SPECIAL REPORT FOR GROUP D2
(Information Systems and Telecommunications)

Gustavo ARROYO

Special Reporter

General

CIGRÉ's Study Committee D2 's mission is to:

- facilitate and promote the progress of engineering and the international exchange of information and knowledge in the field of information systems and telecommunications for power systems
- add value to this information and knowledge by means of synthesising state of the art practices and drawing recommendations

To achieve this goal, the SC D2 has proposed as second preferential subject, the following:

> **PS2: Frameworks for the governance and the management of the information and communication systems in the Electric Power Utilities.**
>
> 1. Description of best practices.
> 2. Utilization of emerging standards (COBIT, ITIL, BS15000...).
> 3. Organization of the utility for ICT governance.

The main reason is the strong tendency to apply different IT governance mechanisms and best practices for planning, acquiring, implementing and monitoring IT performance, in order to ensure that the enterprise's IT assets support the business objectives.

Preferential Subject 2.

The papers included in this report deal with best practices, emerging standards, IT governance, information and communication systems and security for Electric Power Utilities (EPU). Four of the papers are oriented to best practices, emerging standards and governance; nine of the papers are oriented to information and communication systems; and five of the papers are oriented to security information and IT security. For this PS 2 eighteen (18) papers are presented, which are grouped in the following way:

1. Governance and its applications for EPU.

D2-202	Directions and applications of IT governance in CFE
D2-208	Governance principles for the information and communication systems of a transmission system operator
D2-209	Management improvements in telecommunications systems in Japanese Electric Power Companies
D2-212	Modeling and evaluating the maturity of IT governance

2. Information and communication systems for EPU.

D2-203	Information and communication systems in the deregulation of the energy sector in Russia
D2-204	Topology design of optical networks based on existing power grids
D2-205	Implementation of a distributed RTU monitoring system using the IEC60870-5-104 protocol over GPRS networks
D2-206	Ethernet process bus: assuring its availability
D2-207	Assessment of users' needs and modelling of a TETRA digital radio network for Croatia power utility
D2-214	New challenges in electric substation telecommunication and IT networks
D2-215	Evolution towards a unified technology communication network
D2-216	Development of an integrated communications system in Tenaga Nasional Berhad
D2-218	IP trend for control, operation and maintenance of EGAT Patana Sangsriroujana and Phiphat Tanapornchinpong Electricity Generating Authority of Thailand

3. Information security and IT security and its applications for EPU.

D2-201	A novel technique for risk reduction and improved governance in a critical telecommunication network
D2-210	Development of power equipments CMD (Condition Monitoring and Diagnosis) system using the telemetric techniques
D2-211	Enterprise condition monitoring and diagnostics (eCMD)
D2-213	Treatment of information security for electric power utilities – progress report from CIGRE WGD2.22
D2-217	Cybersecurity standards for the electric power industry – a "Survival Kit"

2.1 Governance and its applications in EPU.

Paper **D2-202** describes the status, steps and directions that CFE has taken to apply an IT governance framework. The paper also includes a brief description of the concepts of IT governance and of maturity levels and a study of maturity levels in international companies. The status of the IT governance from the viewpoint of its current and desired maturity levels at CFE is presented together with the limitations that CFE faces to improve its average IT governance maturity level.

Question 2.1: Could the authors share their experience in the application of IT governance? What are the obstacles to overcome? The figure 2 shows the proposed directions of IT governance at CFE, Can the authors explain the frameworks, standards and IT projects? What are the maturity levels impacts on the operating cost of IT processes in CFE? Are there any other experience of the same kind in the audience?

Paper **D2-208** describes the efforts that RTE has done to apply an IT governance framework based on COBIT and ITIL standards. The main objective is to assure the correct operation of the existing information systems and to develop new systems under new models of exchange of information based on Service Oriented Architecture. The

paper also shows some changes in the organization such as a Chief Information Officer (CIO) with the task of guaranteeing the coherence of all of the IT Systems and the definition of information systems committees.

Question 2.2: Could the authors share their experience in the application of IT governance? What were the obstacles to overcome? How was the process of adoption of the COBIT control objectives? Could the authors comment the process to realign the organization of the IT with the different business lines? Are there any other experience of the same kind in the audience?

Paper **D2-209** presents trends and directions for the improvement of IT governance in Japanese electric power companies. The application of ITIL standard to monitoring and management IT operations in Kansai Electric Power Company is presented. The paper also describes the automation of network monitoring, improvements to the operation management system and the use of speech recognition technology as a maintenance check method.

Question 2.3: Could the authors share their experience in the application of ITIL standard? What were the obstacles to overcome? The paper mentions that the network monitoring tasks were outsourced to an affiliated telecommunication company, could the authors explain the advantages and disadvantages of this decision? What are the results on the use of speech recognition technology? Can the audience describe similar experiences in the application of ITIL standards?

