MOVING TOWARDS AN ADVANCED AND SECURE COMMUNICATION INFRASTRUCTURE FOR THE SMART GRID SECONDARY SUBSTATION

Francisco MELO
EDP Distribuição – Portugal
francisco.melo@edp.pt

Luís MATIAS
EDP Distribuição – Portugal
luis.matias@edp.pt

Nuno PEREIRA
EDP Distribuição – Portugal
nunoemanuel.pereira@edp.pt

ABSTRACT

The two main classic vectors a regulated DSO faces from a holistic perspective are the Quality of Service and the Operational Efficiency. The call for improvements on these are indeed the typical trigger for most of the changes and evolutions on the sector, most notably for the current (and the most famous!) undertaking which aims a smarter grid. At a micro level, and focusing on the secondary substation, which for the macro process assumes a pivotal role, the same reasoning applies. Therefore, it is not of a surprise the push towards an integrated, advanced and secure communication infrastructure for the smart grid secondary substation. This enables to target the Operational Efficiency through the integration of services formerly implemented in a silo mode, while embracing a higher Quality of Service by making use of the new tools and processes the new integrated infrastructure brings into the equation.

INTRODUCTION

The electrical distribution grid is considered one of the most critical infrastructures in industrially developed societies. Hence there is an increasing awareness and concern regarding its security and protection against cyber threats. Furthermore, this infrastructure is geographically scattered across large areas, which brings additional technological challenges for two of its main pillars: communications and security.

These pillars become even more relevant while walking through the smart grid path. Here the electrical distribution system becomes managed through an advanced two-way communications network enabling deeper remote monitoring and control of power equipment through DMS/SCADA. Currently the major challenge is to bring the latest monitoring, AMI and DA functionalities to the LV layer while promoting a smooth transition towards a smarter grid.

EDP Distribuição (EDP Group), Portugal, manages and operates more than 400 primary substations (all remotely controlled), over 60.000 secondary substations (more than 2.000 are remotely controlled) and over 6.000.000 clients that, in the near future, will all have a smart meter in their premises (nowadays walking towards 140.000).

Several non-integrated solutions in classical silo approach, usually found in the secondary substation, use dedicated communication equipment and resources for the WAN section: i) remote metering for public lighting and for the transformer, ii) data concentrator for local smart metering management and iii) remote terminal units (legacy equipment) for remote control of MV cells in the secondary substation. Each of these solutions requires dedicated modems for the communication with different central systems, which is implemented through different Public Land Mobile Networks (PLMN). However, these services are not aligned with the most advanced smart grid requirements for performance, efficiency, scalability, reliability, resilience, security and privacy.

This paper describes the concept of an advanced communications front-end for EDP Distribuição's secondary substations – implemented over a router – that provides a superior, secure and integrated solution to support smart grid monitoring, AMI and DA functionalities, regarding the WAN segment. Moreover, a smooth transition and integration of legacy solutions is enabled through transparent support for serial communications; namely for public lighting and transformer meters (Figure 1).

The routers are being integrated with the central systems through advanced VPN technology over a private APN. The former delivers a secure and reliable network between the remote routers and the VPN concentrators located in the edge of EDP Distribuição's core network.

Regarding the Network Operations Center, routers are also being integrated into a NMS, allowing overall supervision. Additional information is planned to be retrieved for KPIs monitoring and also for integration with a Security Information and Event Management system.

Besides benefits as efficient secondary substation communication management and increased network awareness, this concept is also cost-effective as it brings an OPEX reduction. Namely through the reduction of communication costs associated with the number of SIM cards and via maintenance costs reduction due to enhanced remote management capabilities.

