Towards a Complex Networks Modeling of Interdependent Critical Infrastructures

Jose Sanchez Torres, Raphael Caire, Nouredine Hadjsaid

▶ **To cite this version:**

Jose Sanchez Torres, Raphael Caire, Nouredine Hadjsaid. Towards a Complex Networks Modeling of Interdependent Critical Infrastructures. Workshop Interdisciplinaire sur la Sécurité Globale - WISG 2013, Jan 2013, Troyes, France. hal-00780546

HAL Id: hal-00780546
https://hal.science/hal-00780546

Submitted on 24 Jan 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Towards a Complex Networks Modeling of Interdependent Critical Infrastructures

José SANCHEZ, Raphaël CAIRE, Nouredine HADJSAID
Grenoble INP/G2ELAB, ENSE3, Domaine Universitaire, BP 46, F-38402
Saint Martin d'Hères, France
Phone : +33 (0) 4.76.82.64.43
{jose.SANCHEZ, raphael.CAIRE, nouredine.HADJSAID}@g2elab.grenoble-inp

Résumé – La fiabilité et la sécurité des Infrastructures Critiques mettent l'accent sur la nécessité d'identifier et de comprendre les vulnérabilités qui émergent de l'interaction entre eux, notamment entre les systèmes TIC et les réseaux électriques. La modélisation des relations physiques, logiques et géographiques peuvent donner quelques informations sur les interactions entre les infrastructures pour éclairer leurs interdépendances et identifier leurs vulnérabilités. Cet article présente une méthode, developé dans le cadre du Projet SINARI, qui adapte la théorie des nombres complexes à la théorie des réseaux complexes. Le résultat de cette symbiose est un modèle qui permet d'identifier les vulnérabilités inhérentes des infrastructures couplés. La méthode est démontrée sur un réseau de distribution typique français, y compris un système TIC.

Abstract – Power Systems Reliability and Security highlight the need to identify and understand vulnerabilities that emerge from the interaction of two interdependent Critical Infrastructures: Information and Communication Technologies (ICT) and Power Systems. Modeling the physical, logical, cyber and geographical relations can give some information about the interactions between both infrastructures to enlighten their interdependencies and identify their mutual vulnerabilities. This paper presents a method, developed during the project SINARI, which adapts the theory of Complex Numbers to the theory of Complex Networks. The result of this symbiosis is a model that allows inherent vulnerabilities of coupled infrastructures to be identified. The method is demonstrated on a typical French Distribution Network including a surrounding ICT network.

1. Introduction

Systems are all around people, and each day the connections between them are getting increasingly complex. In fact, the world even depends on some of these systems for its survival [1]. Governments use the term "Critical Infrastructures" to refer to systems that are essential to the defense and economic security of their nations. The Commission of the European Communities identified 9 key Critical Infrastructures, including Energy networks, Information and Communication Technologies (ICT) and government national sites and monuments [2].

One important infrastructure concerns the Energy Network, which includes the production, refining, storage, and distribution of oil, gas, and electric power. However, this infrastructure integrates high-speed, reliable, bi-directional, and secure data communications networks. Particularly, Distribution Domain integrates external communication flows with control centers, electricity markets, transmission network, end-users, distributed storage, and distributed generation; and internal communication flows, i.e. between control, measure, and protection components. These interactions are presented in Fig. 1 [3]. This fusion of Power Grid with ICT has added complexity to an already complex field. Recent events [4]-[5] have shown that failures in one infrastructure can affect other infrastructures and that it is not possible to protect an infrastructure without identifying and understanding its vulnerabilities, i.e. multi-infrastructure threats. As a result, when talking about vulnerability studies in the Power Systems, one cannot consider a single system, but a system connected to other systems.

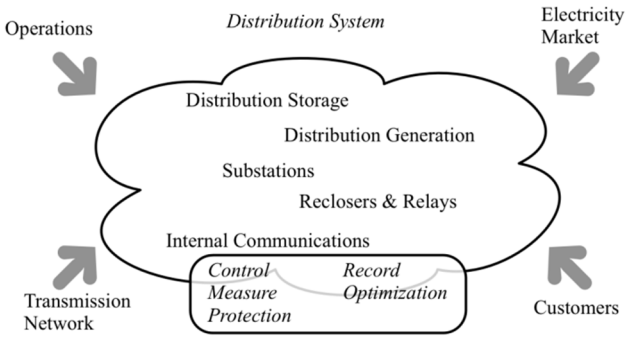

FIG. 1 : Distribution Domain (NIST Smart Grid Framework 1.0)

