Interdependent Behavior of Critical Infrastructures

Nouredine Hadjsaid, Maria Viziteu, Raphaël Caire, Daniel Georges

Interdependent Behavior of Critical Infrastructures

Nouredine Hadjsaid, Maria Viziteu, Raphael Caire, Daniel Georges

***Abstract*— During the last decade, an increasing incorporation of Information and Communication Technologies (ICT) into the power systems has been evidenced. ICT have enabled the improvement of the power grid control and by consequence the reliability and the flexibility of these systems. Presently, ICT are a key aspect in the smart grids development. Today's power systems depend on ICT. However, these technologies can fail and are also exposed to threats that can affect their functioning and the operation of the power system. Therefore, it is very important to consider both interconnected infrastructures (electrical power grid and its information and communication system (ICS)) in the modeling, design and security analysis of electrical power systems. In this paper, we present simulation results illustrating correlations between the electric network state and the ICS state.**

***Index Terms*—critical infrastructures interdependencies, coupled simulation, quality of service**

I. INTRODUCTION

The main objective of power systems is to deliver electrical energy, that is not storable, to final customers on very large areas, where and when this power is required. A large amount of tasks and operations are needed in order to permanently assure a reliable service at the lowest cost. The electrical power network control requires precise coordination in the operation executions. Transactions on the market, load and generation profile, assets upgrades, maintenance and security needs lead to configuration changes of networks.

Power systems are geographically dispersed and have been extended, for reasons of economic profit, through the interconnection of local, national and international utilities. This interconnection requires the sharing and the coordination of basic tasks (such as maintenance programming, control and coordination for emergency situations) among producers, operators and customers which act on the power network in physically isolated places [1]. Additionally, due to the electrical market deregulation, convergence of the participants' information is necessary to reach a global optimal performance of the system.

On one hand, electrical power systems are faced continuously with a series of events which can affect their integrity and operation. The system itself and the operators must cope with these hazards in order to preserve the systems' security. On the other hand, the disparity between growth of electrical demand and investments in the electrical infrastructure leads to systems operating close to their limits, diminishing conservative security margins. Due to this complex situation, a large amount of communication electronic devices are distributed in electrical power systems to control, protect and supervise their functioning. Power systems are for the most part remotely controlled.

Evolutions in ICT have been widely exploited in power systems, improving the quality of operations, allowing automations, enabling a better remote control , creating a fast management system, making data available for specialized analysis. ICT require any communication device or application to acquire, store, process and distribute information by using electronic means. This includes both traditional technologies such as radio, television, print, video and newer technologies such as Internet, among others.

ICS (which are composed of different ICT , each having a specific objective) such as the ones used in power systems, are complex and large. Complexity arises because devices are very heterogeneous and extensively networked with different internal and external systems. Moreover, even if assets dedicated to control and protection had (in most cases) high advanced functionality, some networks also still depend on the human organization [2]. ICS of power systems, such as the ones used in energy control centers and corporate computer's networks, are generally secured. Nevertheless, because of complexity and size, numerous access points can be exploited by attackers in many different ways. Thus, ICS are vulnerable to cyber attacks that can restrain their operation, corrupt important data, or expose private information. In addition, cyber and physical natural failures in ICT may also occur and induce faults in the ICS that could affect the whole power system behavior.

Presently power systems are highly connected and highly interdependent to other critical infrastructures [3]. This interconnectivity has increased efficiency but has also introduced more vulnerability into the system. Failures and attacks on ICT can affect not only the ICS but the concerned power system and other interconnected critical infrastructures. Severity of the events could then be more significant due to a domino effect between infrastructures.

In this context, the security assessment is more vital than ever for the correct operation of power systems. Security is the ability of a power system to withstand sudden disturbances without service interruption [4]. New methods of security assessment are needed to respond to new potential disturbances arising from failures of ICT, increased control complexity and malicious threats to which a power system is exposed.

