http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

D2-01_37

WAN Network Communications Architectures for Smartgrids: Case Study comparison

by

A. Arzuaga*, M.A. Alvarez, S. Martinez, T. Arzuaga, M. Zamalloa

Hampesh T, J. R. Rao

CG ZIV

(ES, IN)

SUMMARY

This article presents an analysis of three different WAN communication architectures used in big scale Smartgrid projects. Two case studies analyse typical configurations in real life European scenarios, with a different approach in terms of dependability and complexity. The third case study analyses a typical configuration used in India for distribution automation programmes. All of these communication architectures make use of third party network providers (mainly cellular networks) in order to implement the Smartgrid communication network. However they follow very different approaches, which are discussed in the article.

Finally, the three communication architectures are compared, an analysis is included, and the main conclusions are discussed.

KEYWORDS

Communication, architecture, network, Smartgrid, WAN, distribution

* Parque Tecnológico de Zamudio, Edificio 210 48170 Zamudio, Spain
Fax: + 34 94 403 7440 e-mail: a.arzuaga@ziv.es

1. INTRODUCTION

One of the fundamental developments of the past years has been the massive introduction of telecommunications and IT technology utilization in the electricity infrastructure, giving rise to the so-called "Smartgrid". The Smartgrid is no other thing than the interconnection of the power electric network and the IT network, applied in grand scale.

Currently the grid in which just primary substations were connected to the central dispatch has given way to a distributed approach, where thousands of points (secondary substations, overhead lines, points of supply…) can be monitored in real time, offering benefits such as a better knowledge of the network in a world in which renewables, distributed generation and electrical vehicles are beginning to be worth to be considered. The key breakthrough to achieve this is the availability of widespread communications capabilities in order to communicate any field RTU or sensor device with a central system.

However there is a new challenge. WAN (Wide Area Network) communications infrastructures must be designed in order to provide the required services in thousands of sites instead of hundreds. The definition of the architecture of this network becomes the critical choice in these projects, as it determines many factors for the overall system, including deployment and operation costs, services that can be supported, scalability of the system…

This work will present comparatively three different case studies. It will analyse two different WAN architectures already used in real Smartgrid projects in Europe, and an architecture currently being used in India in another real project.

This paper describes each of these architectures, and compares them in terms of ease of deployment, scalability, performance, complexity, cybersecurity, maintenance, deployment cost and operation costs. It also analyses their particularities related to their regional characteristics.

2. CASE STUDY #1: SMARTGRIDS COMMUNICATION NETWORK ARCHITECTURE IN EUROPE (A)

Replacing the traditional electricity meters with the new smart meters has been a challenge to the utilities in Europe. New European regulations [1] require the introduction of smart meters in order to encourage consumers to play an active role in the electricity market and thus improve energy efficiency. Utilities have made great efforts to develop solutions for every situation in the electrical grid, which had not been designed to take into account communications needs.

Taking advantage of the European regulations utilities have included in their development planning not only the replacement of meters but also introducing sensors, control remote units, grid monitoring, which make the data information for the utility (for billing, controlling and monitoring) big and decentralized enough to require the deployment of a completely new communication network. The solution must be cost effective, scalable, easy to deploy, reliable and cyber secure. Even more so when some of the functions associated with the Smart Grid concept need communications in real time. In such situations, the requirements for the telecommunications are a great challenge.

The first case study of a European utility is a major smargrid deployment. Its goals are to replace roughly 10 million traditional meters with smart devices; and adapt over 50.000 secondary substations, which will be equipped with remote management, supervision and automation functionalities.

Cellular network technology such as General Packet Radio Service (GPRS) or 3G has been selected for building the access network; however other technologies such as MV PLC and xDSL are also present. Today, cellular is the most successful and wide spread used communication infrastructure. It has been adopted by more than 5 billion subscribers worldwide (both, human and machines). A large ecosystem is built upon chip makers, device manufacturers, network infrastructure vendors, and services providers. Besides being a mature technology, it has been constantly evolving in order to achieve performance and scalability breakthroughs, and is globally preeminent.

The first European case study uses a WAN architecture based in advanced site-to-site VPN. In every distribution substation an industrial GPRS router is used to transmit all the traffic from the distribution substation equipment to the utility central site. Given the number of distribution substations to be updated the ease of deployment was also considered as a key factor in the communication network design.