Although various researchers have studied multi-infrastructures vulnerability, those studies are still in an early stage and many questions remain unanswered [6]. For example, Petri Nets models [7] showed that, despite the stochastic analysis they perform, these models are impractical for large systems due to the great amount of manual effort and the lack of flexibility to evaluate different scenarios. Some of the unanswered questions also revolve around the mutual behavior of connected infrastructures; as most proposed methods evaluate only one infrastructure without taking into account explicitly the interactions and interdependencies with other infrastructures. This paper proposes to develop a

composite vulnerability model for the ICT or Cyber Infrastructure and the Power Systems Infrastructure using Complex Network Theory.

Complex Network is a new tool that allows modeling systems as graphs and has been extensively used to model, analyze, and understand large systems with non-trivial topologies and hidden interdependences [8]-[9]. This approach allows systems topology characteristics and connectivity properties to be known, as well as, fault and cascade phenomena analysis to be performed. This theory has been applied to analyze the vulnerability of Power Systems and Computer Networks [10]. Critical Infrastructures can be modeled as a Complex Network of systems functioning together to achieve common purposes. In order to elaborate a joint model, this paper proposes to adapt the theory of Complex Numbers to the theory of Complex Networks. The result of this symbiosis is a two-dimensional model, which allows inherent vulnerabilities of coupled infrastructures to be identified. Specifically, the proposed method bridges the Cyber Infrastructure and the Power Systems Infrastructure.

Section 2 presents an overview of Dependency and Vulnerability in Power Systems. Section 3 gives an introduction to Complex Networks and describes how the Complex Networks theory can be modified in order to introduce the Complex Numbers. Section 4 shows how this framework is applied to Power Systems. Finally, the conclusions are addressed in Section 5.

2. Dependency and Vulnerability

In order to identify, understand, and study vulnerabilities of Power Systems, it is important to know i) how the Power grid and the ICT inter-work; ii) the types of failures existing in both infrastructures; iii) the types of interdependencies; and iv) how these interdependencies affect the vulnerability of each infrastructure.

The main emphasis of Power Grids has been on providing a reliable, secure and economic supply of electrical energy to their customers. Control, protection, and monitoring systems are necessary for the Power Grid functioning. These systems are composed by ICT, which are defined as the technologies that involve acquiring, storing, processing, and distributing information by electronic means, including RTUs, IEDs, Computers, Servers, SCADA Systems, Routers, Gateways [11]-[12]. Therefore, there is a reciprocal relationship between both Infrastructures including two types of flows: energy and information. In one direction, Power Grid provides energy to ICTs; in the other direction, ICTs supervise, control, and manage the grid through commands and signals.

Three kinds of failures or outages can be found in Critical Infrastructures [1]:

1. Cascading failures: Occur when a failure in one infrastructure causes a failure in a second infrastructure.
2. Escalating failures: Occur when a failure, resulting from the interaction between two infrastructures, exacerbates another failure.
3. Common-cause failures: Occur when two or more infrastructures are affected simultaneously because of an external and common cause, e.g. tornado, earthquake.

Consequently, these failures show that the infrastructures are subjected to an increased risk from direct connectivity or spacial proximity, and that neighbor infrastructures are likely to be damaged after a single failure. In conclusion, Critical Infrastructures have strong interdependences, of which, there are four types: physical, cyber, geographic, and logical [1].

Finally, how can all these dependencies and failures affect the vulnerability of an infrastructure? That is the main and still unanswered question. Coupled infrastructures vulnerabilities are the exploitable weaknesses facing a defined threat. Such threat, from a cyber-security point of view, can be either internal, i.e. people working in the organization and that have physical access rights; or external, e.g. DoS attacks.

Therefore, Power System and ICT Vulnerabilities have common threats that exploit the weakest element in the Coupled infrastructures. The weakest element is identified by its importance in the system. A node is “important” regarding its role in the network, as in [6], the term ‘importance’ is intended to qualify the role that the presence and location of the node plays. There exist many methodologies in order to identify it, but they are made mostly for single infrastructures. However, our work with Complex Networks allows integrating both infrastructures in a single model, focusing on interdependencies and vulnerabilities that emerge from the interconnection of infrastructures.