Research must focus on scalable models and simulation tools to perform risk analysis to power system operation and

integrity, showing up consequences of potential failures. Two main challenges take place to achieve such analysis; the first one in understanding the interactions between the ICS and the physical power grid ; the second one in determining the criticality of the information, IC functions or IC assets, which are crucial to the operation of the power system. Some experts [5, 6] stated that one of the most frequently identified shortfalls in knowledge related to enhancing critical infrastructure protection capabilities, is the incomplete understanding of interdependencies between infrastructures. Interdependency' modeling is the first stage to respond to many queries about the real vulnerability of infrastructures. To have a complete understanding between the ICT behavior and the power grid operation, modeling is required.

This paper summarizes aspects of ICT involved in power systems operation and their relationship with other important concepts such as the "traditional" power system security and cyber security. Different efforts have been made in the area of infrastructure interdependency modeling, risk assessment and vulnerability analysis. In that sense, the objective of this paper is to provide some approaches developed in the Grenoble Institute of Technology and G2ELab (France), on the interdependency modeling between the Information and Communication System (ICS) and the Electrical Infrastructure. Since in traditional security assessment methods, only failures coming from electrical power grids are covered, new considerations in security analyses are proposed for dealing with cyber attacks and ICT failures.

II. ICT FOR POWER SYSTEMS

In order to reach end users, electrical power must be produced, transmitted and distributed through a large electric infrastructure. The objectives of electric utilities are related to security, quality and economy [7]. Each one of these key points is unlikely to be reached without a continuous awareness of the different states of the power system. This is why, 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.

Traditionally, electrical utilities carry out their operation as well as planning and maintenance tasks by using ICS, which enables the flow of information at different levels of the power system. The ICS is generally composed of three networks: a) regular networks including public switched telephone and data networks; b) wireless networks with cellular phones and wireless ATM (Asynchronous Transfer Mode); c) computing networks including different dedicated LANs, WANs and the internet [1]. Before explaining the different technologies employed at the different levels in the power system, generalities of ICT are detailed.

ICT designate the essential resources, such as computers, programs and communication networks, needed to handle information,. These resources are necessary for converting, storing, managing, transmiting and finding information. The present denomination of ICT in the engineering domain indicates everything that concerns the technologies (and techniques) used in the treatment and the transmission of information, mainly data processing and telecommunications. More accurately, Information and Communication Technology was defined by [8], as follows:

"The technology involved acquiring, storing, processing and distributing information by electronics means (including radio, television, telephone, and computers)".

Information acquisition, communication of the information between different entities and information computerization (including information analysis, storing and visualization) are the different processes identified, see Fig. 1.

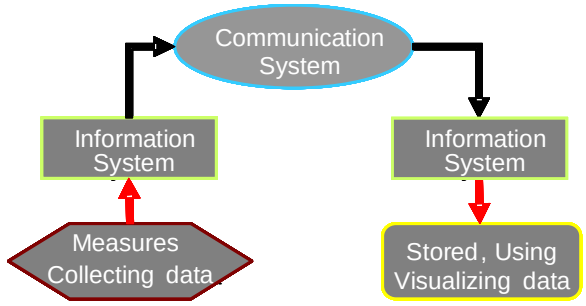

Fig. 1. Information and Communication System. Source [8]

Usually, it is difficult to define a border between the information system and the communication system because both are related very closely. Communication is defined as the action to transmit information between two or more points/agents of the system. The ICS obtains measures, of the physical phenomena, that are needed for specialized functions of control/protection/management. Once the information exists, it is converted to an analogical or digital signal. Thus, the communication system carries the signal from the measurement point to other(s) by using a communication media. A receiver gets the signal and converts it back into usable information. The communication process then finishes when this information is stored. Computerization is the use of the information with specialized functions for analysis or decision making. The information system is frequently referred only to computers. This last system concerns application software as programs and operating systems that can be applied in a computer, PLC or a control unit to store data, handle large amounts of information, perform complex computations, and control processes

III. MODELING INTERDEPENDENCIES BETWEEN THE ICS AND ELECTRICAL INFRASTRUCTURE OF A POWER SYSTEM

The electrical infrastructure is heavily dependent on the ICS for its operation in both normal operating conditions and critical conditions, such as peak load or network restoration after a blackout (blackstart). 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. 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.

