Complexity and vulnerability of Smartgrid systems

E. Kuznetsova, Keith Culver, Enrico Zio

Title draft: Complexity and vulnerability of Smartgrid systems

Elizaveta Kuznetsova[1], Keith Culver[2], Enrico Zio[3,4]

[1] Doctoral candidate, Econoving International Chair in Generating Eco-Innovation, University of Versailles Saint-Quentin-en-Yvelines, France.

[2] Professor and Econoving International Chair in Generating Eco-Innovation, UniverSud Paris / University of Saint-Quentin-en-Yvelines, France.

[3] Chair Systems Science and Energetic Challenge, Ecole Centrale Paris – Supelec, Paris, France

[4] Dipartimento di Energia, Politecnico di Milano, Milano, Italy

Note: This manuscript is meant to be a contribution to the special session "Techno-social Innovations for the Management of Environmental Risks" organized, with the permission of the ESREL 2011 organisers, by Dr. Ioan M. Ciumasu, ECONOVING, University of Versailles / UniverSud Paris, and Prof. Enrico Zio, Chair Systems Science and Energetic Challenge, EcoleCentrale Paris / Supelec.

Abstract

In this paper, we look at the complexity and related vulnerability characteristics of Smartgrids. Typical characteristics of complex systems, such as self-organization, emergence, chaotic behavior and evolution, are considered with respect to Smartgrids as future energy infrastructures. These characteristics are categorized as inherent, challenge-response, or acquired. This guides the identification of major sources of uncertainty in the infrastructure. Topological and behavioral characteristics of Smartgrids are also explored with the aim of identifying potential vulnerabilities.

[1] elizaveta.kuznetsova@uvsq.fr
[2] keith.culver@universud-paris.fr
[3] enrico.zio@ecp.fr, enrico.zio@supelec.fr
[4] enrico.zio@polimit.it

We additionally discuss the assumptions, limitations and degree of precision of Smartgrids modeling.

Keywords: complex engineered system, Smartgrids, vulnerability.

Table of content

1. Introduction

In this paper, we look at Smartgrid systems from the point of view of their complexity and vulnerability related to their characteristics. The framework of analysis is similar to that of other engineered complex systems, e.g. transportation infrastructures, energy networks, telecommunication systems. These systems are characterized by a large number of elements with complex interconnections, nonlinear and discontinuous operation, and the involvement of multiple actors with diverse backgrounds. Further, uncertainties typically exist in the characterization of the system elements and their interconnections (Rouse, 2003). As a result, the modeling and analysis of such systems by reductionist methods are likely to fail, and holistic approaches are needed.

In the context of such complex systems, while it is true that their structural backbones are created by the engineers who develop the constituent components of the system, the connections of such components within the systems are not necessarily all 'designed.' In many instances, undersigned or even undesired connections 'emerge' from system evolution so as to meet the demand under given operation constraints (Ottino, 2004). Complex systems can be said to evolve from the design blueprints to complex structures and behaviors through *engineering*, *updating* and *integration* processes. At the *engineering process* level, elements are assembled by design to provide optimal, consistent and reliable operation, as well as functional safety (Ottino, 2004). In general, this is achieved with engineered systems which may be *complicated* but not yet *complex* (Ottino, 2004). The engineering process is usually organized by hierarchical methods in top-down approaches, managed on a linear timeline organization (Rouse, 2003). In principle, the final product of such process could be reduced to pieces and reassembled, without losing its function. Vulnerability may arise in these systems, particularly from designed defects due to calculation errors or simplifications during the design process.

As the system 'lives', its *updating* and *integration* occurs by insertion of new technology and extension of capacity to meet service demands with the required performance. This creates a need

for connection between the engineering of the system and the ever-changing domains of society, economy, legislation and politics, which determine service demands and generate constraints. In virtue of this connection, the originally complicated engineered system becomes complex with hallmarks of adaptation, self-organization and emergent behavior, which constitute opportunities but pose also vulnerabilities, mostly due to unforeseen complication during the integration process (Ottino, 2004).

One classic example of a complex system is the Internet. Initially built in the United States in the middle of the 20th century as an information technology tool for anti-missile purposes, the Internet has become pervasive. It now 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 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 complex engineered system.

Returning to the concept of a Smartgrid, this term is used to identify the architecture of emerging new energy infrastructures, which use ICT-driven interconnectedness to achieve several goals. These goals include improvements to coordination of energy generation by diverse energy sources (including renewables); improved transmission and distribution for increased efficiency to meet increasing demand, and improved design to ensure protection and resiliency to the vulnerabilities of aging and failing components, natural disasters and human attacks. At regional, national and world

levels, Smartgrid research, development and demonstration is working toward achieving these goals by creating interconnections between energy infrastructure elements, such as producers and consumers, and further introducing intelligent management of electricity balance in the grid (Coll-Mayor, Paget, & Lightner, 2007; Hammons, 2008).

The Internet is particularly relevant as reference complex system in our exploration of Smartgrids. In a sense, the Smartgrid concept may be regarded as referring to a kind of 'Internet of Energy.' While using the Internet as the basis of connection between various elements of the energy grid, the Smartgrid concept additionally borrows from the Internet in the way Smartgrids conceive of the energy grid. Smartgrids, just like the Internet, aim at creating a global, interconnected network of energy actors, while at the same time going further by monitoring, managing and optimizing energy flows.

The remaining of the paper is organized as follows. Section 2 explains the complexity of Smartgrid systems in terms of 'typical' characteristics of complex systems and categorizes these characteristics as engineering, updating and integration processes. Further analysis identifies potential vulnerabilities associated with each characteristic. Section 2 concludes with a nominal ranking of potential vulnerabilities. Section 3 describes methods available for Smartgrids analysis aimed at modeling of characteristics illustrated in previous sections. The last section of the paper provides conclusions and further discussion of strategies for modeling and analysis of Smartgrids complexity.

