# Interdependencies of coupled heterogeneous infrastructures: the case of ICT and Energy

Nouredine Hadjsaid, Maria Viziteu, Benoît Rozel, Raphaël Caire, Jean-Claude Sabonnadière, Daniel Georges, Carolina Tranchita

# Interdependencies of coupled heterogeneous infrastructures: the case of ICT and Energy

N. Hadjsaid[1], M. Viziteu[2], B. Rozel[3], R. Caire[4], J-Cl. Sabonnadiere[5], D.Georges[6], C. Tranchita[7]

[1]*Grenoble Institute of Technology, Grenoble, France. E-mail:* ***nouredine.hadjsaid@g2elab.grenoble-inp.fr***
[2]*Grenoble Institute of Technology /Atos Origin, Grenoble, France. E-mail:* ***maria.viziteu@g2elab.grenoble-inp.fr***
[3]*Nice Sophia Antipolis University, Nice. France. E-mail:* ***benoit.rozel@unice.fr***
[4]*Grenoble Institute of Technology, Grenoble, France. E-mail:* ***raphael.caire@g2elab.grenoble-inp.fr***
[5]*Grenoble Institute of Technology, Grenoble, France. E-mail:* ***jean-claude.sabonnadiere@g2elab.grenoble-inp.fr***
[6]*Atos Origin, Grenoble, France. E-mail:* ***daniel.georges@atosorigin.com***
[7]*European Institute for Energy Research, Karlsruhe, Gremany,* ***carolina.tranchita@eifer.uni-karlsruhe.de***

ABSTRACT: Modern energy infrastructures and Information and Communication Technologies (ICT) are strongly coupled and as such heavily depend on each other. These infrastructures are essential for the proper functioning of our society and economies. Indeed, it is hard to imagine our present society without the services offered by these infrastructures. In addition, any failure of these infrastructures may cause significant economical losses. They are "critical infrastructures". Although, the energy and ICT infrastructures are heterogeneous in nature (different features, dynamics and communities), they need to be addressed in an integrated matter in the perspective of global infrastructures security. However, their interdependencies are not well known and significant efforts need to be dedicated for better understanding criticalities, vulnerabilities and cascading effects characterizing these strongly coupled heterogeneous infrastructures.

*Keywords*: critical infrastructures, ICT, energy, coupled behaviour, heterogeneity

## 1. INTRODUCTION

During more than a century of electricity, the society became more and more dependent on this infrastructure, evolution which caused gradual modifications of the system. Nowadays, electricity is vital to the contemporary society. The European Commission had declared the electrical power system a critical infrastructure (essential for the maintenance of vital societal functions, health, safety, and security, economic or social well-being of people) next to the telecommunication, oil, water, public health, transportation etc.

The continuous growth of the consumption and the highly refined demands of the electricity market have made the electrical power system more and more dependent on ICT services. It is a known fact that it is more interesting from financial point of view to invest in control mechanisms meant to maintain the electric parameters within their normal limits, than to invest in new electric infrastructure components. Also, as a direct consequence of the electricity market, the energy flows have to respect not only the physical laws, but also the contractual agreements. These requirements demand a reactive power system that guarantees economical performance.

The system, necessary to bring the electric energy to the end consumer, needs a lot more than electric components. Together with the classical electrical equipments (generators, substations, transmission lines), instrumentation, communication links, an information infrastructure and some specialized control centers are necessary to satisfy the generation—demand balance and the economic performance and ensure the quality of service and the functioning security [1]. Progress on ICT have been widely exploited in power systems, improving the quality of operations, making available data and specialized analysis and solving challenges for human related activities. ICT involve any communication device or application to acquire, store, process and distribute information by using electronic means. The term includes both traditional technologies as radio, television, print, video and newer technologies as Internet, among others.

The extensive ICT improve the operation of the power systems but they can also be subject to threats (both intentional and accidental) not fully understood, principally those originating from the interdependency of the power grid and the ICT.