As well as power systems, telecommunications and information networks have become critical for the functioning of modern societies. It becomes increasingly difficult to accept failures, even for a short time, on any one of these infrastructures. When this happens it can be at the expense of human lives - e.g. due to a traffic accident caused by the nonfunctioning of traffic lights at intersections in case of power failure or by an inability to contact emergency services in case of overloading of the telecommunications infrastructure. In order to avoid the occurrence of such consequences which can be even more devastating in cases of natural disasters, it is necessary to better understand these phenomena of interdependencies between the ICS and the electrical infrastructure. As this interdependencies are primarily physical, better understanding can be achieved through modeling. The modeling of interdependencies between critical infrastructures is the first step towards securing the systems involved and therefore protecting basic services that save lives. This step is not trivial and the difficulty of the task (due to the aforementioned complexity) combined with the variety of possible goals (minimizing deaths or financial cost, securing one infrastructure or all) requires the use of different approaches that may be theoretical or simulation based, of a high level (throughout a country) or at a local level (on the scale of a city with the integrating of the human factor).

One of the major difficulties in the modeling of infrastructures interdependencies lies in the deep heterogeneity of the systems mathematical behavior. From a systems theory point of view, there were identified 3 main components necessary to deliver energy from generation points to consumption points:

1. The electric network, with a behavior characterized by differential equations (a continuous subsystem).
2. The telecommunication network, with a behavior characterized by events (a discrete subsystem) and
3. The control center, which provides different commands according to each circumstance and behaves as an expert system with a human in the loop.

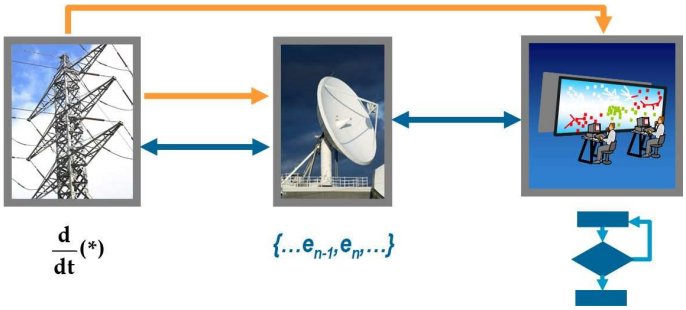

Fig. 2. Heterogeneous components of a power system and their typical modeling.

IV. Multi-infrastructure Simulator for Interdependencies Studies

In [9], 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, at the Grenoble Institute of Technology, is one of the few laboratories that have developed a combined simulator for inter-infrastructure studies [10]. This section details the main steps and the methodology used to build a combined simulator that models both an electrical power network and the corresponding ICT infrastructure needed to monitor and to control it.

The focus of the study is the power grid and the purpose is to better understand its interactions with the ICT infrastructure. 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 is then mainly on the phenomena caused by information interdependencies.

As it was mentioned, the difficulty in modelling these infrastructures interdependencies rests in the deep heterogeneity of their mathematical behavior. A coupled simulator has to be able to show the interactions between the three families of components of a power system. The choice was made to use single infrastructure simulators and connect them together in one unitary tool.

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 main 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 compliant 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 simulation tools with inter-process communication principles. A fourth step was essential for creating the inter-infrastructure simulation and it consisted in building a multi-infrastructure benchmark. Simulations in different scenarios were run and the final tool was validated using behavior principles.

A. *The electric network/ infrastructure*

The purpose of this section is to illustrate scenarios inspired by real blackouts where medium/long term stability aspects (lasting from minute up to one day) were mainly taken into account. Thus, the level of simulated details does not reach electromagnetic transient phenomena.