2. Identification of Smartgrids complexity

In order to understand the complexity level of Smartgrids, this Section recalls classical general characteristics of complex systems (Figure 1), from the point of view of both topological and behavioral properties. Properties of particular relevance for Smartgrids are emphasized. Each characteristic will be further analyzed from the point of view of Smartgrids and allocated to groups

enabling identification of primary sources of system vulnerability related to the processes of *engineering*, *updating* and *integration*.

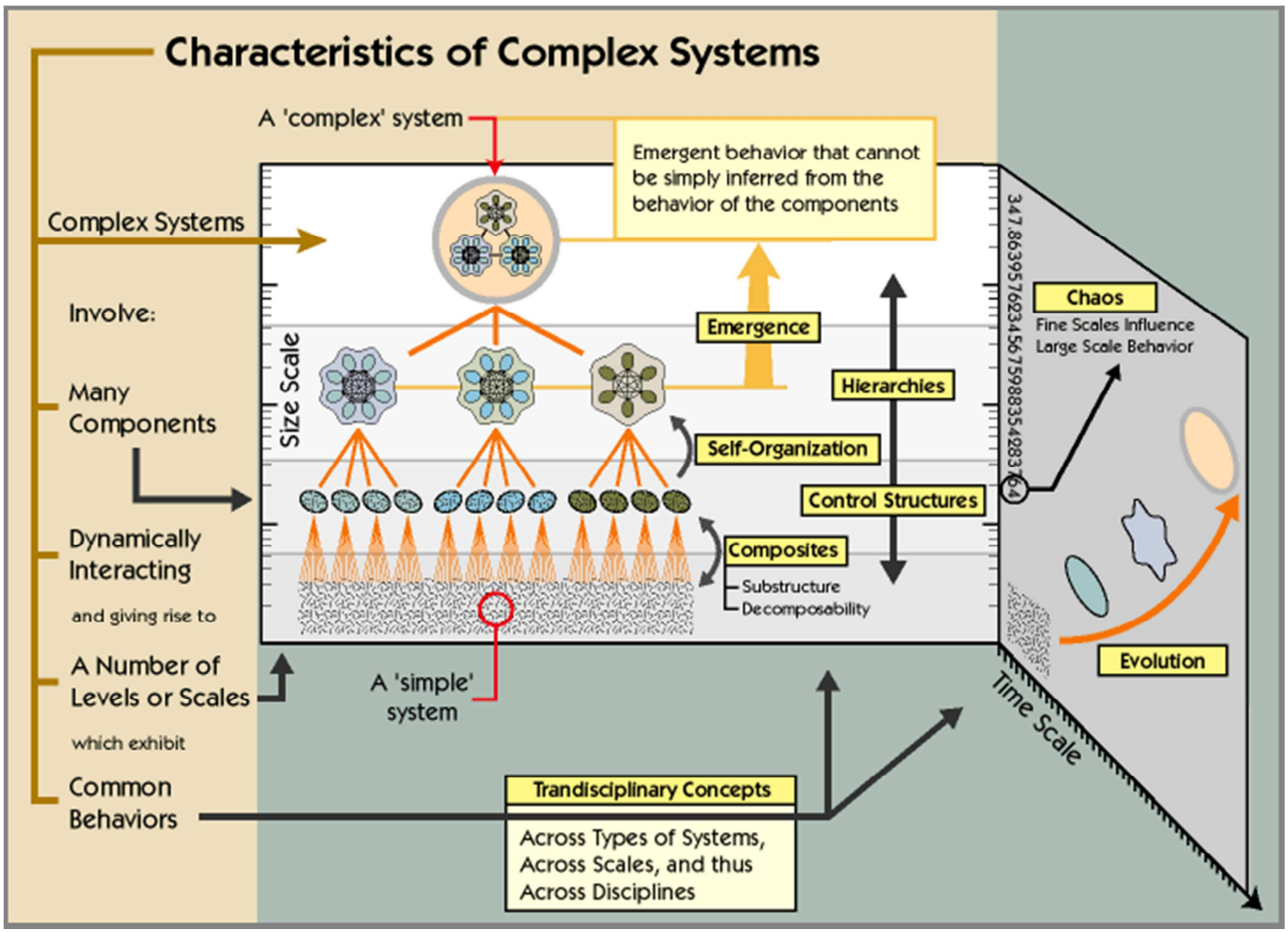


Figure 1: Characteristics of complex systems (NESCI, 2005).

2.1. Characteristics of complexity in Smartgrids

2.1.1. Architecture

System architecture is the core characteristic defining the topological and/or logic structure linking the elements of the system through their interrelations. System architecture is therefore responsible for system behavioral features such as adaptive learning, emergence and evolution. A common structure is hierarchical organization, typical for ecological, taxonomic, genealogical and somatic organization of biological systems. The adaptive and evolutionary mechanisms of organisms of such systems, trying to maintain or increase their fitness in the face of changing environmental conditions, are driven by their hierarchical structural-interactive architecture (Nederbragt, 1997).

Complex engineered systems, such as the Internet, manifest pronounced hierarchical structuring with highly connected nodes related to “isolated sub-systems, forming a mantle-like mass of peer-connected nodes” (Duncan, 2007). Apart from the presence of hierarchical interdependencies, the overall system structuring itself and the wiring of the different elements in it is very complex to model. Currently, many empirical and theoretical approaches attempt to analyze the structure of complex networks by graph theory of different levels of abstraction – unweighted graphs for pure topological characterization, weighted graphs for attributing physical meaning to the connections, planar graphs to account for physical constraints. Typical categorization based on the nodes connectivity distribution considers free-scale (inhomogeneous) networks, and small-world and random (homogeneous) networks. In this view, the architecture of Smartgrid systems is considered to be a relevant feature of future electricity networks, which needs careful consideration for its possible influence in the system’s evolution and adaptation. On the other hand, system architecture not only lays down the topological map of system structure, but also allows taking into account the differences between its elements and connections, which are heterogeneous physically, functionally and in role.