GRID [2-4] is a consortium supported by the Trust and Security objective of the Information Society and Technologies Program of the 6$^{th}$ Framework. Its aim is to achieve a common strategy at European level concerning ICT vulnerabilities in power systems considering the transformation in the European power infrastructure. By using multiple methods including questionnaires, workshops and conferences and stakeholders consultations, GRID has identified the main research priorities for next decades. The main pillars that sustain the strategy for securing the critical infrastructures needed to provide the electricity to final customers: risk and vulnerability assessment tools and methods, control architectures and technologies and awareness and

governance of risk in society. The security assessment of power systems must take into consideration along with the intrinsic weaknesses of the multi-infrastructure system, cyber-security in order to satisfactorily deal with the economic and technical challenges faced by this type of system. At present, there is a lack of appropriate methodologies to assess impact of different scenarios and cyber-security related events frequency of critical equipment. Control architectures are far too complex and refined, so that full redesign investments would be too high. Efforts are presently focused towards understanding the interdependencies between the ICT and the power system in order to identify vulnerabilities and come up with suitable mitigations. Risk analysis taking into account the intrinsic vulnerabilities and the cyber-security aspects are considered priority areas for research. On the long run, the changes in the architecture of the power system and adjacent ICT will produce major mutations in the power sector. Appropriate methodologies of conception and implementation of security strategies, and correlated training will be required.

## 2. IMPROVING COMPREHENSION

In order to conceive and implement healthy strategies that will ensure a healthy evolution of the power system architecture and coupled ICT, a better comprehension of the inter-infrastructure phenomena and the vulnerabilities is necessary. Presently, there are very few appropriate methodologies to assess the impact of ICT failures on the behavior of electrical power system. The study of the interdependencies between the power network and the ICT infrastructure open new multidisciplinary research horizons.

The objectives of electric utilities are related to security, quality and economy [5]. Each one of these key points is unlikely to be reached without a continuous awareness of the different states of the power system. In order to reach end users, electrical power must be produced, transmitted and distributed through a large electric infrastructure. Local automation and communication devices are used to gather measurements and send them through a telecommunication infrastructure to a control center. The latter disposes of advanced software systems to process information and come up with coherent reactions to keep the electric parameters within nominal ranges.

The electrical infrastructure is heavily dependent on the ICS (the Information and Communication System of the power system) for its operation in both normal operating conditions and critical conditions, such as peak load or network restoration after a blackout. Conversely, all components used by the ICS need to be supplied with electric power. During a power outage, only devices equipped with Uninterruptible Power Supply (UPS) will be likely to operate. As these power interruptions/situations are relatively exceptional at present, these systems will not be all available when a failure occurs. Consequently, if the outage lasts several hours, the batteries will gradually run out as occurred during the 2003 Italian blackout [6]. Indeed, the design of UPS is not based on actual costs of non-functioning of equipment supplied, but rather according to their perceived importance which is generally underestimated. This underestimation arises because only first order consequences are generally considered and consequences of higher orders (i.e. due to the effects of the first consequences and combined with the initial cause of the interruption) are taken into account at a lower importance at best, or neglected at worst. It appears that the electrical infrastructure depends on the information flow and the ICS depends on the availability of electricity. These two coupled phenomena, for which the dependency relationships are very nonlinear and strongly coupled, produce interdependencies that are very difficult to capture and analyze.

Improving comprehension relies on modeling principles that allow quantifying the interdependencies between these critical infrastructures. This would lead to identifying critical vulnerabilities and suitable mitigations

### *2.1 Heterogeneity*

In order to improve comprehension, studies are needed to be made in research conditions. This demands a scale-representation of the large system made of interdependent infrastructures and implies building a model of the studied system.

Modeling critical infrastructure interdependencies is not trivial and the difficulty of the task combined with the variety of possible goals (securing one infrastructure or all, minimizing financial cost) requires the use of different approaches that may be simulation based or theoretical, of an expanded level (national, continental) or at a reduced level (metropolitan with a possible integration of the human factor).

