Saf 95(12):1335–1344

Kaplan S, Visnepolschi S, Zlotin B, Zusman A (1999) New tools for failure and risk analysis: anticipatory failure determination (AFD) and the theory of scenario structuring. Ideation International Inc., Southfield

Kröger W (2008) Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. Reliab Eng Syst Saf 93(12):1781–1787

Kröger W, Zio E (2011) Vulnerable systems. Springer, London

Kundzewicz ZW, Ulbrich U, Graczyk D et al (2005) Summer floods in Central Europe–climate change track? Nat Hazards 36(1–2):165–189

Latour B (2005) Reassembling the social: an introduction to actor Network theory. Oxford University Press, Oxford

Lee EE, Mitchell JE, Wallace WA (2007) Restoration of services in interdependent infrastructure systems: a network flows approach. IEEE Trans Syst Man Cybern Part C Appl Rev 37(6):1303–1317

Leveson N (2004) A new accident model for engineering safer systems. Saf Sci 42(4):237–270

Leveson N (2011) Engineering a safer world. The MIT Press, Cambridge

Liu YY, Slotinef JJ, Barabási AL (2013) Observability of complex systems. Proc Natl Acad Sci 110(7):2460–2465

Masys AJ (2012) Black swans to grey swans: revealing the uncertainty. Disaster Prev Manag 21(3):320–335

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

Newman DE, Nkei B, Carreras BA, Dobson I, Lynch VE, Gradney P (2005) Risk assessment in complex interacting infrastructure systems. In: System Sciences, HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on, IEEE

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

Ottino JM (2004) Engineering complex systems. Nature 427(6973):399

Ouyang M (2014) Review on modeling and simulation of interdependent critical infrastructure systems. Reliab Eng Syst Saf 121:43–60

Ouyang M, Hong L, Mao ZJ, Yu MH, Qi F (2009) A methodological approach to analyze vulnerability of interdependent infrastructures. Simul Model Pract Theory 17(5):817–828

Reed DA, Kapur KC, Christie RD (2009) Methodology for assessing the resilience of networked infrastructure. IEEE Syst J 3(2):174–180

Rinaldi SA, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21(6):11–25

Rouse WB (2003) Engineering complex systems: implications for research in systems engineering. Syst Man Cybern Part C Appl Rev IEEE Trans 33(2):154–156

Ruzzante S, Castorini E, Marchei E, Fioriti V (2010) A metric for measuring the strength of interdependencies. Comput Saf Reliab Secur 6351:291–302

Sansavini G, Piccinelli R, Golea LR, Zio E (2014) A stochastic framework for uncertainty analysis in electric power transmission systems with wind generation. Renew Energy 64:71–81

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

Song CM, Havlin S, Makse HA (2006) Origins of fractality in the growth of complex networks. Nat Phys 2(4):275–281

Swain AD (1987) Accident sequence evaluation procedure (ASEP). NUREG/CR-4277, US NRC

Swain AD, Guttmann HE (1983) Handbook of reliability analysis with emphasis on nuclear plant applications. Technical Report NUREG/CR-1278. Nuclear Regulatory Commission, Washington

Trucco P, Cagno E, De Ambroggi M (2012) Dynamic functional modelling of vulnerability and interoperability of critical infrastructures. Reliab Eng Syst Saf 105:51–63

Turati P, Pedroni N, Zio E (2015) An entropy-driven method for exploring extreme and unexpected accident scenarios in the risk assessment of dynamic engineered systems, ESREL 2015 7–10, Sep 2015. Zurich, Switzerland

Wang S, Hong L, Chen X, Zhang J, Yan Y (2011) Review of interdependent infrastructure systems vulnerability analysis. In: Intelligent Control and Information Processing (ICICIP), 2nd International Conference on, IEEE, 1:446–451

Watts DJ, Strogatz SH (1998) Collective dynamics of 'Small-World' networks. Nature 393:440–442

Zhang PC, Peeta S (2011) A generalized modeling framework to analyze interdependencies among infrastructure systems. Transp Res Part B Methodol 45(3):553–579

Zio E (2007) An introduction to the basics of reliability and risk analysis. World Scientific Publishing, Singapore

Zio E (2009) Reliability engineering: old problems and new challenges. Reliab Eng Syst Saf 94(2):125–141

Zio E (2013) The Monte Carlo simulation method for system reliability and risk analysis. Springer, London

Zio E, 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, Sansavini G (2011) Modeling interdependent network systems for identifying cascade-safe operating margins. Reliab IEEE Trans 60(1):94–101

Zio E, Sansavini G (2013) Vulnerability of smart grids with variable generation and consumption: a system of systems perspective. IEEE Trans Syst Man Cybern Syst 43(3):477–487

Zio E, Piccinelli R, Sansavini G (2011) An all-hazard approach for the vulnerability analysis of critical infrastructures. In: Proceedings of the European Safety and Reliability Conference: 2451–2458