2.1.2. Heterogeneity of elements and connections

Heterogeneity refers to the differences in the elements, their interconnections and roles within the system hierarchical organization, often with high-connected core elements and low-connected periphery nodes. Heterogeneity is strong in current electricity systems, with in architectures in the form of hierarchical trees where production facilities are connected by centralized high-voltage transmission stems to transformation substations linked in their turn by distribution branches to final consumers. Notably, Smartgrid 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.

2.1.3. Self-similarities

Also called fractals, self-similarities are complex system structures as "a rough or fragmented geometric shape that can be split into parts, each of which is (at least approximately) a reduced-size copy of the whole" (Mandelbrot, 1982). Where self-similarities are present in a complex system, they amount to the presence of similar properties at all hierarchical levels, similar complexities at different scales without a unique characteristic size for their structures. Assertion of the existence of a fractal structure in a given complex system depends on the possibility of ascribing to that structure specific dimensionless numbers indicating the nature of self-similarity in the structure or behavior in the complex system. The dimensionless quantification of a fractal structure permits fractals to exhibit the property of scalability. These aspects of fractals are expressed in an instructive structural analogy between a human biological circulatory system and the Internet. The principle of fractal structuring of veins, characterized by an efficient mechanism of blood distribution with minimum structure and shortest path, was borrowed to study the optimal design of the Internet network (Caldarelli, Marchetti, & Pietronero, 2000). A further structural analogy can be found in the extension of the Internet concept into Smartgrid networks. The Smartgrid concept exhibits fractal structuring insofar as a particular Smartgrid may contain an ‘energy automation network’ for ‘positive energy building’ inside district Smartgrids, district Smartgrids inside city Smartgrids and so forth. Here, the ‘energy automation network’ constitutes the mini Smartgrid network, involving consumers, local renewable energy producers, transportation and storage facilities. Smartgrids for ‘positive energy building’ manifest clear periodical self-similarities, with district Smartgrids included in energy flows management with respect to day and season energy demand fluctuations. Certainly, self-similarities appear as an evident characteristic of Smartgrids system structuring.

2.1.4. Self-organization and decomposability

Two other characteristics related to the structure of engineered systems are *decomposability* and *self-organization*. The former relates to the divisibility of the system structure into subsystems, and

into further separate elementary elements. Electricity grids seem to exhibit a structural property of decomposability, especially evident within the fractal patterns envisioned for Smartgrids structures.

Self-organization refers mostly to the behavioral 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. 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 (Granic, 2000). In this sense, self-organization constitutes mostly an adaptive and evolution property of complex dynamic systems, spontaneously emerging from the interactions of the different system components. In this view, the possibility that Smartgrids will possess such complexity will depend on the level of autonomy of the system from other systems, and the number and dynamics of Smartgrids users. For the moment, the role and involvement of consumers in the mechanisms of the electricity network management are not clearly defined, but the potential for failure-resilient self-organization, responsible for other properties such as emergence, adaptive learning and evolution, is ripe for exploitation.

2.1.5. Emergence

Induced by the complex non-linear interconnections between the separate system elements, subsystems and fractals at a micro level, emergence is a 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). 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: the recent dramatic facts related to revolutions in Northern Africa countries and acts of terrorism in Russia prove how in some countries liberty of speech is tolerated only in social blogs, and manifestation or rescue expeditions in emergency situations are organized directly by massive use of the Internet. Electricity 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, Smartgrids are also expected to be characterized by emergent behavior, also in connection to the above mentioned self-organization mechanisms of complex systems and depending to the extent and type of active involvement of users in the energy management process.

2.1.6. Adaptive learning

Adaptive learning allows a system 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. This adaptation process is made possible by a set of internal mechanisms, named detectors and effectors (NESCI, 2005). 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 provides changes in time to the system components and their interrelations through the successive consideration and evaluation of external and internal factors (NESCI, 2005). In complex engineered systems like the Internet, the adaptive learning process partly relies on the ability of self-organization driven by local changes. As the Smartgrid concept strongly relies on a system of intelligent and sustainable management of power flows, adaptive learning mechanisms are expected to be a central feature of design, operation and control.

2.1.7. 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 also exposed to constant growth of user portfolios. Future Smartgrid complex systems will both evolve in the way typical of analogous biological systems, and they will incorporate unanticipated new elements.

2.1.8. Chaos

Chaos theory is used to describe and explain various processes occurring in complex systems, e.g. earth atmosphere and aerodynamics processes (Baas, 2002; Macek, 2010), chemical processes (Lee, 1996) and information and communication processes (Chen, Wang, & Han, 2004). In these processes chaos is used to characterize the capacity of non-linear dynamic systems to produce an unpredictable change in large-scale behavior or a sudden shift in system pattern, in response to fine-scale changes in initial conditions (Baas, 2002). Hence, the well-known aphorism, that butterfly wings flapping can cause a tornado (Lorenz, 1987). Engineered chaotic systems are characterized by high sensitivity to changes, but also by mixing and periodicity. These two last properties are mainly responsible for the formation of complex fractal structures as a manifestation of chaotic properties within a complex system. On the other hand, the fractal structure resulting in 'positive energy building' within Smartgrids is more a man-made structuring aimed at facilitating electricity flows management than an emerging result of chaotic evolution. However, even if Smartgrids patterns will be mainly characterized by 'artificial' structuring, some periodic daily or seasonal self-

similarities, for example in energy consumption behavior between building and district Smartgrids, are likely to arise in manifestation of chaotic behavioral patterns.

2.1.9. Multidisciplinary relations

Multidisciplinary relations are an integral part of engineered complex systems. Smartgrids in particular involve a number of engineering and non-engineering disciplines for defining the successful implementation of new energy systems, e.g. by creation of necessary legislative frameworks for technologies use, finding adequate finance models for innovative projects elaboration, providing incentive support and elaboration of standards, and securing social acceptance and participation.