A time-domain simulation software (PSAT) was chosen, that is based on the integration of algebraic-differential equations. PSAT (Power System Analysis) is an open source tool, able to perform time domain simulations in Matlab environment [11]. It gives the user the possibility to modify the source code. New models were also implemented such as load variations according to real load tendencies, overload line protections or automatic under-frequency load shedding among others.

B. *The telecommunication network/ infrastructure*

The goal was to simulate the behavior of the external telecommunication infrastructure. For the modeling, a “black box” approach was used where the events are packets entering and exiting the network. The principle is called “discrete time simulation” and it illustrates the behavior of discrete systems. The components of the network are measurement concentrators, routers, links between them and Remote Terminal Units (RTU) which give settings to the power components (that can command the turbine governors of generators, the alternator excitations and the switches in the electric network).

The priority criteria for the choice of the simulation tool were basic features and usage simplicity. The SimPy library, “an object oriented, process based discrete-event simulation” [12], from the Python language was used. .

C. *The control center/ Information infrastructure*

The aim was to simulate a complete response loop. Once the data is gathered through the telecommunication infrastructure, the control center needs to provide suitable commands, according to the circumstance, meant to maintain the electric parameters within the acceptable limits. It receives frequency and voltage alarms from the measurement system and it sends new references to the generator RTUs, according to specific situation.

Matlab software was chosen to simulate the control center. It is important to underline the fact that this is a different process than the one in which the electrical network is computed.

D. *Inter-process Communication*

In order to couple the three dedicated simulators in one unitary tool, inter-process communication was used. The implementation depends strongly on the operating system, but it is possible to choose an approach that uses the same concept for all the platforms.

The basic concept “Named Pipe” was used for the implementation of the inter-process communication (IPC). On Portable Operating Systems Interface (POSIX) it does not raise any difficulties and can easily be integrated with Python or Matlab. On Windows platform, Matlab cannot manage them directly. The integration was, therefore, possible by using Perl. This is an interpreter that can manage Windows named pipes and is provided with Matlab. Fig. 3 depicts the scheme of combined simulator made out of the three individual simulation tools coupled through inter-process communication pipes. The major difficulty is to preserve the synchronization of the different infrastructure [10].

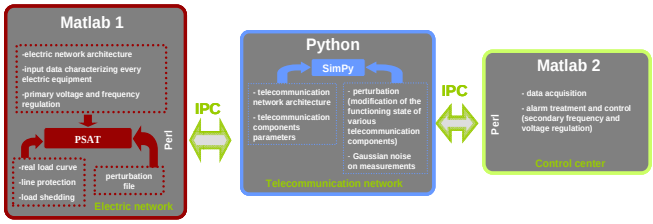

Fig. 3. The combined simulator

E. *The Benchmark*

A study case involving an educational test network was also developed. It consists of a multi-infrastructure model that describes scenarios together with user programmed functions. It was used as a first input of the combined simulator. For the electrical infrastructure the IEEE 9 bus benchmark was used. This was enriched by equipping the generators with turbine governors and automatic voltage regulators and by paralleling the lines and implementing line protection functions. Real load curve for the consumption were imposed.

V. ABNORMAL FUNCTIONING IN COUPLED INFRASTRUCTURES

The coupled simulator can be used for different inter-infrastructure purposes. The first version could mainly be employed to measure 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.

Presently, the coupled simulator was enriched with early detection mechanisms of blackouts for the power network and quality of service for ICT. The purpose was to illustrate the interdependent behavior of the coupled infrastructures, during serious scenarios.

For the power system, an aggregated robustness index was integrated. First proposed in [13], the index was conceived in an anticipation perspective, in order to give synthetic information about the state of the network to the power system dispatcher. The index was adapted here for time-domain simulations and it takes into consideration the following aspects: static performance (based on voltage, currents and reactive power analysis), small signal stability, voltage collapse indicator [14] [15], loss of synchronism and reserve monitoring.