The communication will be available between the cellular (GPRS/3G) routers and the utility central site. The communication between cellular routers is not allowed. This type of topology is known as spoke to hub, where spoke refers to GPRS router and Hub is for the equipment needed in the utility central site (see Figure 1). Note that the links between the hub and the spokes may represent other technologies than cellular (such as xDSL or MV PLC) without significant impact in the architecture.

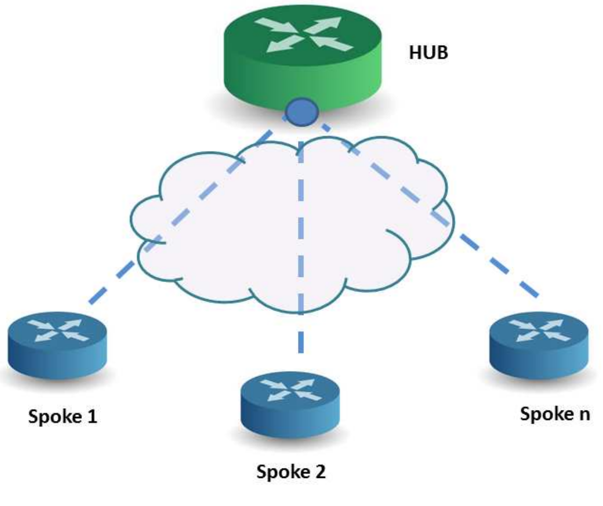

Figure 1. Spoke to Hub communication architecture

The architecture described is known as DMVPN, Dynamic Multipoint Virtual Private Network. In addition to providing a secure path for communications it facilitates the deployment of the communication network. DMVPN relies on two proven technologies:

- Next Hop Resolution Protocol (NHRP) creates a distributed mapping database of all the spoke tunnels to real IP addresses (public interface, cellular operator given). This database is stored in the Hub.

- Multipoint GRE tunnel interface is used in the Hub to communicate with every Spoke. IPsec tunnels are also established between the spokes and the Hub, using the public IP address. A static, known IP address is configured in the Hub, so that the Spokes can establish the IPsec tunnel. Spokes will have dynamic IP address obtained from the cellular operator.

In the hub Dynamic Tunnel Destination simplifies support for dynamically addressed spokes, because each spoke uses NHRP registration through the IPsec tunnel established to transmit the mapping between the dynamic IP address and the NHRP address (this NHRP address is given by an IP addressing plan known for every spoke).

The GPRS router provides access to the local subnetworks attached to it, which makes necessary a dynamic routing protocol to publish the proper underlying subnetworks. In this case study RIPv2 is used as dynamic routing protocol because of its simplicity, having in mind that there is very few segments path between the interconnecting subnets (LAN inside the DT and the central systems). Once the spokes publish their subnetworks the Hub updates its routing table, so all the routing information is stored in the Hub, from where every subnetwork will be accessible.

Summarizing the advantages of DMVPN architecture as presented in this case study for a Smartgrid communication network are the following:

- Automatic IPsec triggering for building an IPsec tunnel from the GPRS router to the equipment in the central site.
- It facilitates zero-touch configuration for addition of new GPRS router and equipment in the distribution substation, because they will be accessible from the central site as soon as the GPRS router obtains a public IP address.
- Addition of spokes requires no changes on the central site configuration. There is no need to configure any security context in the tunnel termination servers each time a new GPRS router is commissioned.

In order to achieve high availability communications, two backup solutions are provided. The GPRS router has dual SIM support for connection redundancy and independence from the availability of a single cellular operator. Additionally every GPRS router defines two Hubs to establish communication with. One Hub is configured as the default route, but if it fails, the second Hub will be used instead of the former. Figure 2 presents the DMVPN architecture with double Hub, considering one SIM connection, as it is used in this real case study.