2.1.10. Vague boundaries

Through the integration process, complex engineered systems become open systems with interactions with the environment. Their multiple relations with non-engineering domains and with other engineered systems result in difficulties of boundary definition. Necessarily, then the modeling of the complex system limits depends on the observer's scope of analysis rather than an intrinsic property of the system. In some associated analyses of analogous systems, other organizational categories are proposed. For example, in legal theory, some theorists argue that while the law of countries is usefully characterized as systemic, international law lacks a systemic quality and is better described as an 'order' which interacts with national legal systems. This example illustrates the extent to which ascription of 'system qualities' may depend on the purposes and initial scope analysis of investigators, rather than any inherent features of the phenomena which in practice, as in the case of international and national law, may appear seamlessly interlinked (Culver & Giudice, 2010).

2.1.11. Self-healing and attacks resistance

As discussed above, Smartgrids potentially exhibit a number of topological and behavioral characteristics typical of complex systems. In addition, they are intended to have specific characteristics arguably conceived as core to the Smartgrids concept: according to a popular vision

of ‘intelligent electricity grids’, they will possess a range of additional properties such as *self-healing* and *resistance* to external natural disasters and human attacks (Battaglini, Lilliestam, Haas, & Patt, 2009; Breuer, Povh, Retzmann, Urbanke, & Weinhold, 2007; Chassin, 2010; Fox-Penner, 2010). These two particular characteristics are related to adaptive learning and evolutionary mechanisms. However, to mark their importance for the Smartgrid concept we will consider these properties apart.

2.2. Categorization of Smartgrids complexity characteristics

In order to explore and explain the complexity of Smartgrids, this Section maps the characteristics of complexity discussed in Section 2.1 into three major categories – *inherent*, *challenge-response*, and *acquired* characteristics (Table 1). These categories are defined in relation to the three processes of *engineering*, *updating* and *integration* of complex engineered systems. The first *inherent* category contains characteristics of Smartgrid systems designed at the *engineering* process level. Properties such as the heterogeneity of elements and connections as well as system architecture, are considered as inherent characteristics of system complexity amenable to control and, therefore, of minimum uncertainty impact on Smartgrid functioning. The second category includes *challenge-response* characteristics. Inspired by the underlying Smartgrids strategy of a flexible and transparent energy management concept for the reinforcement of electricity infrastructure reliability (Hledik, 2009), these characteristics result from the continuous *updating* process in response to the evolution of the challenges to the Smartgrid function. In this context, adaptive learning and self-healing are desirable prospective characteristics for effective challenge-response by smart electricity infrastructures. Due to the uncertain and somewhat unpredictable evolving environment, the challenge-response properties of Smartgrids could not be guaranteed through design process, and their achievement is a challenge itself. Eventually, the third category of acquired characteristics includes self-organization, emergence and chaos which arise as a consequence of the *integration* of the system in the complex socio-economical environment which

drives its functioning. This category regroups the major sources of uncertainty on the functioning of Smartgrids.

Table 1
Categorization of Smartgrids complexity characteristics

Smartgrids complexity characteristics		
Inherent (engineering)	**Challenge-response** (updating)	**Acquired** (integration)
Architecture Heterogeneity Self-similarities Decomposability	Adaptive learning Evolution and growth Self-healing Attack resistance	Vague boundaries Self-organization Emergence Chaos Multidisciplinary relations

Note that this categorization may not be exclusive as some characteristics could be mapped into more than one category. For example, evolution could be considered as both a challenge-response and acquired characteristic. On the one hand, this property can provide Smartgrids the challenge-response characteristic needed for flexibility in handling the uncertain stresses upon the system. On the other hand, evolution may have uncertain negative effects on Smartgrids functioning resulting in increasing of vulnerabilities and incapability to correctly respond to challenges of electricity demand. This may occur under specified conditions: as in the next Section, characteristics such as adaptive learning, evolution and growth can not only produce a positive impact on the Smartgrid functioning, but can also turn into vulnerabilities in the absence of a central authority.

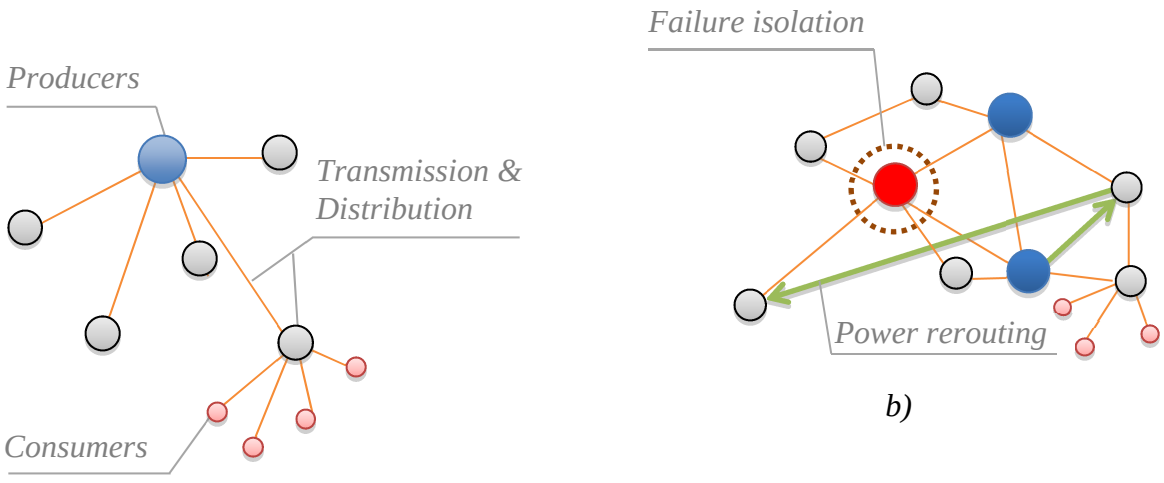
In this respect, not only the uncertain properties of the acquired category, but also inherent complex system characteristics could become vulnerability sources. For example, topological properties of Smartgrids could induce behavioral vulnerability by facilitating disturbance propagation within the network of connections, giving rise to cascading processes which would impair system functioning. This leads to the need to identify sources of potential vulnerability within the system characteristics, and ranking them according to their impact on Smartgrids development and functioning.