Paper **D2-212** presents the tool ITOMAT (IT Organization Modeling and Assessment Tool) which is an IT governance decision support tool. ITOMAT is based on COBIT and it can be use to model an IT organization from the point of view of governance, including processes, activities, roles, documents and metrics. An application example of ITOMAT at an electric utility is presented in which ITOMAT is used to predict IT governance performance.

Question 2.4: What were the main challenges faced during the development stage of this tool? Could the authors describe the intelligent model and how it was implemented in the tool? What are the main future developments of the tool? Would the audience and the different authors provide a more extended discussion on the experiences of EPU in the application of IT governance?

2.2. Information and communication systems for EPU.

Paper **D2-203** describes the transformation of a Russian communication network into a United Technological Communication Network of the Electric Power Industry (UTCNEPI). The paper presents the basic principles of the UTCNEPI, the network composition and structure in the EPI and the future works of implementation.

Question 2.5: Could the authors explain the scope of the UTCNEPI? What are the planning and implementation processes? From the information technology's point of view, could the authors comment the main challenges in the deregulation of the energy sector?

Paper **D2-204** gives an introduction to the use of optical networks for the existing power grid and the technology trends in optical transmission networks such as DWDM (Dense

Wavelength Division Multiplexing), next generation SDH (NG-SDH), and Automatically Switched Optical Network (ASON). As case study, the authors present the design of the network based on EGAT's (Electricity Generating Authority of Thailand) power grid.

Question 2.6: How efficient the proposed design method used is compared to other reported methods? How reliable DWDM networks with OPGW results compared to other traditional or new transmission technologies? Can the authors explain the use ILP technique in the design of the network of EGAT's power grid? Could the authors or the audience provide a more extended discussion on the experiences of EPU in the use of DWDM technology?

Paper **D2-205** describes the application of a communication network with GPRS (General Packet Radio Services) technology for the monitoring of an electrical network. The modernization of RTU using protocol IEC-61850-5-104 and the integration of GPRS technology in legacy RTU are presented. The paper also presents the challenges imposed by the new architecture.

Question 2.7: What is the communications efficiency test with GPRS applications on real time telecontrol system? What is the statistics? How measure the parameters communications efficiency when a GPRS mobile operator leaves? How many RTU in legacy protocol cover with this technique? How much investment in this project was needed?

Paper **D2-206** analyzes the process bus as a critical system when deploying a substation based on the IEC 61850 standard and gives some requirements that process bus must comply. Based on a common architecture approach, the paper discusses the term reliability which comprises other components such as availability, performance and capacity. The network performance is discussed by using a test scenario in order to analyze the performance characteristics of data flows inside an Ethernet switch. Finally, the paper presents the results obtained from latency and lost frames of the proposed process bus for different traffic loads.

Question 2.8: How feasible the AFDX standard can be applied directly to the IEC 61850 Ethernet process bus design? In opinion of the authors, what should be the appropriate topology for a reliable Ethernet process bus which meet the "no frames lost" requirement? For a real implementation, what is the availability value the Ethernet process bus must provide?

Paper **D2-207** describes a methodology for determining the user needs and the definition of an appropriate communication solution. Based on the analysis of strengths, weaknesses, opportunities and threats, the solution was identified as TETRA mobile radio system. The modelling and implementation of the TETRA digital radio network are presented. Finally, a technical and financial evaluation is discussed.

Question 2.9: What are the future steps in the implementation of nationwide TETRA system? Based on the financial evaluation, what are the investment recovery plan and the associated time frame? Could the authors or the audience provide a more extended discussion on the experiences of EPU on the use of TETRA based solutions?

Paper **D2-214** presents different views for convergence of corporate and operational networks in an electric power substation using IP technology, industrial Ethernet and IEC 61850 communication standard. Some best practices for converged infrastructure communications between interoperable network elements in substation automation, operation and communication processes are presented.

Question 2.10: Could the authors assign priorities to the factors involved in the process of converged network for electric substations? How would you recommend dealing with the security aspects, once the enterprise is involved in the network integration process? Could the authors present some practical examples of modern IP multimedia network architectures?

Paper **D2-215** describes the legacy telecommunications networks and their solutions for a unified technology communication network. It describes the evolution that this network struggling to accommodate new services and internal customer demands as they are appearing, maintain an acceptable quality of service and security levels. The paper recommends that in any telecommunication migration process it is strongly encouraged to use project and risk management techniques.

Question 2.11: Could the author comment about the telecontrol solution to continue service without interruption in presence of a single failure. What is the performance of fitting the SDH boxes with Fast-Ethernet tributaries? What is the limited performance in terms of speed and resilience from the management network using the digital multiplexers superimposed on the transmission network?

