D2 – 00

SPECIAL REPORT FOR SC D2
(Information Systems and Telecommunication)

Lars NORDSTRÖM (PS1 and PS2) and Hermann SPIESS (PS3)
Special Reporters

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 synthesizing state of the art practices and drawing recommendations.

The Strategic Plan (2012-2021) defines the organization of the SC D2 to cope with the following objectives:

- To be more customer oriented;
- To foster the participation in the working bodies;
- To be well balanced between information systems, telecommunications, telecontrol and automation;
- To draw the interest of the customers for the work done in the SC.

Three Preferential Subjects are presented in this Special Report:

PS1, Information and telecommunication technologies for connecting distributed energy resources

- Facilities for control, monitoring, security and safety.
- Use of existing standards, interoperability and cyber security issues.
- Operating conditions, EMF, installation and maintenance issues.

PS2, Maintaining operational IT reliability in an evolving environment

- Virtualization applied to power system operations and disaster recovery.
- Cloud services availability and security.
- Impact of operational systems on IT governance, practices and experiences.

PS3: Trends in managing utility communication networks

- Smart grid communication network and service management.
- Evolution of operation support systems.
- Security of communications and of the management system.

A total of 15 papers have been received; they have been used as the material for this Special Report.

lars.nordstrom@ics.kth.se
hermann.spiess@ch.abb.com

Preferential Subject 1: Information and telecommunication technologies for connecting distributed energy resources

Introduction

Distributed Energy Resources (DER) ranges from larger scale wind power farms to household level PV panels. From a communication and control perspective two aspects are common for these types of resources, regardless of their capacity or form of generation, that is:

- that they are located geographically dispersed,
- and that they are sometimes under the control of other entities that the grid operator itself.

These two aspects imply first that the information and telecommunication technologies for connecting them need to cover large geographical areas, sometimes in a very fine grained mesh. Second it also means that the communication solution borders two organisations, which may require additional interoperability and security implications.

Papers

9 synopses for PS1 have been received, of which 3 papers have been selected for the Preferential Subject No. 1 as hereunder:

D2-103	Powerline communications for connecting distributed energy resources	Spain
D2-104	Security of communications in voltage control for Grids connecting DER: impact analysis and anomalous behaviours	Italy
D2-108	Technical specification for the utilisation of web services for the electronic data interchanges on the Internal Electricity Market	SC D2

Discussion and Questions

Paper D2-103 addresses the issue of using Power Line Carrier to communicate with DER resource connected in a MV and LV grid. Since PLC well covers the area in which the DER resources could be located, the technology is suitable for communication with these resources. The paper presents the use of existing AMI systems based on PRIME for communication with DER resources, and also a solution similar to Teleprotection that is used for controlling the DER by sending ON-OFF commands to the DER unit.

Q103-1 What are the today solutions enabling the connection of a DER unit both with the grid operator and with the DER unit owner control system? Are there examples of such case? Would remote access to the DER by PLC or other means still be possible? Could there be cases where the communication to the DER unit would be blocked by other communication means being used, preventing access via PLC or other means?

Q103-2 What is the experience as concerns the performance (in terms of latency and packet drop) of the PLC communication system? Depending on the amount of traffic being sent, in particular during situations where several DER units need to be controlled, is it possible to have a degradation of communication?

Q103-3 Are other protocols than PRIME possible to be used? And could it be assessed that the results of the study are still valid for other means of PLC communication not using the PRIME protocol?

Paper D2-104 discusses how failures caused by cyber attacks on the ICT infrastructure that supports a Voltage control function in a rural MV grid with high levels of penetration of DER (Distributed Energy Resources) impacts grid operation. Since the DER may be outside the control of the utility, the resulting overall architecture interconnects a variety of ICT entities and network segments.