2.3. Mapping complexity into vulnerability

This Section points at potential vulnerabilities hidden in the complexity characteristics of Smartgrids.

2.3.1. Architecture

As mentioned above, Smartgrid systems will be developed mainly on the backbone of existing infrastructures. Traditional electricity grid architecture is organized in a strong hierarchical infrastructure with only few centralized electricity transmission channels from energy producers to load consumers (Figure 2a). This type of organization is characterized by unidirectional power flow and vertical control and operation. This centralized hierarchical structure is widely used for systems modeling and presents a relatively transparent system organization with clearly identifiable elements of topology, purpose and control. This system structure is regarded as supplying organizational advantages and facilitating system monitoring, fault detection and correction (Pattee, 1973). Current electricity architecture defines clearly an authority domain and a role for each actor on the energy market, as well as operation and interaction modes between the diverse elements. In this view, the major vulnerability of electricity grids architecture comes from their scale-free organization standing on a limited number of core, highly connected nodes of production sources and few unidirectional transmission channels through which cascading failure propagation may occur in the absence of bypass transmission (Hines, Blumsack, Cotilla Sanchez, & Barrows, 2010; Rosas I Casals, 2009; Zio, 2007).



a) *b)*

Figure 2: a) Centralized hierarchical structure; b) Failure isolation in homogeneously distributed networks.

Smartgrids design is likely to implement a structure with more homogeneous connected nodes (Figure 2b), capable to reroute power supply and isolate undamaged lines (Rosas I Casals, 2009).

2.3.2. Heterogeneity of elements and connections

Strong heterogeneity of elements and connections in current electricity grids, which will serve the foundation for Smartgrids, is translated into high sensitivity to direct attacks on a node or connection (Crucitti, 2003; Zio, 2007). The high vulnerability to direct attacks of scale-free networks can be smoothed by allocating supplemental connections and elements for a more homogeneously distributed architecture. In homogeneous networks, the networks' tolerance of errors is similar for the case of random failures and direct attacks, independent of network size (Rosas-Casals, Valverde, & Solé, 2007).

2.3.3. Self-similarities

Looking at fractal properties for engineering and non-engineering complex systems, it appears that it is not the presence of self-similarities, but rather their absence which may render Smartgrids vulnerable (Caldarelli, Marchetti, & Pietronero, 2000; Goldberger & West, 1987; Krummel et al., 2008; Song, Havlin, & Makse, 2006). For example, there are nearly no fractals in the current scale-free architecture of electricity grids connected with energy production to form the core production sub-system. In this setting, a direct attack on a production hub may result in the failure of the core production sub-system (Song, Havlin, & Makse, 2006). For this reason, Smartgrids are likely to seek fractal architectures, where consumers are regrouped around distributed production sources without strong connections with other production hubs. This needs to emerge from more sustainable evolution and growth mechanisms of the system (Song, Havlin, & Makse, 2006).

2.3.4. Self-organization and decomposability

By enabling 'disassembly' of a complex system into its subsystems and their components, decomposability allows understanding and categorization of system elements. Low decomposability

implies potential vulnerability as the system is characterized by massive elements with limited capacity for adaptation and evolution in response to nearly 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 Smartgrid, resulting in system stiffness and possible instabilities.

As for the self-organization process, its impact is significant in systems without central authority; for Smartgrids it may turn into vulnerability depending on the extent and type of active involvement of users.

2.3.5. Emergence

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, Wang, & Han, 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 I Casals, 2009). For Smartgrids, 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, emergence process driven in reasonable proportion between social participation and central authority will make Smartgrids more resilient to environmental changes without losing their functional capacity.

2.3.6. Adaptive learning

Adaptive learning is a challenge-response property which results from the tradeoff 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 exercise of the system's resilience and adaptation capacity. These raise the uncertainties in the level of extent of adaptive learning property in Smartgrids, as well as in the suitable functioning of its mechanism.

2.3.7. Evolution and growth mechanisms

Smartgrids may be exposed to vulnerabilities emerging from the growth mechanisms of the system. Restricted by technical constraints and transmission capacity, the extension of current electricity grids is done by preferential attachment, whereby highly connected nodes attract new links. This is a typical mechanism of growth of complex networks of different nature (Barabasi, Albert, & Jeong, 2000; Boccaletti, Latora, Y. Moreno, Chavez, & Hwang, 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 directed attacks and propagation of cascading failures. This means that 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, Havlin, & Makse, 2006). On the other hand, user involvement in the energy management process may cause drastic shifts in system evolution, leading to unexpected events and system vulnerabilities.

2.3.8. Chaos

The extent of system exposure to chaos is related to the level of influence of the controlling central authority. In the case of Smartgrids, chaos may arise mainly after the integration process, due to the influence of system-affecting non-engineering factors which are difficult to forecast and control, including social acceptance and participation. Given the nature of these factors, modeling scenarios of chaotic behavior at the design stage is a challenging forecasting problem of multidisciplinary

nature, since realistically the major interrelations among elements arise after system implementation.

2.1.9. Multidisciplinary relations

The nature and dynamics of multidisciplinary relations which will affect the Smartgrids life cycle are difficult to forecast and control, and the related uncertainties may hide potential vulnerabilities.