3. Complex Networks

3.1 Methodology

A *Network* is a set of items with connections between them and a *Graph* is the network mathematical representation [13]. Networks are present in almost every aspect of life, e.g. traveling, calling by cell-phone, finding a job, chatting, etc. For this reason, mathematicians and experts in many domains have tried to find the best way to model real systems, considering the relations and dependencies between their components. Leonhard Euler solved the enigmatic seven bridges of Königsberg problem during the 18th century using what has been called the foundations of the Graph Theory.

Since its origin, the Graph Theory has been evolving thanks to the computerization of data acquisition and the availability of high computing power. Some of the main contributions include the Random Graphs Theory by Paul Erdös and Alfred Rényi in 1959 [14], the introduction of the `Small-World' Concept by Watts and Strogatz (WS) [15], and the discovery of `scale-free' characteristic in large

networks by Albert Barabasi [16]. The application of Graph theory to study large and complex systems is called Complex Networks theory. A complete overview of Complex Networks history is presented in [15] and [17].

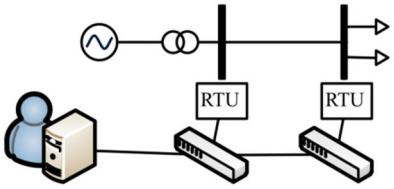

FIG. 2 : Example System

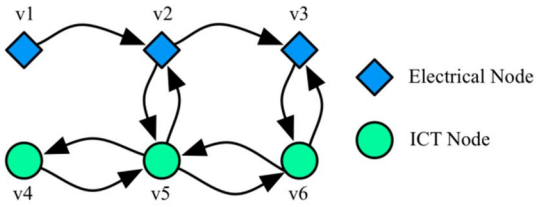

FIG. 3 : Example System Graph

Vertices and Edges compose Complex Networks. Vertices represent system elements such as buses, routers, airports or people. Edges represent the connections or relations between vertices; these connections can be physical, logical or functional. Some common edges include: power lines, optical fiber, flight itineraries, and friendship.

A graph G is a pair of sets (V,E). Where the elements of $V \equiv\{v_1, v_2, v_3,\ldots, v_n\}$ are the vertices or nodes and n is the number of vertices. While the elements of $E \equiv\{e_1, e_2, e_3,\ldots, e_m\}$ are the edges between the vertices and m is the number of edges.

A graph can be represented by a $n \times n$ matrix A, called adjacency matrix; where every row and column represents a vertex in the graph. Normally, its entry a_{hj} is 1 if the edge exists between the hth and jth vertices and 0 otherwise. However, in order to create a Complex Network for two infrastructures, this paper proposes to set the entry a_{hj} as a Complex Number (i.e. $1+1i$). The matrix A is constructed according to (1), with w the number of outbound links from node h to node j, and x the number of inbound links from node h to node j [18].

$$a_{hj} = w + i\,x \tag{1}$$

Since there are different layers in systems (electrical and ICT connections, logical and geographical dependencies), different adjacency matrices will represent each system. For example, Fig. 2 shows a basic electric grid and its ICT system. It is clear that there are many interdependencies between its components. For instance, Generation node supplies energy to loads, switches help to send and receive information from and to the control center, so electrical nodes depend on Control Centrer throught the ICT network. A single representation, as shown in Fig. 3, is not suitable to model all types of interdependencies. Therefore, this paper proposes to use multiple adjacency matrices. To show how to create these matrices, (2) and (3) show the adjacency matrices for the Electrical Layer and the ICT Layer shown in Fig. 4.

$$A_{elec} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ i & 0 & 1 & 0 & 1 & 0 \\ 0 & i & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 0 & 0 & 0 \end{bmatrix} \tag{2}$$

$$A_{ICT} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+i & 0 \\ 0 & 0 & 0 & 0 & 0 & 1+i \\ 0 & 0 & 0 & 0 & 1+i & 0 \\ 0 & 1+i & 0 & 1+i & 0 & 1+i \\ 0 & 0 & 1+i & 0 & 1+i & 0 \end{bmatrix} \tag{3}$$

Vulnerability assessment is a systematic evaluation in which quantitative or qualitative techniques are used to identify exploitable weaknesses in a system exposed to hazard. In order to do so, Power Grid and ICT infrastructures are modeled as Complex Networks using Complex Numbers. The assessed indexes are Node Degree and Efficiency. The higher the degree is (or lower the efficiency becomes), the more important the vertex in the system is. Then, an important vertex is highly vulnerable to a coordinated attack and/or a random failure.