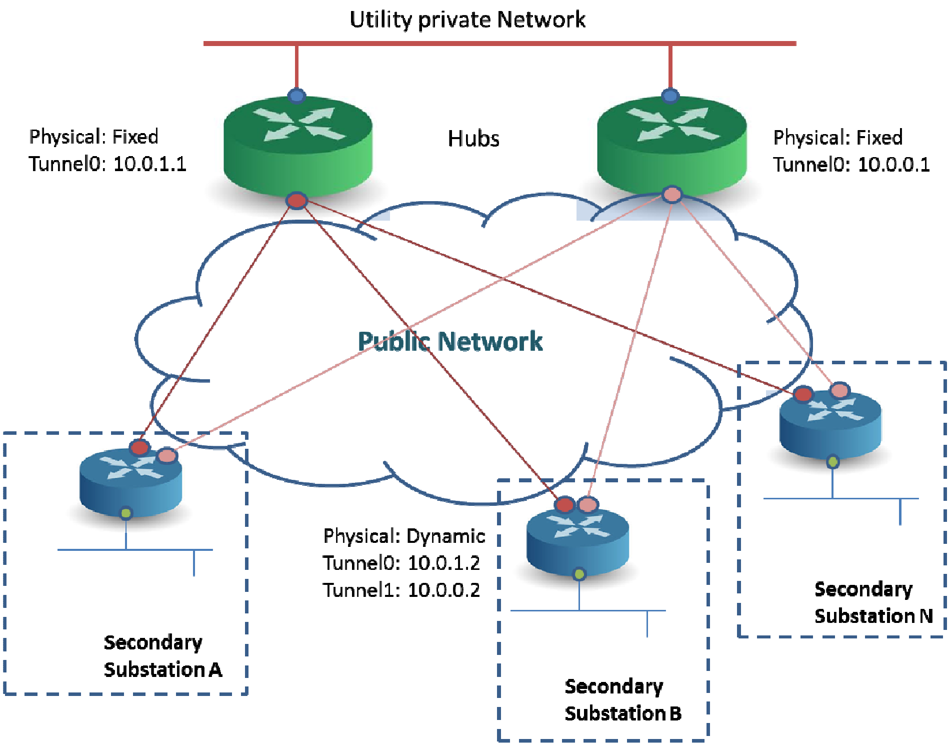

Figure 2. DMVPN architecture with double Hub

3. CASE STUDY #2: SMARTGRIDS COMMUNICATION NETWORK ARCHITECTURE IN EUROPE (B)

An alternative to the implementation of Ipsec in terminal equipment is to use the cellular (GPRS/3G) core network and the services provided by the cellular network operators in order to achieve tunneling and VPN features. This is the solution adopted in several smartgrids projects in Europe where thousands of distribution substations must be provided with communication elements, and cellular coverage and availability are nearly ubiquitous. In this case the complexity of network availability and security management is inside the operator network, as opposed to the first case study.

GPRS/3G is selected as communication technology due to the matureness of the core network equipment and the offered services; meanwhile the carrier network provider is responsible for managing the set up for VPN connection in this type of tunnelling. The GPRS core network is the central part of the GPRS which allows 2G, 3G and WDCMA mobile networks to transmit IP packets to external networks, such as Internet or a corporate network.

The main elements of the packet switched cellular core network are the System GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) [2]. The GPRS SGSN performs mobility management, implements authentication procedures and routes packet data. SGSN is the node to which mobile devices attach via the base station. The SGSN performs session management and status control. It detects new GPRS devices in a given service area, processes new subscriber registrations, and keeps records of their locations in that area.

The GGSN is the gateway node between Public Land Mobile Network (PLMN) GPRS Backbone Systems and external data networks. It terminates the GPRS Tunneling Protocol (GTP) tunnels running over IP-based backbones between the GGSN and the SGSN to which the device is currently attached. The GGSN also provides functions including Authentication, Authorization and Accounting (AAA), address management, and advanced IP services.

The interconnection between private GPRS networks and corporate IP network of the utility is made using non-transparent access mode based on L2TP protocol (RFC 2661). L2TP operates in compulsory mode in which tunnels are supported by the service provider network equipment (GGSN), not needing the GPRS router in distribution substation to implement any protocol. L2TP compulsory service operation is made possible in GRPS and UMTS CN by the R'98 and RR '99 standards (PPP-relay case). In order to support this option, GGSN must support PPP-based PDP contexts. In this case, the GPRS router installed in the secondary substation must include a SIM provided by the cellular network operator to access the utility central site by first attaching to the GPRS network and then initiating PPP session and specifying Access Point Name (APN) that must match the one assigned to the utility's VPN.