The possible quantitative and qualitative values of this index are:

$$RI = \begin{cases} 1 \Rightarrow \text{Alert} \\ 2 \Rightarrow \textit{Action} \\ 3 \Rightarrow \text{Danger} \\ 0 \Rightarrow \text{Normal} \end{cases}$$

The telecommunication network's state is illustrated by quality of service parameters like: the telecommunication load, the throughput, delay and jitter. Congestion and retransmission mechanisms were also integrated.

A. *Simulation results*

1) *Normal functioning*

The curves below present the normal functioning of the multi-infrastructure system. The 3 charges follow the imposed ones; the electrical parameters are within normal limits. Only the currents' values are higher reflecting the higher load towards the end of the simulation.

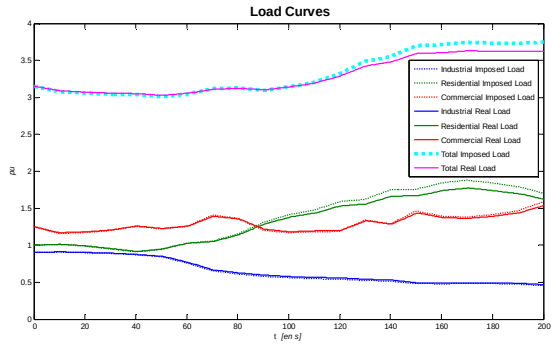

Fig.4. Electric load in normal state

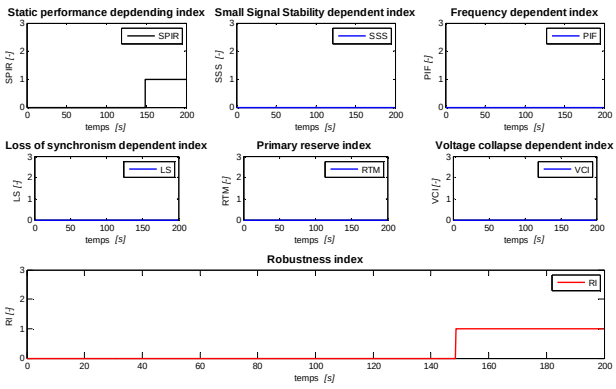

Fig.5. Robustness index in normal state

The telecommunication network's behavior is rhythmic reflecting data injection frequency, which reflects the built model. Also, the load has no peaks variations, which proves the fact that there is no significant loss of data and very little retransmission is necessary.

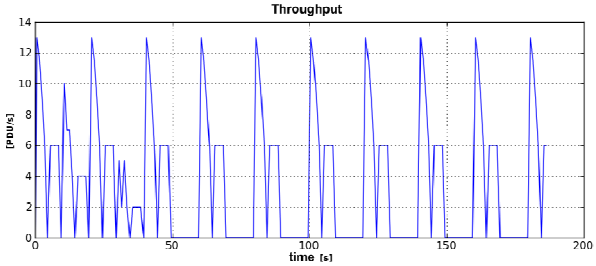

Fig.6. Telecommunication network throughput in normal state

2) *Abnormal functioning*

The abnormal functioning is given by the linear constant growth of the consumption in a load node until voltage instability is reached. As you can see the industrial imposed load does not follow the imposed one, but grows until voltage instability.