One of the major difficulties in the modeling of infrastructures interdependencies lies in the deep heterogeneity of the interdependent infrastructures.

From a physical phenomena point of view, the infrastructure, consisting of the power system and adjacent ICT, holds electric phenomena, thermal phenomena, electromagnetic phenomena and wave propagation, among other. The coherent functioning of such a multi-physic system raises reliability problems, security problems, electromagnetic compatibility problems, and a lot more. Added to all that, the interaction with software raises a new class of problems that aren’t part of any physical phenomenon taxonomy.

From a systems theory point of view, there are 3 main components necessary to deliver energy from generation to consumption:
- The electric network, with a behavior characterized by differential equations is a continuous system;
- The telecommunication network, with a behavior characterized by events is a discrete system and;
- The control center, which provides different commands according to each circumstance, is an expert system with human in the loop.

From reliability point of view, material faults and software faults are different notions and have different origins. The first ones are caused by natural hazard, conception error or usage. The second ones are caused by human errors. The most common mitigation for damaging events is ensuring redundancy. This consists of doubling the critical components. When referring to physical equipment, redundancy is ensured by identical components. When referring to software, classical redundancy has not reveal good results, as the input data that caused the fault to the main algorithm, will cause the exact same fault to its double [7].

### *2.2. Modelling methods*

Available literature present techniques of social networks and reliability modeling and the modeling based supply-demand graphs [8-11]. It exist also modeling and simulation approaches of critical infra-structures based on a Geographic Information System (GIS) [12-13]. The inconvenient to use this last approach is that accurate and complete data on the studied zone is necessary. Besides, the zone's size is limited and in the case of real large critical infrastructures, e.g. at the continental scale, the modeling by this method becomes not easy.

The use of a database on accidents affecting critical infrastructures to enhance their vulnerabilities and interdependencies is presented in [14]. The approach can be useful to determine the most frequent or most severe vulnerabilities and by consequence to reduce them. However, because this method is based on historical data, new vulnerabilities cannot be identified.

In [15], modeling of critical infrastructures is coupled with a genetic algorithm for the purpose of infrastructure planning. A study of the propagation of failures in critical infrastructures is made in [16] using the theory of fuzzy sets to quantify the links of failure propagation between infrastructures. Presently, it is difficult to foresee the usefulness of this approach on large systems, as a very simple case was only studied.

Finally, two other approaches are described in the following sections: the use of the theory of complex networks and the behavioral simulation of infrastructures. The theory of complex networks is a new field applied to many different infrastructures and can be helpful at the time to analyze large interconnected systems. Behavioral simulation is a time dependent simulation of the studied infrastructures.

## 3. COMPLEX SYSTEMS

The large-scale interconnected electricity systems have grown into one of the most complex man-made technological networks in this era. The nodes and edges of the power grid increase almost every year, and the interaction of the components in power systems become more and more complex [17].

Complex Network Theory, in which the vertices represent the elements of a system, and the edges stand for the physical or logical interaction between different elements, is a powerful tool. With the development of modern statistical physics theory and computing technology, it has become possible to quantitatively study the topological and dynamical properties of large networks that can be mapped into various real systems. Traditionally the research on complex network has been the territory of graph theory. With the emergence of large databases increased computing power and the breakdown of boundaries between disciplines, complex network theory achieves a tremendous development. Many new concepts and measures have been proposed and investigated in depth for real-world complex networks.

Methods for graph partitioning allow researchers, for instance, to find the weak arcs in a graph, or more precisely, the arcs that are the most involved in holding the graph together, arcs without which the graph would break into different areas. If the studied graph models a real network, it becomes possible to evaluate the weak connections between different regional networks. Using this method for a critical infrastructure, such as an electrical grid, can give information about the critical lines that can be used for better load forecasting of potential load cascading - when large unbalances of load are found between different network areas. Moreover, the graph partitioning methods will reveal the potential island areas. This study leads to mitigations for avoiding large scale black-outs. It is based on topological data of the actual UCTE network (zone 1). The resulted information indicates the weak arcs where building new lines or taking certain countermeasures may help the independent sub-networks to successfully resist a long range of disturbances.