In compulsory service operations, the wireless operator assigns an APN network identifier to the utility. This APN is used by the SGSN to select the GGSN to be addressed for every GPRS router. Once the PDP context is active, the control of the communication session is passed to the L2TP Access Concentrator (LAC) supported by GGSN, which triggers the establishment of a L2TP connection to the corporate L2TP Network Server (LNS) and performs GTP-to-L2TP tunnel switching. It is remarkable that newly-attached GPRS routers can share previously established L2TP tunnels by creating new L2TP sessions within those pre-established tunnels. If the tunnel does not exist, a new tunnel will be created. The GGSN/LAC then uses the L2TP control connection to establish an L2TP call (L2TP tunnel to carry PPP) between the LAC and the LNS. Using the services of the utility AAA system, which will be a RADIUS server, the LNS performs the authentication of the GPRS router. Following authentication, an IP address is assigned to the GPRS router using IPCP. For corporate network management purposes, using private corporate intranet IP addresses is preferable. It also saves carrier's limited number of public Internet addresses.

The described architecture for this second case study can be observed in figure 3:

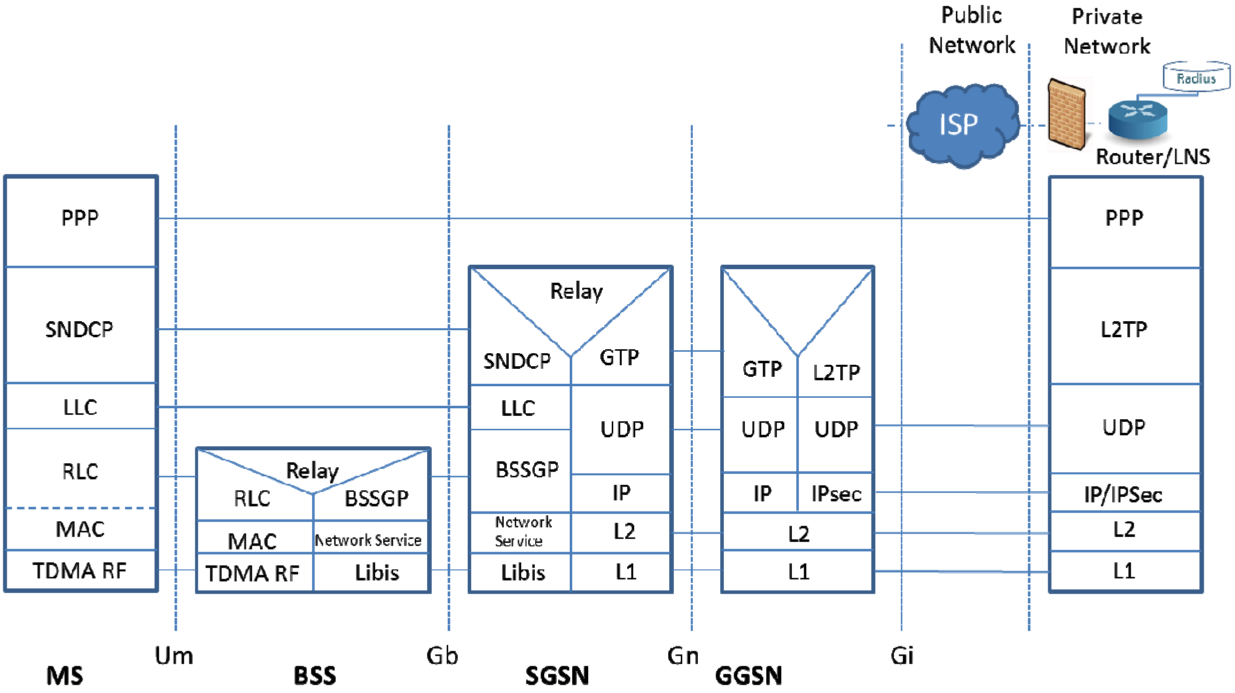

Figure 3. L2TP based VPN

The advantages of this solution include:

- Much easier configuration of GPRS routers in distribution substation.
- The architecture and its complexity rely on the cellular network operators and equipment.
- The IP addressing scheme is controlled by the Radius server in the utility central site.

However, there are some disadvantages too:

- L2TP does not provide full security. Although it can provide secure CHAP-like authentication of the L2TP control connection, tunnel hijacking remains a possibility. To fully secure L2TP tunnels, service providers can use standard IPSec mechanisms independently developed by IETF.
- Regardless of the strength of any link layer security implemented by the communications service provider, without end-to-end VPN security the traffic remains accessible to insiders at the service provider. This can permit legitimate access such as lawful intercept but also can allow unscrupulous insiders at the service provider access the traffic.