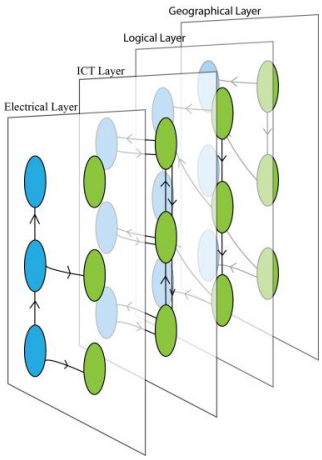

FIG. 4 : Multi-Layer Analysis

The importance or prestige (for Social Networks) of a node is characterized by the *node degree* (number of inbounds and outbounds connections). According to [8], the degree k_h of a node i is defined in terms of the adjacency matrix A as shown in (4).

$$k_h = \sum_{j \in V} a_{hj} \tag{4}$$

In the proposed method, the degree k_h is a complex number ($k_h = y + iz$) where y is the out-degree and z the in-degree. Results from the test case are shown in Table 1.

TAB. 1 : Node Degree results

Vertex	v_1	v_2	v_3	v_4	v_5	v_6
k_h Elec	*1*	*2+i*	*1+i*	*0*	*i*	*i*
k_h ICT	*0*	*1+i*	*1+i*	*1+i*	*3+3i*	*2+2i*

Another method to identify important nodes is the *Efficiency*. The concept of Efficiency was introduced in [19]. It is used to evaluate and measure how efficiently a node exchanges information with other nodes. The mathematical representation is in (5) and (6) for multi-infrastructures, where d_{hj} is the shortest path length between h and j.

$$E_c = \frac{1}{m_e m_c} \sum_{h \in V_c, j \in V_e, h \neq j} \frac{1}{d_{hj}} \quad (5)$$

$$E_e = \frac{1}{m_c m_e} \sum_{h \in V_e, j \in V_c, h \neq j} \frac{1}{d_{hj}} \quad (6)$$

m_e is the number of electrical edges, and m_c is the number of ICT edges. For the test case, presented in Fig. 2, Table 2 presents the efficiency of nodes.

TAB. 2 : Efficiency results

Vertex	v_1	v_2	v_3	v_4	v_5	v_6
E_e	*0,28*	*0,11*	*0,18*	*0,37*	*0,20*	*0,17*
E_c	*0,43*	*0,20*	*0,22*	*0,33*	*0,11*	*0,17*

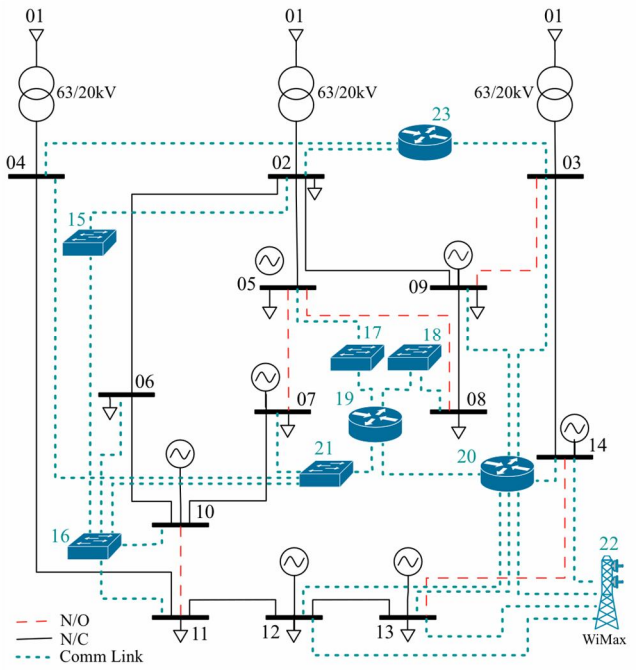

FIG. 5 : Power System and ICT networks

4. Test System and Results

4.1 Test System Description

The test system is a modification of the typical French Distribution Network presented in [20]. The Power Grid has 14 power-bus, 17 lines, 7 distributed generation, 9 loads, and 3 transformers HTB / HTA, as shown in Fig. 5. Aside from this network, there is a considerable supporting ICT infrastructure which involves 2 routers from a communication network of a public ICT provider (nodes 19 and 20) and 1 WiMax BS (node 22). It includes as well multiple links ADSL, PSTN / ISDN, Optic Fiber, and Ethernet technologies. Router 23 represents the private LAN-GigaEthernet connecting the electrical buses 2, 3 and 4.