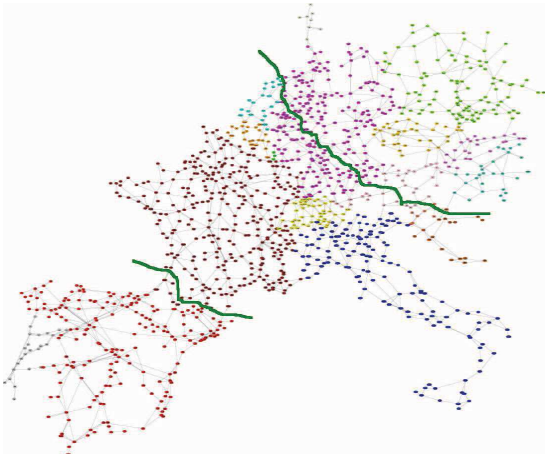

Fig. 1: Second cut of the UCTE network [18]

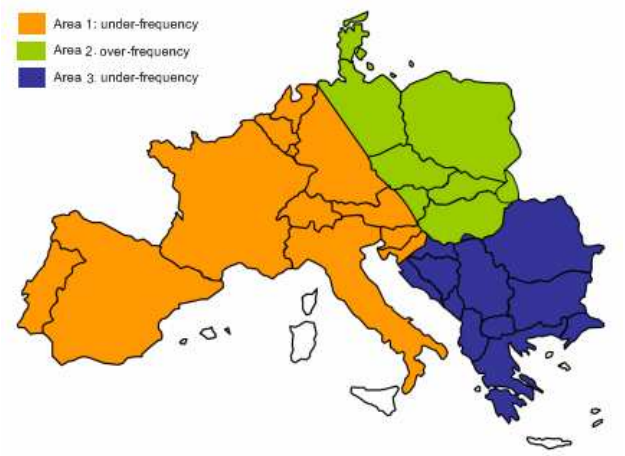


Fig. 2: Areas resulted after the 4th of November blackout of the UCTE network (credits www.ucte.org)

The graph partitioning algorithm was used to identify a different number of possible cuts in the UCTE network. Analyzing the possibility of breaking the UCTE network into 2 areas revealed a well known vulnerability corresponding almost to the interconnection lines between France and its eastern neighbors. The most interesting results were revealed by the second cut, corresponding to the break of the UCTE in 3 areas. The partitions presented in Fig. 1 correspond to the real separation of the electrical network that occurred due to the massive blackout in 2006, on 4th of November [19] as seen in Fig. 2. Our program found a second cut, between Spain and France, which may did not happen, maybe thanks to the decisive actions of Spanish operators.

## 4. MULTI-INFRASTRUCTURE OBSERVATORY

The idea of a multi-infrastructure observatory departed from the criticality theory. Classical approaches look for key components whose faults have intolerable impacts and reduce their fault frequency to zero, if possible. Criticality is dependent of a factor that quantifies the monitoring capacities and it is based on a preventive approach. The idea is to have a tool able to show the global state of a multi-infrastructure system on real-time basis. The main advantage would be that an operator would have the information of a damaging state of an interconnected infrastructure in due time, so that he could diminish the impact on the service he is providing. Such a tool could also be used for off-line analysis for inter-infrastructure studies. It implies a non-empirical severity metrics and it can illustrate more refined vulnerabilities For instance: which telecommunication component should be changed/ upgraded from a given architecture, so that the operability would not diminish in severe states of the electric network. Or, how do the performances and the frequency of the call of advanced algorithms in the control center can influence the service provided by the electric utility.