2.1.10. Vague boundaries

Imprecise definition of Smartgrid boundaries at the design stage driven by ‘preconceived’ engineering views on current energy challenges results in losses of information about the patterns of interconnections with influencing non-technical factors and their possible underestimation. Even in the case of well-engineered, smart electricity management, vulnerabilities in Smartgrid systems can arise if relevant influencing factors are neglected, e.g. social involvement and participation in the design and operation processes.

2.1.11. Self-healing and attacks resistance

These two properties were underlined as specific Smartgrids characteristics within adaptive learning and are considered as challenge-response characteristics. In the case of their strong influence, the adaptive learning property will dominate the evolution process and obstruct system upgrades, which will be restrictive for Smartgrids development. Therefore, these properties must be considered carefully.

2.4. Vulnerability ranking

Most of the complexity characteristics discussed in the previous Section are candidate sources of Smartgrid system vulnerability.. Their ranking with respect to their potential impact on the most valuable system resources and functionalities of electrical network is an objective of vulnerability assessment, because it can guide allocation and protection at the design and operation phases. However, at this stage of development of the Smartgrid concept, ranking vulnerabilities by the importance of their expected impact would be an unhelpfully abstract exercise. A preliminary

qualitative ranking could follow the categorization of Smartgrids complexity characteristics of Table 1 and their mapping into inherent, challenge-response and acquired categories, each of them related to the engineering, updating and integration processes of Smartgrids as complex engineered systems. The engineering process can be regarded as providing the designer with full control of a given Smartgrid's topological and behavioral properties. In this view, in this first category the characteristics manifesting vulnerabilities could be subordinated and their consequences reduced. In the updating process, the level of designer involvement is lower and the vulnerabilities to which Smartgrids may be exposed are more difficult to control and avoid, without intervening associated environments, e.g. social and economic contexts. The second category regroups vulnerabilities of more unforeseen character than at the engineering stage. The last category expresses the most uncertain characteristics of Smartgrids, capable of producing echo effects in different contexts with consequences which are difficult to predict. For this reason these characteristics are considered to potentially highly lead to vulnerable states of Smartgrid systems.

3. Methods of vulnerability analysis

This Section takes a comparative approach to exploration of options for modeling and analysis of the vulnerability characteristics of Smartgrid systems (Kroger & Zio, 2011). By taking into account the peculiarities of Smartgrid infrastructures, some methods regarded as most suitable have been selected. Obviously, statistical analysis of generation and failure records cannot be used at the current early stage of Smartgrid systems development to predict failures and time lapses between them. Also, the probabilistic analysis approach, used to model and predict the stochastic system state transition process may be difficult to pursue for such large systems with many multi-state components linked in complex patterns of interconnections.

The methods selected for the purposes of this paper's discussion are risk analysis, complex network theory and agent-based modeling and simulation (Table 2). The description of these approaches is organized as follows: for each method we supply a brief definition of the problem it addresses, and

analysis procedure and results are provided; finally, advantages and disadvantages for the analysis of Smartgrid systems are briefly discussed and synthesized in Table 2.

3.1. Risk analysis

Risk analysis of complex systems aims at the identification of vulnerabilities for complex systems, prioritizing them according to a combination of quantitative and qualitative indicators. The procedure for the analysis of network systems like Smartgrids is based on logical structural modeling by directed or undirected graphs and analysis of structural particularities under different uncertainty scenarios. Vulnerability ranking can be based on heuristic risk factors at the component level, which are the combination of complexity and severity indicators at the system level (Yacoub & Ammar, 2001).

The risk analysis framework is poorly suited to analysis of Smartgrids and large-scale electricity systems in general, which hold multidisciplinary connections and can experience a very large number of scenarios of uncertain occurrence, development and consequence. For this reason, application of risk analsys is limited to simplified case studies. Examples of suitable case studies include the analysis of the chaotic behavior of a complex industrial system in terms of stochastic variations in its technical parameters (Bruzzone, 2004) and the analysis of existing multidisciplinary relations in the context of project management environment (Biffl, Moser, & Winkler, 2010).

3.2. Complex network theory

Complex network theory provides a means for representing the inherent structural characteristics of large-scale networks (Boccaletti, Latora, Y. Moreno, Chavez, & Hwang, 2006). It also allows describing the architecture evolution and growth mechanisms (Song, Havlin, & Makse, 2006; Watts & Strogatz, 1998). Complex network theory also provides some connections to non-engineering domains, for example, by taking into account geographical and social constraints (Barth, 2010). In this view, most challenge-response and acquired characteristics are considered by this approach.

Yet, complex network theory can be used mostly for a preliminary vulnerability analysis limited to capturing the topological and behavioral bottlenecks of Smartgrids (Kroger & Zio, 2011). The approach consists in modeling by unweighted graphs the topological configuration of the network (Watts & Strogatz, 1998). For accounting of the electricity networks characteristics, weighted and planar graphs can be used (Boccaletti, Latora, Y. Moreno, Chavez, & Hwang, 2006). Weighted graphs allow including the heterogeneous characteristics of components and interconnections, while planar graphs enable introducing technical, social and geographical constraints in the analysis.

3.3. Agent-based modeling and simulation

The agent-based model and simulation approach allows, in principle, for accurate representation of complex dynamic systems. The agent-based method is capable of simulating almost all challenge-response and acquired characteristics of Smartgrids. Table 2 provides relevant examples of the diverse properties which can be simulated by agent-based methods. The integration of physical models for the representation of engineering and non-engineering factors with their complex relations, must be rendered computationally feasible in order to represent realistically the complex behaviors of large-scale systems in reasonable times (Kroger & Zio, 2011).

However, the accurate representation of multiple components and connections in multiple agents appears to be a complicated task, with a large number of parameters whose values need to be determined on the basis of data and information that may be unavailable for some components and connections. It is therefore expected that for Smartgrids, the agent-based approach can be used for studying only specific geographically limited areas of vulnerability in the system (Kroger & Zio, 2011).