4.2 Complex Network Modeling

To create the complex network, the power-bus, loads, routers and Wimax are considered as vertices; and the power-lines, communication links (ADSL, Ethernet, etc.) are considered as edges. Fig. 6 shows the resulting graph. Electrical nodes are numbered from 1 to 14 and ICT nodes from 15 to 22.

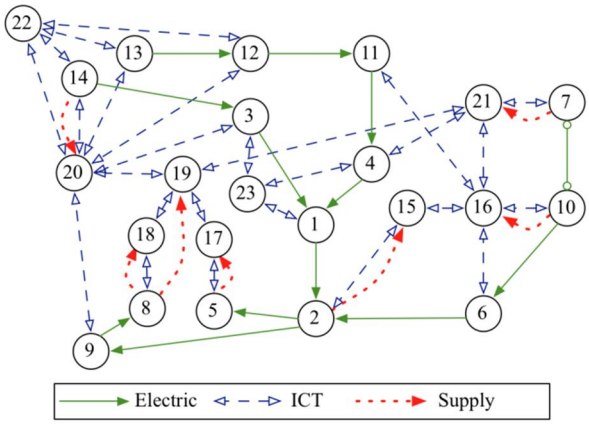

FIG. 6 : Graph

Tables 3 and 4 show the node degree and efficiency indices for the resulting graph. According to the tables nodes 2, 8 and 1 are the most critical for the Power System, and the failure consequences can be measured thanks to the node degree. For instance, to loose the node 2 means to loose 3 other nodes. However, it is more interesting the case of the set of nodes {8, 9, 19}, the three of them have a low efficiency index and the node 19 is supplied of energy from node 8, that depends on node 9 (source). Therefore, this method can help to identify important and critical elements on the coupled system, and to detect possible consequences.

TAB. 3 : Node Degree results

Vertex	k_h Elec	k_h ICT
1	*1 + 2i*	*0*
2	*3 + 2i*	*2 + 2i*
3	*1 + 1i*	*2 + 2i*
4	*1 + 1i*	*2 + 2i*
5	*1 + 1i*	*1 + 1i*
6	*1 + 1i*	*1 + 1i*
7	*1*	*1 + 1i*
8	*2 + 1i*	*1 + 1i*
9	*1 + 1i*	*1 + 1i*
10	*2*	*1 + 1i*
11	*1 + 1i*	*1 + 1i*
12	*1 + 1i*	*2 + 2i*
13	*1*	*2 + 2i*
14	*2*	*2 + 2i*
15	*0 + 1i*	*2 + 2i*
16	*0 + 1i*	*5 + 5i*
17	*0 + 1i*	*2 + 2i*
18	*0 + 1i*	*2 + 2i*
19	*0 + 1i*	*4 + 4i*
20	*0 + 1i*	*7 + 7i*
21	*0 + 1i*	*4 + 4i*
22	*0*	*4 + 4i*
23	*0*	*3 + 3i*

TAB. 4 : Efficiency results

Vertex	E_e	Ranking	E_c	Ranking
1	*0,0911*	*3*	*0,4062*	*23*
2	*0,0556*	*1*	*0,3729*	*15*
3	*0,1254*	*15*	*0,3639*	*9*
4	*0,1157*	*10*	*0,3688*	*11*
5	*0,1106*	*6*	*0,3792*	*22*
6	*0,1210*	*11*	*0,3782*	*18*
7	*0,1314*	*17*	*0,3751*	*16*
8	*0,0833*	*2*	*0,3792*	*21*
9	*0,0992*	*4*	*0,3762*	*17*
10	*0,1236*	*13*	*0,3782*	*20*
11	*0,1235*	*12*	*0,3782*	*19*
12	*0,1298*	*16*	*0,3722*	*13*
13	*0,1349*	*21*	*0,3722*	*14*
14	*0,1252*	*14*	*0,3722*	*12*
15	*0,1087*	*5*	*0,3669*	*10*
16	*0,1314*	*18*	*0,2943*	*3*
17	*0,1106*	*7*	*0,3505*	*5*
18	*0,1113*	*8*	*0,3505*	*6*
19	*0,1113*	*9*	*0,2664*	*2*
20	*0,1314*	*19*	*0,2482*	*1*
21	*0,1314*	*20*	*0,3087*	*4*
22	*0,1394*	*22*	*0,3598*	*8*
23	*0,1394*	*23*	*0,3573*	*7*

5. Conclusions

Vulnerability assessment for Critical infrastructures is an important task in order to guarantee the availability, reliability, and security. In order to do so, a new method to model Critical Infrastructures using Complex Networks have been presented. It shows a great flexibility and capability to perform vulnerability assessment for Power Systems.