This goal is to be achieved in several phases. Presently, a prototype is developed in research conditions. It is based on a coupled simulator [20] that takes into consideration the electric network, the telecommunication network and the corresponding control center. In order to better understand the cascade mechanisms, in this phase, maximum observability is assumed for each infrastructure.

In [21], authors present a survey, listing the projects developed in Europe and the US meant to virtually simulate the interactions between critical infrastructures. Among thirty listed simulators, only five of them take into consideration the electrical power grid and the ICT infrastructures. G2Elab, within the Grenoble Institute of Technology, is one of the laboratories that have developed a behavioral simulator for inter-infrastructure studies [20]. In order to build a robust tool to illustrate the behavior of a multi-infrastructure system, the following steps have been pursued. The first one consisted of identifying the major mechanisms of the interdependencies and the mathematical behavior of the studied subsystems. These observations helped to choose the suitable tools able to simulate the behavior of each individual infrastructure with appropriate models (in a validity domain point of view), which was the second step of the approach. The third phase was to build the combined simulator: a coupling of individual specialized simulation tools with inter-process communication principles. A last step was essential for creating the inter-infrastructure simulation and it consisted in building a multi-infrastructure benchmark.

The focus of the study is the power grid and its initial purpose was to better illustrate its interactions with the ICT infrastructure. As described in previous sections, the interdependencies between the electric network and the ICT infrastructure are caused

mainly by two types of flows: energy and information. The electric network depends on the data flowing through the telecommunication infrastructure and the commands received from the control center. The focus was mainly on the phenomena caused by information interdependencies. This type of simulator can be used for different inter-infrastructure studies. The first version could mainly be employed to quantify the impact of various scenarios on electric network and its ICT operation infrastructure. The events that can be simulated include load variations associated with contingencies in the electric network and also failures in the telecommunication infrastructure or even breakdown of the control center.

This behavioral simulator was enriched with early detection of blackouts mechanisms for the power network and other synthetic state metrics and quality of service for ICT. Data characterizing the state of each infrastructure is centralized and analyzed by the multi-infrastructure observatory.

This approach descends to a more detailed level of the multi-infrastructure system and can illustrate more refined interdependencies. The main difficulty is that it implies knowledge from power system, computer science, software reliability and integrating this knowledge implies the collaboration of different experts. Also, as input data is richer than in the complex system approach, studies for large and very large scale system would be a lot more time consuming.

## 5. CONCLUSIONS

After more than a century of electricity usage, and within the era of Internet, it is unacceptable to live without electrical energy and to experience any media interruption. The consequences of a generalized incident, or blackout, either from natural origin, assets' failures or malicious attack are dramatic both economically and socially.

Present power systems are heavily dependent on ICT at various levels from measurement/bay level to control centers with its related communication and information exchange with market places and other control systems (neighboring systems). Indeed, they are used for gathering information as well as for issuing control actions that are vital for the system survivability. In addition, effective integration of ICT in power system can lead to more optimized operation and better control of these systems thus increasing efficiency. Moreover, ICT are key components and functions in the ongoing research and development of "SmartGrids". However, ICS and power systems have evolved differently and are considered by different communities. Hence, the integration of ICS in power systems is mostly carried out in layer shape structure (adding the ICT infrastructure once the electrical infrastructure is already built). These infrastructures were planned almost independently. Nevertheless, these infrastructures are heavily dependent on each other. With liberalization and the following responsibility partitioning between the various actors, the interdependencies of these infrastructures are becoming more and more critical. This is why, the power system and the ICT communities should strengthen communication and know-how passing methods in order to come up with systemic solutions and service oriented infrastructures that consider all the concerned networks.

On the long term, the power infrastructure's societal, organizational and human dimension will have to embrace a culture of security that will concern physical and ICT components of the systems.

## 6. REFERENCES


[1] D., Kirschen; F., Bouffard (2009). Keeping the lights on and the information flowing, IEEE power & energy magazine, PAE M Jan-Feb, page(s) 50-60

[2] A., Stefanini; R.M., Gardner; N., Hadjsaid; J.P., Rognon (2007). A Survey on ICT Vulnerabilities of Power Systems, European CIIP Newsletter, European Commission IRRIIS Project, contract no 027568, WEB-Publication, January / February 2007, Volume 3, Number 1, page(s) 6 - 8.