Table 2.
Categorization of approaches for vulnerability assessment of Smartgrids

Characteristics/Analysis method		Risk analysis	Complex network theory	Agent-based modeling and simulation
Acquired	Self-organization and decomposability	No	No	Yes (Grimm & Railsback, 2006; Wolf, Holvoet, & Leuven, 2003)
	Emergence	No	No	Yes (Kroger & Zio, 2011; Schlapfer, Kessler, & Kroger, 2008)
	Chaos	Only for engineering analysis (Bruzzone, 2004)	No	Yes (Wolf, Holvoet, & Leuven, 2003)
	Multidisciplinary relations	In analysis of multi-disciplinary projects management (Biffl, Moser, & Winkler, 2010)	Partly with planar graphs (Barth, 2010; Waxman, 2002)	Yes (Grimm & Railsback, 2006; Schlapfer, Kessler, & Kroger, 2008)
	Vague boundaries	No	No	No
Challenge-response	Self-healing and attacks resistance	No	No	No
	Adaptive learning	No	No	Yes (Grimm & Railsback, 2006)
	Evolution and growth	No	Selective pressure and preferential attachment mechanism (Watts & Strogatz, 1998), hub repulsion growth (Song, Havlin, & Makse, 2006)	Yes (Mitchell & Newman, 2002)
Inherent	Architecture	Graph theory for complex systems modeling and further analysis with heuristic risk measures (Kroger & Zio, 2011; Yacoub & Ammar, 2001)	Generation of complex infrastructures with graphs theory (Boccaletti, Latora, Y. Moreno, Chavez, & Hwang, 2006; Watts & Strogatz, 1998)	Accurate and realistic simulation model of dynamic complex systems including physical laws (Kroger & Zio, 2011)
	Heterogeneity of elements and connections	Weighted graph concept (Wilson & Boyd, 2008)	Weighted graphs (Boccaletti, Latora, Y. Moreno, Chavez, & Hwang, 2006)	Explicit modeling of autonomous agents and their interactions
	Self-similarities	No	Kronecker product graph model (S. Moreno, Kirshner, Neville, & Vishwanathan, 2010)	Yes (Batty, 2007)

5. Conclusions

We have looked at Smartgrids from an original point of view of understanding their complexity. Topological and behavioral characteristics ‘typical’ of complex systems have been considered in the context of their instantiation in a typical or ideal Smartgrid. Further categorization of these characteristics has been made with regards to the engineering, updating and integration processes, which characterize a system life cycle. The indications that arise concern mainly the uncertain impact, that these complexity characteristics may have on Smartgrids vulnerabilities, and the possibility to foresee it, counteract and avoid vulnerability factors. System-acquired properties are considered most uncertain, and thus most difficult to control. Inherent characteristics, shaped mostly during design stage, do not pose particular vulnerabilities, and may be easier to avoid. Challenge-response properties occupy an intermediate position between inherent and acquired characteristics.

The analysis of the methods available for the vulnerability assessment of complex engineered systems has taken into account the ranking of Smartgrids vulnerabilities. Complex network theory seems suitable for preliminary analysis and identification of critical areas, with agent-based modeling following up as most adapted to the detailed study of the identified vulnerable zones.

References

Baas, A. C. W. (2002). Chaos, fractals and self-organization in coastal geomorphology : simulating dune landscapes in vegetated environments. *Geomorphology*, *48*, 309 - 328.

Barabasi, A., Albert, R., & Jeong, H. (2000). Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A: Statistical Mechanics and its Applications*, *281*(1-4), 69-77. doi: 10.1016/S0378-4371(00)00018-2.

Barth, M. (2010). Spatial networks. *Networks*, 1-86.

Battaglini, A., Lilliestam, J., Haas, A., & Patt, A. (2009). Development of SuperSmart Grids for a more efficient utilisation of electricity from renewable sources. *Journal of Cleaner Production*, *17*(10), 911-918. Elsevier Ltd. doi: 10.1016/j.jclepro.2009.02.006.

Batty, M. (2007). *Cities and complexity: Understanding cities with cellular automata, agent-based models, and fractals*. The MIT Press.

Biffl, S., Moser, T., & Winkler, D. (2010). Risk assessment in multi-disciplinary (software+) engineering projects. *Integration The Vlsi Journal*, 1-25.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D. (2006). Complex networks: Structure and dynamics. *Physics Reports*, *424*(4-5), 175-308. doi: 10.1016/j.physrep.2005.10.009.

Breuer, W., Povh, D., Retzmann, D., Urbanke, C., & Weinhold, M. (2007). Prospects of Smart Grid Technologies for a Sustainable and Secure Power Supply. *World Energy Council*. Rome, Italy. Retrieved from http://www.worldenergy.org/documents/p001546.pdf.

Bruzzone, A. G. (2004). Anticipating the chaotic behaviour of industrial systems based on stochastic, event-driven simulations. *AIP Conference Proceedings*, 557-565. Aip. doi: 10.1063/1.1787359.

Caldarelli, G., Marchetti, R., & Pietronero, L. (2000). The fractal properties of Internet. *Europhysics Letters (EPL)*, *52*(4), 386-391. doi: 10.1209/epl/i2000-00450-8.

Chassin, D. P. (2010). What Can the Smart Grid Do for You? And What Can You Do for the Smart Grid?. *The Electricity Journal*, *23*(5), 57-63. Elsevier Inc. doi: 10.1016/j.tej.2010.05.001.

Chen, L., Wang, X., & Han, Z. (2004). Controlling chaos in Internet congestion control model. *Chaos, Solitons & Fractals*, *21*(1), 81-91. doi: 10.1016/j.chaos.2003.09.037.

Coll-Mayor, D., Paget, M., & Lightner, E. (2007). Future intelligent power grids: Analysis of the vision in the European Union and the United States. *Energy Policy*, *35*(4), 2453-2465. doi: 10.1016/j.enpol.2006.09.001.