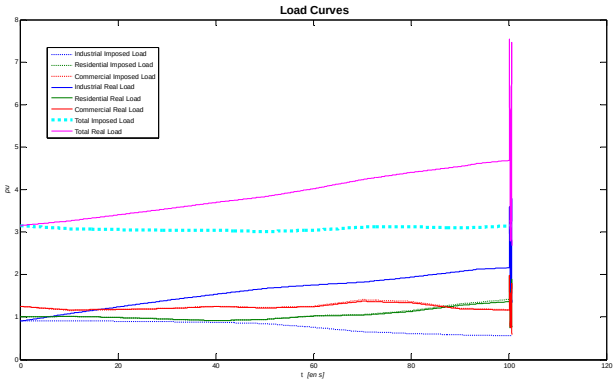

Fig.7. Electric load in abnormal state

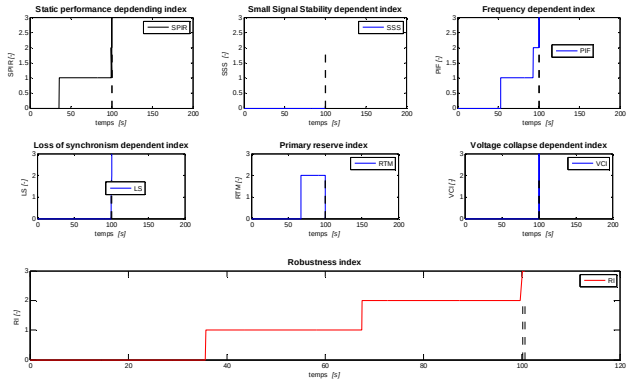

Fig.8. Robustness index in abnormal state

The average telecommunication load increases as alarms are transited through the network and cause a growth of the number of lost data units. In consequence, data retransmission is necessary; which increases the telecommunication load even more. This is reflected by the growing trend of the peaks.

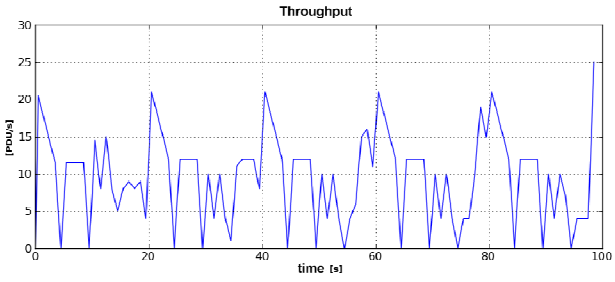

Fig.9. Telecommunication network throughput in abnormal state

Building multi-infrastructure simulation tools and multi-infrastructure test-cases is an important step for reaching a better understanding of critical infrastructures. The coupled simulator is a very flexible, extensible and highly modular simulation tool. It can be easily adapted to new needs. The presented simulation results prove that, based on a known telecommunication transit, remarks can be made about the

general state of the electric networks, only by looking at quality of service parameters of the dedicated network.

VI. Conclusion

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 a 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 paper presents a method for simulating the interdependencies between these infrastructures.)

References

[1] M. Shahidehpour, Y. Wang, "Communication and control in electric power systems," *IEEE Pres Power Engineering Series*, 2003

[2] M. Ekstedt, T. Sommestad, "Enterprise architecture models for cyber security analysis," *Proceedings of Power System Conference and Exposition*, Seattle USA, 2009

[3] European Commission, "Terms of reference feasibility study: European network of secure test centers for reliable ICT- controlled critical energy infrastructures," July, 2007

[4] IEEE Working Group "Reliability indices for use in bulk power system supply adequacy evaluation," *IEEE Transactions on Power Apparatus and Systems*, Vol. 97, No. 4, 1097-1103, 1978

[5] D. Mussington, "Concepts for enhancing critical infrastructure protection: relating Y2K to CIP research and development," RAND: Science and Technology Institute, Santa Monica CA, 29, 2002

[6] GRID consortium "ICT vulnerabilities of power systems: a roadmap for future research," *European Communities*, ISBN 978-92-79-07138-6, 2007

[7] P. Kundur, *Power system stability and control*, EPRI Editors and McGraw-Hill, Inc. ,1993

[8] T. Bjorn, M. Fontela, P. Mellstrand, Gustavsson, C. Andrieu, S. Bacha, N. Hadjsaid, Y. Besanger, "Overview of ICT components and its application in electric power systems," *Proceedings of 2nd International Conference on Critical Infrastructures*, Grenoble, France , 2004

[9] M. Zima, M. Bockarjova, "Operation, monitoring and control technology of power systems," EEH Power Systems Laboratory, ETH Zurich, [Online]. Available: http://www.eeh.ee.ethz.ch, Accessed March 2007