[3] R.M., Gardner; The GRID Consortium (2007). A Survey of ICT Vulnerabilities of Power Systems and Relevant Defense Methodologies, IEEE Power Engineering Society General Meeting, Tampa, Florida, USA

[4] GRID consortium (2007). ICT vulnerabilities of Power Systems: A Roadmap for Future Research, December 2007, European Communities, ISBN 978-92-79-07138-6

[5] P., Kundur (1993). Power system stability and control, EPRI Editors and McGraw-Hill

[6] UCTE (2003), Interim Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, online available at http://www.ucte.org, consulted in April 2009

[7] Olivier, Gaudoin ; James, Ledoux (2007). Modélisation aléatoire en fiabilité des logiciels, Hermès science publications Lavoisier, Paris, France

[8] H.M., Kim; M., Biehl; J.A., Buzacott (2005). M-ci2: Modeling cyber interdependencies between critical infrastructures, The 3rd IEEE Conference on Industrial Informatics

[9] E. E., Lee; D. J., Mendonça; J. E., Mitchell; W. A., Wallace (2003) Restoration of services in inter-dependent infrastructure systems: a network flows approach. Technical Report 38-03-507, Rensselaer Polytechnic Institute, USA

[10] E. E., Lee; J. E., Mitchell; W. A., Wallace (2004). Assessing vulnerability of proposed designs for interdependent infrastructure systems. The 37th Hawaii Conference on System Sciences, Hawaii, USA

[11] E. E., Lee; J. E., Mitchell; W. A., Wallace (2005). Restoration of services in interdependent infra-structure systems: A network flows approach. IEEE Transactions on Systems, Man, and Cy-bernetics, 37(6):1303–1317
[12] S. D., Wolthusen (2005). GIS-based command and control infrastructure for critical infrastructure protection. First Workshop on Critical Infrastructure Protection, Darmstadt, Germany
[13] C.W., Johnson; R., Williams (2008). Computational support for identifying safety and security related dependencies between national critical infrastructures. The 3rd IET International Conference on System Safety, Birmingham, UK
[14] R., Zimmerman (2004). Decision-making and the vulnerability of interdependent critical infrastructures. IEEE Conference on Systems, Man and Cybernetics, Singapore, Singapore
[15] M.R., Permann (2007). Toward developing genetic algorithms to aid in critical infrastructure modeling. IEEE Conference on Technologies for Homeland Security, Woburn, USA
[16] S., Panzieri; R.; Setola (2008). Failures propagation in critical interdependent infrastructures. International Journal of Modeling, Identification and Control, Volume 3, Issue 1, page(s) 69-78
[17] A.M., Wildberger (1997). Complex adaptive systems: concepts and power industry applications, Control Systems Magazine, IEEE Dec 1997, Volume: 17, Issue: 6, page(s): 77-88.
[18] B., Rozel; R., Caire; N., Hadjsaid; J.-P, Rognon; C., Tranchita (2009). Complex network theory and graph partitioning : Application to large interconnected networks. IEEE PowerTech 2009, Bucharest, Romania
[19] UCTE (2007). Final Report – System Disturbance on 4 November 2006, Union for the Co-ordination of Transmission of Electricity
[20] B., Rozel; M., Viziteu; R., Caire; N., Hadjsaid; J.P., Rognon (2008). Towards a common model for studying critical infrastructure interdependencies. IEEE Power and Energy Society General Meeting, Pittsburgh, USA
[21] P., Pederson; M., Permann (2006). Interdependency Modeling: A Survey of U.S. and International Research, Idaho National Laboratory report INL/EXT-06-11464, Idaho, USA
[22] European Commission (2008), COUNCIL DIRECTIVE on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, 10934/08