4. CASE STUDY #3: SMARTGRIDS COMMUNICATION NETWORK ARCHITECTURE IN INDIA (C)

The Government of India in its XIth plan, through the Ministry of Power, launched the Restructured Accelerated Power Development and Reforms Programme (R-APDRP) [3] in July 2008 in order to greatly improve the distribution grid in towns (cities) fulfilling some eligibility criteria. The main goals are the reinforcement and upgrade of the distribution network in order to improve service, and sustainable loss reduction (including non-technical) to a level of 15%, and the introduction of Information Technology and Automation. Projects under the scheme are taken up in two parts. Part-A includes the projects for establishment of baseline data and IT applications for energy accounting/auditing & IT based consumer service centres. Part-B includes regular distribution strengthening projects and covers system improvement, strengthening and augmentation, etc. About 10 such projects have been recently awarded (2012/2013) by various states in India and are in the early stages of implementation. The following paragraphs will focus on the angle of the design that R-APRDRP projects implement. The communication architecture of these projects is as described in figure 4.

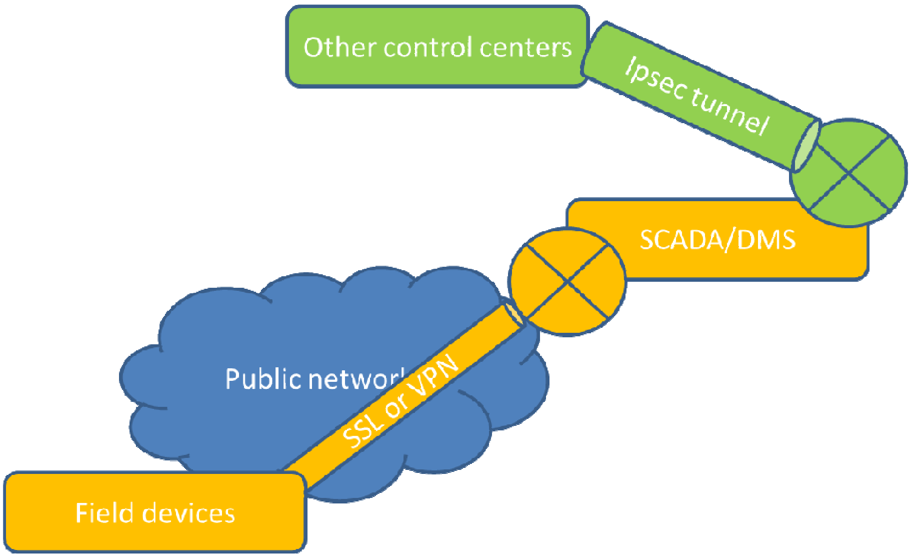

Figure 4. Communication architecture for R-APDRP Smartgrid in India

The communications between the field RTUs and the SCADA systems for operating town distribution systems are usually based on IP communications networks. These IP communications for RTUs and FRTUs (field RTUs) over public networks are encrypted using SSL Security or VPNs. In order to improve security, field equipment authenticates control commands, so only allowed Master IP addresses can be the source of such orders. The RTU, FRTU and all IP based devices whose connectivity relies on a Public Network form a private VPN network with the SCADA Front End, through which encrypted and authenticated data gets exchanged.

The Communication Front End system complies with SSL based security for connecting with IEC 60870-5-104 &101 nodes on public networks (IEC 62351). Further the nodes and Communications Front End CFE are NERC/CIP compliant. The Front End Processor exchanges encrypted and authenticated data through secured SSL/VPN whether it traverses a public network or a private one.

All RTU/FRTU/Fault Passage Indicators (FPI) in a City are connected to the SCADA/DMS Control Center of that City thus having centralized architecture (star). RTU communication Modules support VPN/SSL Security/Encryption of data coming to it through Public network and then send it over private & secure utility network to the SCADA Control Center.

IP routers are used for data exchange of SCADA/DMS control centers with other Control Centers as mentioned below. The data exchanges between the two centres are over IP using Ethernet based communication network on various mediums viz. MPLS/MLLN/Copper etc.
IP central Routers are also required for data exchange of SCADA/DMS control centres with RTUs at various locations in the respective town.

The data exchange between the two centers are primarily over MPLS based secured network using IP on various mediums as per the requirement and availability in the respective project area viz Fiber Optic, Radio, etc.