Paper **D2-216** describes structured and hierarchical network architecture as a basis of the integrated communications system using next generation SDH technology, called multi service provisioning platform (MSPP-SDH). The network equipment enables both deterministic TDM and non-deterministic packet based traffic to be switched and transported. The network architecture adopted for developing the communications system supports multiple types of services and is scalable to meet capacity and service expansion.

Question 2.12: What are the asymmetrical communications delays caused by single ended protection switching? Could the author explain the organizational support structure to operate and maintain the integrated system employing ITIL best practices? How will this ensure efficient operation of the system? When services for real time grid system operational applications are provided through dedicated networks, what is the communication systems performance for critical operational services such as teleprotection and telecontrol (their response time/delay)?

Paper **D2-218** describes the effort of EGAT to introduce IP technology in its corporative and operative networks. Three stages were defined for the development of the IP network for the transmission equipment. First stage: development of transmission equipment using IP network via series port such as RS-232 or RS-485. Second stage: separation of IP networks between operation and administrative network. Third stage: enhancement of operation network to conform to IEC-61850 standard.

Question D2-13: What were the main obstacles to overcome in the project? Could the authors explain, what are the new IP technologies that EGAT applied in its corporative and administrative network? What are the most important factors that EGAT took in account for its IP technology plan? Would the authors and audience like to comment how these communication standards and technologies can help in the application of frameworks of IT governance?

2.3 Information security and IT security and its applications for EPU.

Paper **D2-201** describes a methodology for risk reduction based on artificial intelligence techniques. The objective is the early detection of anomalies in order to avoid electrical outages to communication equipment and other network's breakdowns. The approach is integrated as a software application with communication network using a middleware layer as interface between the application throughout a network.

Question 2.14: What are the techniques used for early detection of anomalies? What were the main challenges when this tool was developped? Could the authors give some examples of the application of the model? Can the authors comment on the future steps of middleware applications in the telecommunications network?

Paper **D2-210** describes the development of condition, monitoring and diagnosis (CMD) systems using telemetrics technique. CMD systems can monitor and diagnose power equipments in transmission and distribution lines and substations based on IEC61850 standard. The paper also presents the architecture of an enterprise asset management (EAM) composed by CMD, maintenance management system (MMS) and fault event analyzer (FEA).

Question 2.15: Could the authors share with the audience the implementation and operation experiences of telemetric techniques? Could the authors describe the model to detect faults and how it was implemented in the CMD system? From the information technology's point of view, could the authors comment on the strategy to integrate the CMD, FEA and MMS? What is the future upcoming work?

Paper **D2-211** presents a software architecture that can be used to implement a condition based maintenance system (CBM). The CBM is based on novel software concept, for example: the open system architecture (OSA), using tools like common object request broker architecture (CORBA), simple object access protocol (SOAP), extended markup language (XML) and rich internet application (RIA).

Question D2-2.16: Could the authors give a more detailed description of the state detection and decision support layers? Is there any pilot implementation of the technique proposed in the paper? Could the authors share with the audience the reasons behind the decision to develop CBM system based on novel software technologies?

Paper **D2-213** presents the preliminary results from the study of treatment of information security for Electric Power Utilities. The first purpose is to provide guidance to the EPU on how to adapt and implement a framework in its own environment. The second purpose is the adoption of common advanced methods for risk

assessment usable in the EPU practice. Finally, the third purpose is to identify effective strategies for applying appropriate security technologies to secure EPU technical infrastructures. The aim is to identify most common EPU architectures, and thereby identify leads to security technology recommendations that apply directly to EPU networks.

Question 2.17: What are the frameworks that can be applied to manage information security for EPU? What are the best practices identified for risk assessment for EPU? What are the security technologies for SCADA/Control systems? Could the authors or audience provide a more extended discussion on the today's status on the use of risk assessment and security for EPU?

Paper **D2-217** presents different kinds of relevant cyber security standards for the Electric Power industry. Standards are a powerful tool to ensure interoperability of systems, minimize costs of new developments or maintenance, and ensure high technical and organizational level of quality. This is particularly true when it comes to cyber security issues for Electric Power Utilities. The following set of standards has been considered as particularly relevant: the ISO/IEC 2700x series, the IEC 62351 technical specification, the IEEE P1711 & P1689 drafts, the ANSI/ISA 99 Technical Reports and Standards series, the NERC CIP standards, the NIST SP800-53 (annex 1) & SP800-82 special publications and the CPNI Guidelines.

Question 2.18: Could the authors comment: Which world class companies have implemented these standards within their organization? How much and how long has taken those companies to implement such standards? Based on your experiences, are there any specific recommendations you would like to share the audience? Could the authors or audience provide a more extended discussion on the application of cyber security standards in EPU?