The paper presents a security and risk analysis framework based on the SGIS – Smartgrid information Security working group of CEN-CENELEC-ETSI, and uses this to assess the above question in a qualitative manner. The paper also includes a study of the ICT architecture as well as benchmark grid data all used to estimate the threat likelihood. The paper also clarifies the link between the outcome of the use case risk analysis and the security requirements/measures from available and ongoing security standards.

Q104-1 The study has used the Smartgrid Architecture Reference Model to describe the functional level mapping for communication and ICT components, this is not presented in the paper. Would that be possible, or does the context of security analysis require an alternative modelling of the ICT infrastructure not supported by the SGAM?

Q104-2. Have utilities in genera carried out such assessment? In particular to which extent would it be possible to quantify the levels assessed in the risk analysis used; which value would quantified risk levels have above more general terms like **high** and **critical**?

Q104-3 Have any utilities developed a security assessment framework including also failures due to poor maintenance or random chance, simply by removing the attacker from the analysis and only focus on the effects (loss of measurement for instance, can be a consequence also of a computer failure)?

Paper D2-108 defines a list of services needed to support the electronic data interchanges between actors on the European Energy Market for electricity in a near real-time secure way using an IEC 61968-100 based web services solution. The paper presents in great detail the data exchange mechanisms to be used and also the security measures put in place to protect the communication.

Q108-1 Web services provides a flexible means of communication between several actors, to which extent does the Electricity market communication require this flexibility, or could more static, but higher performing means of communication be use

Q108-2 Can the proposed information exchange framework be used widely across the electricity market, or only on the Transmission system level? Are they other information exchange framework used for the electricity market?

Q108-3 What is the utilities practices in using these generic message types defined in the communication framework for electricity market communication? Would a more context specific message types allow for simplified processing at participating actors?

Preferential Subject 2: Maintaining operational IT reliability in an evolving environment

Introduction

The importance of well functioning IT systems for protection, operation and control of electric power system is without question. The reliability of the operational IT systems must not reduce the overall reliability of the power system but should instead facilitate in increase in the power system reliability.

Given the increasing use of IT systems in ever more complex configurations, the reliability of the IT systems becomes increasingly difficult to predict and manage.

Proper quality assurance processes needs to be put in place both during design and operation of the IT systems in order for them not to jeopardise the overall reliability of the systems. Such quality assurance process need also be adaptable to the evolving environment in which new systems are used for purposes where there was earlier little or no automation in place.

Papers

3 synopses for PS2 have been received, of which 3 papers have been selected for the Preferential Subject No. 2 as hereunder:

D2-201	IT platforms of Japanese electric power companies	Japan
D2-202	Experiences and practices in the implementation of IT governance in Mexican electrical utility	Mexico
D2-203	Security in remote services used by EPUs	SC D2

Discussion and Questions

Paper D2-201 discusses the new conditions facing Japanese Electric Power Companies (EPCO) as a consequence of the large Japanese earthquake disaster in 2011. These conditions include both new business climate and stricter requirements on fault tolerance of the IT infrastructure to natural disasters. The paper presents a handful of mitigation strategies that some Japanese EPCOs have, or are putting in place to manage these new conditions.

Q201-1 Many of the actions put in place by the EPCOs that are described in the paper could potentially be implemented in a centralised Cloud solution. Meaning that the monitoring applications could be running in one (or several) redundant data centers providing service to the EPCOs. To which extent would that be a possible solution, given existing requirements on reliability and performance? Do utilities have some experiences in such a solution?

Q201-2 The additional systems and measures being installed to manage the new requirements require high fault tolerance and reliability. Normally such solutions are very costly, is it possible for the utilities to get coverage for such costs through normal tariffs from customers? Does the regulation of the electricity business allow for these types of IT investments?

Paper D2-202 discusses the importance of establishing proper IT governance processes in place at electric power companies. The emerging Smart grid will involve a much larger degree of IT and communication resources, that need to be managed in a reliable manner just as the power grid is. Within the IT industry a number of frameworks for IT management have been developed since 10-15 years, and the paper reports on the experiences with implementing them at a Mexican electric power utility.