The Wide Area Links are designed for 2Mbps or higher Bandwidth capacity. The Routers support IP/MPLS features and Layer 3 MPLS VPN connection and PPP/Frame Relay transport over MPLS. In this way, advanced quality of services features can be set up.

5. COMPARISON OF THE PRESENTED CASE STUDIES

The following table summarizes the comparison of the three presented case studies in relevant areas for the communication architecture.

As already mentioned in the case study descriptions, case studies A and C implement similar architectures in terms of VPN end to end security solution implementation, while case study B offers an approach based on features provided by a 3rd party company (mobile operator). Case studies A and C represent a more, reliable and secure solution at the cost of deploying routers with advanced VPN features and dealing with a significantly more complex logistical process.

When comparing case studies A and C, A might be a more complex solution (due to the utilization of DMVPN), and also it requires fully customized per-site configurations, but lets the utility have full control over the communication architecture, communications means (different networks can be used simultaneously) and provides minimal external dependencies.

	European case A	European case B	Indian case C
Field device deployment complexity	Low (plug and play architecture) All routers have the same conf.	Medium – each router is configured independently – provisioning required	Medium – each router is configured independently for interconnecting field devices to control centres.
Scalability	Medium	High	Medium
Performance (Application layer throughput for the same physical links)	Medium	High	Medium
Communication reliability	High (redundancy provided by the Utility)	High (redundancy provided by the operator)	High for interconnecting Control Centres (MPLS)
Flexibility	High (any WAN technology)	Low (Just GPRS/UMTS)	High (any WAN technology)
Dependence on 3rd party	Low	High (GPRS / UMTS operator)	Low
System Complexity	High	Low	Medium
Cybersecurity	High	Medium (not end to end)	High
Logistical complexity	High (highly customized field configurations)	Low (standardized field configurations)	Medium (customized field configurations)
Equipment complexity	Medium (VPN support is a must)	Low (simpler routers)	Medium (VPN support is a must)
Operational costs	Low	Low	Low

Table 1: Case study Communication architecture comparison

6. CONCLUSIONS

The real time requirements imposed by smart grids, their geographical dispersed nature, and their sheer size in terms of communication endpoints, will ultimately determine the new telecom networks that the utilities need to deploy. The main challenge is in the access side, where electrical Utilities usually rely on services provided by public network operators.

As discussed in this paper, utilities share the main requirements they expect from the public network operators:

- **Cybersecurity** is one of the main concerns when critical data such as telecontrol traverses a 3rd party network. Data integrity and data authentication are considered the most important requirements for RTUs. When customer revenue metering data is involved, data privacy is also a critical requirement.
- **Reliability**. Utilities are requesting different redundancy approaches, depending on the criticality of the information. Usually VPN servers are redundant due to the big impact of a failure in such a critical device. When dealing with field WAN router redundancy, different policies can be followed. Not all the utilities require network carrier redundancy.
- **Cost**. Cost is the critical requirement in distribution, due to the number of endpoints. For this new telecom network where hundreds of thousands new installations may be involved, capital and operation expenditures are critical.
- **Network monitoring**. The packet switched public networks will allow utilities to monitor service availability. In this way, SLAs can be assessed by the utility on its own, independently of the information provided by the public network carrier.

After the analysis of the case studies, a primary conclusion is that cellular technologies are a reality for smart grids applications. Not only it is the most cost effective telecom infrastructure, but also all stakeholders, manufacturers, utilities and public operators now understand how to successfully operate this wireless infrastructure.

Network carriers are starting to understand the requirements of the utilities beyond effective pricing plans as the only requirement. Service Level Agreements, cyber security and service monitoring tools are also becoming part of their offer.

Utilities are also adapting their legacy private networks to enable interconnection with public networks in a holistic way, making its architecture independent of the cellular packet switched technology evolution (GPRS, 3G, HSPA, LTE…).

Telecom equipment manufacturers are launching robust products that incorporate the requirements of the field electricity distribution application. These are not wireless routers, but robust, reliable and cyber secured routers that can be easily integrated with both public carrier networks and utility private networks.

BIBLIOGRAPHY

[1] EC Directive 2009/72, “Common rules for the internal market in electricity and repealing Directive 2003/54/EC”.

[2] 3GPP Mobile Broadband Standards Series, http://www.3gpp.org/specifications.

[3] R-APDPRP, Restructured Accelerated Power Development Reforms Programme, Ministry of Power, India, XIth plan, http://www.apdrp.gov.in.