The proposed method should serve to understand the interactions between different system components in a Power Systems, and to develop a risk analysis to identify ways to reduce the vulnerabilities. It will also help develop resilience studies, specifically in robustness, redundancy, and resourcefulness studies.

Modifications of this method can be made in order to model dependencies of different infrastructures, others than Power Grids and Cyber-systems. For instance, it can be applied to other Complex Networks parameters such as Centrality indexes, path length, clustering coefficient, or even to create dynamic multi-dimensional Complex Networks to model Cyber-attacks and their consequences. It could thus be extended to an *n* dimensional Complex Network to assess interactions between more than two infrastructures.

The significance of this paper lies in its ability to bridge two infrastructures in a single flexible model, which is an important step to study Critical Infrastructures vulnerability and to design safe and secure Power Systems, in this new era where utilities increasingly rely on the public Internet.

References

[1] S. Rinaldi, J. Peerenbon, and T. Kelly, "Indentifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11-25, 2001.

[2] Critical Infrastructure Protection in the Fight against terrorism, Commission of the European Communities, 2004, N°. 702.

[3] "NIST Framework and roadmap for smart grid interoperability standards," National Institute of Standards and Technology, Report 1108R2, Release 2.0, 2012. [Online]: http://www.nist.gov

[4] N. Falliere, L. Murchu, and E. Chien, "W32. Stuxnet dossier," *White paper 1.3*, Symantec Corp. Security Response, 2011.

[5] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope (v1.0)," ESET, pp. 1-85, Feb. 2011.

[6] W. Kröger, "Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools," *Reliability Engineering & System Safety*, vol. 93, no. 12, pp.1781-1787, 2008.

[7] C. Tranchita, N. Hadjsaid, M. Viziteu, B. Rozel and R. Caire, "ICT and power systems: An integrated

approach," in *Securing Electricity Supply in the cyber age*. Ed. Springer, 2010, ch. 5, pp. 71-109.
[8] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. Hwang, "Complex Networks: Structure and Dynamics," *Physics reports*, vol. 424, no. 4, pp. 484-499, dec 2006.
[9] R. Albert and A.-L Barabasi, "Statistical mechanics of Complex Networks," *Reviews on Modern Physics*, vo. 74, pp. 47-97, Jan 2002.
[10] W. Kröger, E. Zio, *Vulnerable Systems*, New York: Springer, 2011.
[11] T. Bjorn, M. Fontela, P. Mellstrand, R. Gustavsson, C. Andrieu, S. Bacha, N. Hadjsaid, and Y. Besanger, "Overview of ICT components and its applications in electric power systems," in *Proceeding of 2nd international Conference on Critical Infrastructures*, Grenoble, 2004.
[12] G. Ericsson, Å. Torkilseng, G. Dondossola, M. Tritschler and L. Piètre-Cambacédès, "Information security for Electric Power Utilities – results of Cigré WG D2.22," Proceedings of the 43rd CIGRE Session, Paris, France, Aug. 2010.
[13] M. Newman, "The Structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167-256, 2003.
[14] P. Erdös and A. Rényi, "On random graphs," *Publicationes Mathematicae Debrecen*, vol. 6, pp. 290-297, 1959.
[15] D. Watts and S. Strogatz, "Collective dynamics of 'Small-World' networks," *Nature*, vol. 393, pp. 440-442, 1998.
[16] A. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509-512, 1999.
[17] X. F. Wang and G. Chen, "Complex networks: Small-world, scale-free and beyond," *IEEE Circuits and Systems Magazine*, vol. 3, no. 1, pp. 6-20, 2003.
[18] Hoser, B. and Geyer-Schulz, A. "Eigenspectral Analysis of Hermitian Adjacency Matrices for the Analysis of Group Substructures," *Journal of Mathematical Sociology*, vol. 29, pp. 265-294, 2005.
[19] V. Latora, M. Marchiori, "Efficient behavior of small-world networks", *Physical Review Letters* vol. 87, 2001.
[20] B. Stahl, L. L. Thanh, R. Caire, and R. Gustavsson, "Experimenting with infrastructures," in *5th International CRIS Conference on Critical Infrastructures*, Beijing, 2010.