Q202-1 The MAAGTIC-SI framework described in the paper includes also Enterprise Architecture models of the business. Since Enterprise Architecture has its roots in administrative IT systems models may not be readily available for Operation IT systems. Based on this, to what extent are of Enterprise Architecture models of Operational IT systems generally available at electric utilities?

Q202-2 Creating Enterprise Architecture Models of both administrative IT and operational IT systems, can sometimes be managed by a specific function at a company, that is also responsible for keeping the models up to date. Alternately models can be created within procurement or upgrade projects – Comments on both benefits and disadvantages would be interesting to hear.

Paper D2-203 discusses the important issue of security for remote services in electric power utilities. Remote access to systems and platforms within a utility's IT infrastructure is a common procedure in order to achieve the efficiency offered by automation and control systems. The paper gives an introduction in securing the components of remote services by analysing relevant security standards and best practices. The paper highlights possible gaps in the present standards and procedures. It also addresses the important issue of responsibility through the contracts that need to be in place for remote access.

Q203-1 Remote access can be made more secure by actions proposed in the paper. A general question is to which extent weaknesses in the security management at the external partner can be compensated by these actions. What is a proper balance between protection at the utility, and requirements on that the external partner has sufficient security mechanisms in place? What is the utilities experience in such a field and in particular which kind of access are allowed either for the Corporate IT or the Operational IT?

Preferential Subject 3: Trends in Managing Utility Communication Networks

Introduction

Technology changes and migration scenarios entail special challenges with respect to the design and operation of telecommunication networks for the EPI. The growth and increasing complexity of modern communication infrastructures requires efficient tools to operate and manage the same in order to secure the requested reliability. The complexity of today's communication solutions for electric power utilities manifests itself in challenges like:

- Fulfilling the demanding requirements of mission-critical application for the protection and control of the electric power grid
- Mastering the evolution of IT and Telecom technology
- Mastering the coexistence of different communication technologies and media in the network
- Mastering of Cyber Security threats for critical infrastructures

The submitted papers address these subjects from various perspectives.

Papers

12 synopses for PS3 have been received, of which 9 papers have been selected for the Preferential Subject No. 3 as hereunder:

D2-302	Experiences with an IP/MPLS Network in Utility Environment	Belgium
D2-303	The telecommunications business expansion at Eletrobras Eletronorte and the needs for changes in operation and maintenance	Brazil
D2-304	Beyond Chesf's telecommunications information security analysis	Brazil
D2-305	Managing adapted packet network architectures for smart IP-based services	France
D2-306	Challenges in Establishment of Large OPGW based Communication Network - Indian Experience	India
D2-307	Smart Grid Network through Integrated SCADA System-Karnataka Model- A case Study	India
D2-308	Telecommunication Networks for Smart Grids Deployment	Spain
D2-310	Trends of communication networks in Japanese electric power utilities	Japan
D2-312	Smart Communication System SCS	Venezuela

Discussion and Questions

Papers discussing technology migration and network management

The migration from circuit to packet networks has been dealt with by Cigré SD D2 in various forms in the past. While the introduction of packet technology follows the general trend in public networks, its application for the operational services of the EPI has been strongly challenged by the stringent real-time and security requirements of Teleprotection and Current Differential Protection services. Failures of the protection can result in loss of supply of electrical energy, damage to equipment and humans, and high consequential cost. Mastering of time synchronisation and deterministic signal transfer between IEDs is crucial for reliable and secure operation of protection.
In addition to performance issues the introduction of new technologies, their coexistence with the installed base and the diversity of an increasing number of services with different quality requirements make the management of such networks a challenging task.

Paper D2-302 from Belgium reports about experiences with IP/MPLS packet-switched technology in the utility environment. General requirements, design and implementation options including security architectures are discussed. Because the transmission of protection signals over Packet-Switched Networks is a Greenfield for most TSOs, a special focus has been put on the testing of the performance of Teleprotection and Current Differential Protection services.