Crucitti, P. (2003). Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, *320*, 622-642. doi: 10.1016/S0378-4371(02)01545-5.

Culver, K., & Giudice, M. (2010). *Legality's Borders*. Oxford: Oxford University Press.

Duncan, G.-R. (2007). Mapping the Internet. *Technology Review*. Retrieved from http://www.technologyreview.com/printer_friendly_article.aspx?id=18944.

Fox-Penner, P. (2010). Smart Power. Climate change, the Smart Grid and the Future of Electric Utilities. Washington.

Goldberger, a L., & West, B. J. (1987). Fractals in physiology and medicine. *The Yale journal of biology and medicine*, *60*(5), 421-35.

Goldstein, J. (1999). Emergence as a construct: History and issues. *Emergence*, *1*(1), 49-72. doi: 10.1207/s15327000em0101_4.

Granic, I. (2000). The self-organization of the Internet and changing modes of thought. *New Ideas in Psychology*, *18*(1), 93-107. doi: 10.1016/S0732-118X(99)00039-2.

Grimm, V., & Railsback, S. F. (2006). Agent-based models in ecology: patterns and alternative theories of adaptive behaviour. In F. C. Billari, T. Fent, A. Prskawetz, & J. Scheffran (Eds.), *Agent-Based Computational Modelling* (pp. 139-152). Physica-Verlag HD.

Hammons, T. (2008). Integrating renewable energy sources into European grids. *International Journal of Electrical Power & Energy Systems*, *30*(8), 462-475. doi: 10.1016/j.ijepes.2008.04.010.

Hines, P., Blumsack, S., Cotilla Sanchez, E., & Barrows, C. (2010). The topological and electrical structure of power grids. *IEEE*.

Hledik, R. (2009). How Green Is the Smart Grid?. *The Electricity Journal*, *22*(3), 29-41. doi: 10.1016/j.tej.2009.03.001.

Kroger, W., & Zio, E. (2011). Vulnerable Systems. *Springer*.

Krummel, J. R., Gardner, R. H., Sugihara, G., Neill, R. V. O., Coleman, P. R., & Mar, N. (2008). Landscape patterns in a disturbed environment. *Oikos*, *48*(3), 321-324.

Lee, J. (1996). Applications of chaos and fractals in process systems engineering. *Journal of Process Control*, *6*(2-3), 71-87. doi: 10.1016/0959-1524(95)00051-8.

Lorenz, H. (1987). Strange attractors in a multisector business cycle model. *Journal of Economic Behavior* , *8*(3), 397-411. doi: 10.1016/0167-2681(87)90052-7.

Macek, W. M. (2010). Chaos and multifractals in the solar wind. *Advances in Space Research*, *46*(4), 526-531. doi: 10.1016/j.asr.2008.12.026.

Mandelbrot, B. B. (1982). *The fractal geometry of nature*. W.H. Freeman and Company.

Mitchell, M., & Newman, M. (2002). Complex systems theory and evolution. *Encyclopedia of Evolution*, 1-5.

Moreno, S., Kirshner, S., Neville, J., & Vishwanathan, S. V. N. (2010). *Tied kronecker product graph models to capture variance in network populations* (pp. 1 - 8). West Lafayette.

Nederbragt, H. (1997). Hierarchical organization of biological systems and the structure of adaptation in evolution and tumorigenesis. *Journal of theoretical biology*, *184*(2), 149-56. doi: 10.1006/jtbi.1996.0266.

NESCI. (2005). Visualizing complex system science (CSS). *New England Complex Systems Institute*. Retrieved from www.necsi.org/projects/mclemens/viscss.html.

OECD. (2008). The future of the internet economy. *Policy Brief*. Retrieved from http://www.oecd.org/dataoecd/20/41/40789235.pdf.

Ottino, J. M. (2004). Engineering complex systems. *Nature*, *427*(6973), 399. Retrieved from http://dx.doi.org/10.1038/427399a.

Pattee, H. H. (1973). *Hierarchy theory — the challenge of complex systems*. New York: George Braziller.

Rosas I Casals, M. (2009). *Topological complexity of the electricity transmission network. Implications in the sustainability paradigm. Language.*

Rosas-Casals, M., Valverde, S., & Solé, R. V. (2007). Topological vulnerability of the european power grid under errors and attacks. *International Journal of Bifurcation and Chaos*, *17*(07), 2465. doi: 10.1142/S0218127407018531.

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. doi: 10.1109/TSMCC.2003.813335.

Schlapfer, M., Kessler, T., & Kroger, W. (2008). Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. *16th Power Systems Computational Conference* (pp. 1-7). Glasgow.

Song, C., Havlin, S., & Makse, H. A. (2006). Origins of fractality in the growth of complex networks. *Nature Physics*, *2*(4), 275-281. doi: 10.1038/nphys266.

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of “small-world” networks. *Nature*, *393*(6684), 440-442. Retrieved from http://dx.doi.org/10.1038/30918.

Waxman, B. M. (2002). Routing of multipoint connections. *Institute of Electrical and Electronics Engineers*, *6*(9), 1617 - 1622.

Wilson, S., & Boyd, C. (2008). Structured assessment of complex systems. *Aerospace Conceots*, (1.8), 1-18.

Wolf, T. D., Holvoet, T., & Leuven, B.-H. (2003). Towards autonomic computing: agent-based modelling, dynamical systems analysis, and decentralised control. *IEEE International Conference on Industrial Informatics, 2003. INDIN 2003. Proceedings.*, 470-479. Ieee. doi: 10.1109/INDIN.2003.1300381.

Yacoub, S. M., & Ammar, H. H. (2001). A methodology for architectural-level reliability risk analysis. *IEEE Transactions on Software Engineering*, 1-37.

Zio, E. (2007). 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. doi: 10.1504/IJCIS.2007.014122.