[10] L. Andersson, K.P. Brand, W. Wimmer, "The impact of the coming standard IEC61850 on the life-cycle of open communication systems in substations," *Proceedings of Transmission and Distribution, Brisbane, Australia*, [Online]. Available: http://www.nettedautomation.com/download/mannheim-2003-03/Brisbane_Brand_2002-08.pdf, 2001, Accessed March 2007

[11] R. P. Gupta, "Substation automation using IEC61850 standard". *Proceedings of 15th National Power Systems Conference, Bombay*, [Online]. Available: http://www.ee.iitb.ac.in/~npsc2008/NPSC_CD/Data/Oral/DIC4/p107.pdf , 2008 , Accessed January 2008

[12] F.F. Wu, K. Moslehi, A. Bose, "Power system control centers: past, present, and future", *Proceedings of IEEE*, 2005 doi: 10.1109/JPROC.2005.857499

[13] M. Fontela, "Transmission networks and dispersed generation, Ph.D. dissertation," G2Elab, Grenoble National Polytechnic Institute, 2008.

[14] P. Gopi Krishna, T. Gowri Manohar," Voltage stability constrained ATC computations in deregulated power system using novel technique," *Proceedings of ARPN Journal of Engineering and Applied Sciences*, vol. 3, no. 6, ISSN 1819-6608, December 2008

[15] P Kessel, H Glavitsch, "Estimating the voltage stability of a power system", *IEEE Transactions on Power Delivery*, vol. PWRD-1, No.3, July 1986, pp. 346-354

Nouredine Hadjsaid (SM'05) received his Diplôme d'Etudes Approfondies (DEA) and Doctorat de l'INPG degrees from the Institut National Polytechnique de Grenoble (INPG) in 1988 and 1992. From 1988 to 1993, he served as a research and teaching assistant at the Ecole Nationale Supérieure d'Ingénieurs Electriciens de Grenoble (ENSIEG) and at the Laboratory d'Electrotechnique de Grenoble (LEG). He is now a full time professor at Grenoble InP at the Ecole d'Ingénieurs pour l'Energie, l'Eau et l'Environnement de Grenoble (ENSE3) in the Grenoble Electrical Engineering laboratory (G2Elab). His research interests are power system operation and security. Since 1992, he has been involved as a scientific director for more than 20 industrial and European projects in the power energy sector and critical infrastructures. These projects concern in particular power system security, new technologies to enhance power system control and monitoring, optimization of distribution systems, distributed generation, ancillary services and planning under deregulation, Information and Communication for Energy for example.

Maria-Georgeta Viziteu (S'06) graduated the Power Engineering Faculty in the University "Politehnica" of Bucharest, Romania, in 2006. She obtained her Master at the Grenoble Institute of Technology, France, in 2007. Presently she is preparing a Ph.D. thesis regarding securing critical infrastructures, within a project supported by Atos Origin and G2Elab.

Raphael Caire (M'04) received his Diplôme d'Etudes Approfondies (DEA) and Doctorat de l'INPG degrees from the Institut National Polytechnique de Grenoble (INPG) in 2000 and 2004. He had been working in Power Electronic field, in USA at the Center of Power Electronic System (CPES) in 2000 and within several EDF research centers in Germany and in France from 2004 to 2006. He is now associate professor at Grenoble Institute of Technology (Grenoble-InP) at the Ecole Nationale Supérieure de l'Eau de l'Energie et de l'Environnement de Grenoble (ENSE3) in the Grenoble Electrical Engineering laboratory (G2Elab). His research is centered on the impacts, production control of dispersed generation on distribution system and critical infrastructures.

Daniel Georges graduated INPG - Institut National Polytechnique de Grenoble - France. Presently, he is in charge of Business Development for Atos Origin Energy Network activity since 2004, Daniel has managed previously several implementation projects of SCADA_GMS (Gas Management System), EMS (Energy Management) and DMS (Distribution Management). His technical background covers as much Information Technology as Metier domains and gives him a high capability in understanding Transmission and Distribution Company needs, especially in Security domain. Daniel brought already contributions to different international congresses such as APCE 06, CIGRE, CIRED, CEPSI, SIMONE Congress, among others.