Q302-1: Given the special requirements of operational services, various predictions supported by two Cigré polls have been made in the past as to when the migration of operational services from SDH/TDM to packet networks will turn into reality. Concerns have repeatedly been raised concerning lack of determinism for relay protection and security.
What is the current status and experience with using packet-switched (e.g. IP/MPLS) wide-area networks for operational services like SCADA and Line Protection? What are issues and obstacles for packet networks to eventually substitute SDH/TDM? Given the huge installed base of SDH in the EPI, is the substitution scenario desirable and realistic? Are dedicated fibres or wavelength a viable alternative? In which cases?

Q302-2: Precise **t**ime synchronization is critical for Line Differential Protection and Phasors. Synchronization may be based on GPS, on echo principles or on real-time clock distribution across the WAN.
Which synchronization principles for IEDs (Protection Relays) are used and preferred today? What is the experience regarding reliability of the different methods? Can the same principles be applied for Packet Networks? What are possible consequences or restrictions for circuit-to-packet migration scenarios, considering the huge installed base of “legacy” protection relays?

Q302-3: How did – in the case presented in paper D2-302 – the inclusion of protection applications impact the design of the MPLS network regarding cyber security architecture and network engineering?
Are there significant differences with respect to engineering efforts and ease of implementation for Teleprotection (binary commands) and Current Differential protection services? Given the pioneering work, could the author make a prepared contribution on key learnings and conclusions?

Paper D2-305 from France and Brazil deals with the transition from TDM to Packets from the Network Management perspective. It analyses and explores service requirements, network architectures and communication network management challenges in the light of the migration of Circuit-Switched (SDH/TDM) to Packet-Switched (Ethernet/IP) networks with an anticipated long transition period for hybrid networks.

Q305-1: Hybrid communication networks are the reality considering that different generations and technologies of PLC, radio and fibre systems from different manufacturers usually coexisted in a typical utility network.
How have utilities and manufacturers addressed the management of complex an inhomogeneous communication infrastructures? Can examples be provided of current practices? Are integrated or isolated management systems the rule or the exception?

Q305-2: The introduction of packet networks and the integration of new services will add a new dimension to the network management complexity. The authors anticipate a long transition period for hybrid TDM/packet networks considering equipment life cycle and migration issues for operational services.
How can this transition be mastered from a network management perspective? Can examples be given for migration scenarios and network management architectures for an integrated management system? Is a tighter integration of communication NMS with SCADA and Substation Automation (IEC61850) and Relay protection desirable or fiction? What are the rationales in favour or against fully integrated systems?

Papers on network development and Smart Grid deployments

Paper D2-306 from India reports on the steady growth of OPGW installation across India. The deployment of OPGW started in 2002 under the ULDC project (Unified Load Dispatch & Communication) and is now continually expanded to POWERGRID's EHV Transmission System as the demand for reliable communication and bandwidth grows. Eventually around 90'000 km of OPGW based fibre network is being implemented under various project stages. Communication technology is predominantly based on SDH and EoS (Ethernet over SDH) which allows to transport IP/Ethernet services efficiently and effectively.

Paper D2-312 from Venezuela proposes the PLC (Power Line Carrier) with routing capabilities as key element for reliable integrated communication solutions capable of transporting TDM and IP traffic across a hybrid network composed of optical fibre, radio and PLC for backing up critical services.

Q306/312-1: The operational experience with OPGWs is extensive as OPGWs have been installed since more than three decades worldwide.
Based on this long-lasting experience, what are the main causes affecting the reliability of OPGWs? Have typical or specific failure patterns or aging phenomena be observed? What are typical causes for downtimes of OPGWs? What kind of preventive performance monitoring practices are in place? Can examples for repair times be presented?

Q306/312-2: While OPGWs are considered to be very reliable, the impact of the failure of the same must be taken into account for the design of resilient communication networks. Can solutions for risk mitigation and backup scenarios be discussed which secure the uninterrupted communication service for critical applications? What technologies are being used, and how are fault contingencies and dependencies avoided?

Paper D2-307 from India presents the Karnataka Model as a case study for Smart Grids implemented through SCADA with extensive use of VSAT for communication. Potential benefits, ultimately aiming at a reliable and secure supply of electric energy to customers, are shown with the recommendation to apply the Karnataka Model to all the states in India to incorporate the requirements of the National Electricity Policy.

Paper D2-308 from Spain analyses telecommunication networks for smart grid deployment in view of standardization, technologies, service requirements, processes and security. Given the diversity of the services, the mix of communication technologies and split network ownerships it becomes apparent that the integration of processes supported by a global monitoring and management system for such infrastructures becomes key, jointly with the need for mastering demanding security challenges.

Paper D2-310 from Japan presents the development of models for the evaluation of smart grid-capable radio communication systems for smart meter communication, and verification of the same in field tests. The paper also addresses technology trends and presents an IP-based redundant communication architecture for the fail-safe communication for SCADA and mutual backup of two control centres.

Q307/308/310-1: Communication plays a vital role in Smart Grids. While the question about the selection of the “right” technology is prevalent, the actual choice depends on many factors like performance, operating environment, regulatory conditions and total cost, to name a few. In the context of AMI or DA, various flavours of radio or PLC (Power Line Carrier) communication are described in the papers. Satellite communication has been used to access remote areas with SCADA.

Which factors are (or have been) decisive for the selection of specific communication solutions in actual Smart Grid/Smart Metering/DA deployments, and how do they match the requirements on cost effectiveness and performance? Please consider also aspects of dedicated (single purpose) versus open communication solutions. How do these systems integrate into the backhaul network?

Q310-1: Hokuriku EPCO proposes a redundant and secure communication scheme for SCADA/RTU and Control Centre backup based on IP technology and gateways.
Could the authors make a prepared contribution and comment on the expected improvements regarding availability and security compared to the traditional approach?

Q310-2: In paper D2-310 from Japan the authors suggest the introduction of SDN (Software Defined Networks) technology to utilities’ Wide-Area Networks as a means to reducing operational cost and enabling the introduction of new and secure multi-services.
Could the authors make a prepared contribution explaining the concept of SDN and explain how SDN would contribute to reducing operational cost and support new business opportunities? SDN is considered a trend, with some use cases already adapted to WANs. Will SDN complement or substitute current network technologies?

Papers discussing security policies and service problems management

Paper D2-304 from Brazil reports about the implementation of Chef’s Security Policy which followed the preceding security analysis as presented in the Cigré 2012 Technical Session.
Human behaviour, cultural aspects, rapid business expansion and changes in company ownership as well as new regulatory models accompanied by budget constraints are factors which have impacted the roll-out and enforcement of security policies and procedures. Cultural changes seem however to be the prime challenge.

Q304-1: State-of-the-art security measures as implemented in ITC equipment needs to be complemented by work processes in the organization in order to become fully effective.
What are the main obstacles and challenges for implementing security policies and processes? How have these been overcome? Can examples be presented of how implemented policies and measures proved to be effective in preventing cyber security related incidents?

Paper D2-303 from Brazil discusses the implementation and ongoing improvements of the “Service Problems Management” process at Eletrobras Eletronorte. Mastering of this process is key when the utility provides its communication infrastructure and services to external customers, or when a utility is authorized to act as a telecom operator. Improvement of the methodology is driven by the increasing size and complexity of the services with cost and efficiency optimization becoming imperative.

Q303-1: The paper addresses issues and suggests process improvements for the specific case of Eletrobras Eletronorte where the utility is acting as a telecom service provider.
Could the authors make a prepared contribution summarizing the current situation and highlighting key issues and problem areas which are addressed with the proposed tools and methodologies? What are the main obstacles in the improvement process to be overcome, and how can the acceptance of the proposed measures be fostered?