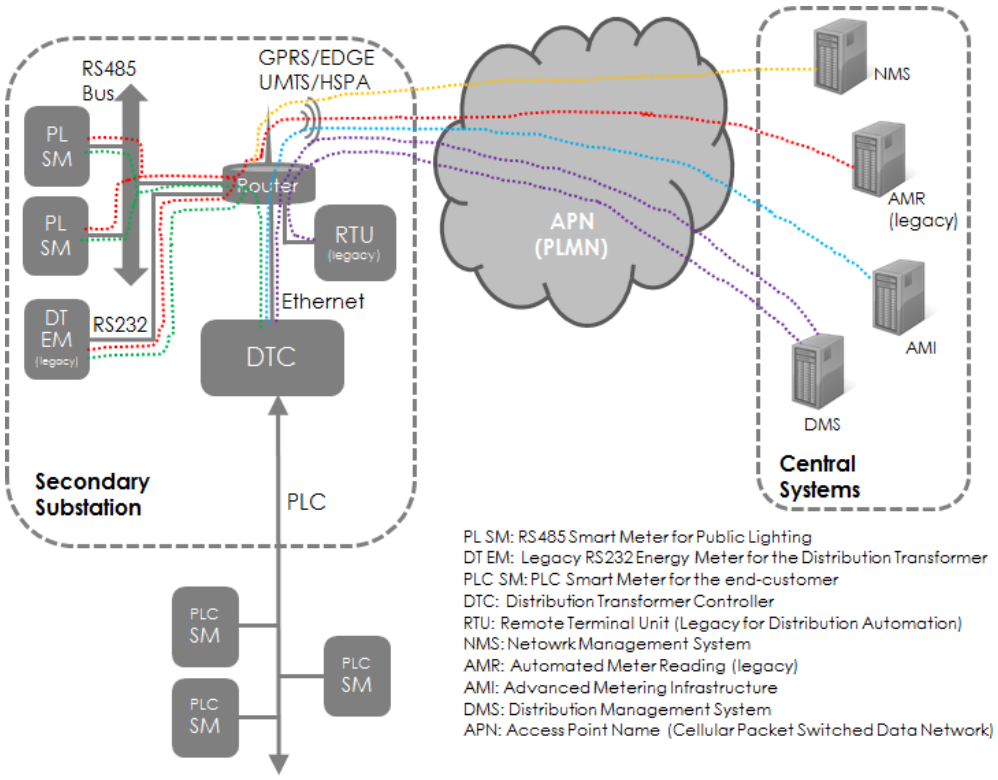

Figure 1 - Secondary Substation Communications' Architecture

A proof of concept was carried, on the lab, in order to assess its feasibility. The overall concept is being validated through a pilot touching 138 secondary substations, expected to be completed by 1H2014. Building up on the latter, a complete rollout is expected to extend this solution to the remaining fleet until the end of 2015.

PROJECT DESCRIPTION

The national mandate for the deployment of telemetering in every secondary substation, ahead of the smart grid roll out, imposed a deep analysis on how to better accommodate the first while also considering the later arrival of the second, hence maximizing the long term benefit-cost ratio. For this a number of different scenarios, including transition scenarios, were assessed. Additionally an European benchmarking was conducted in parallel. All this together led the EDP task force in charge of the project to define an overall solution enabled by an industrial grade router with support for legacy interfaces as depicted in Figure 1.

Classical Scenario

Up until now, the typical implementation has followed the well-known and classical silo mode where secondary substation meters, AMI equipment – Distribution Transformer Controller (DTC) [1] – and DA equipment – Remote Terminal Units (RTU) – do require dedicated communications solutions to link them to the central systems (Figure 2).

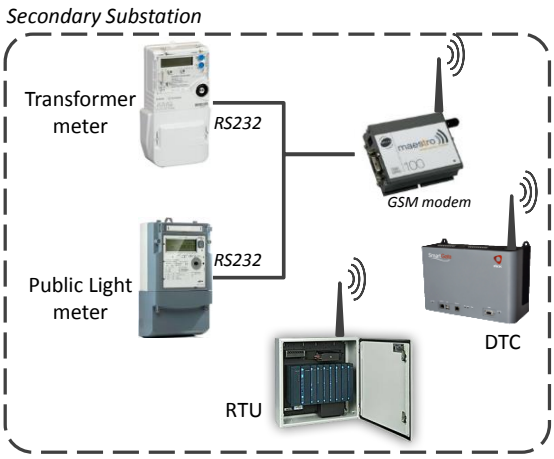

Figure 2 – Classical scenario

Initial Scenario

The initial scenario for deployment of the presented concept should intersect the secondary substation telemetering process, thus integrating this service at the very beginning by supporting the communications between classical energy meters and the long existing AMR system (Figure 3).
These communications are going to be implemented over a Packet Switched Data (PSD) network, whereas the classical silo approach for this service was going through the old Circuit Switched Data (CSD) infrastructure, which is unable to deliver the same management and security tools the former can.

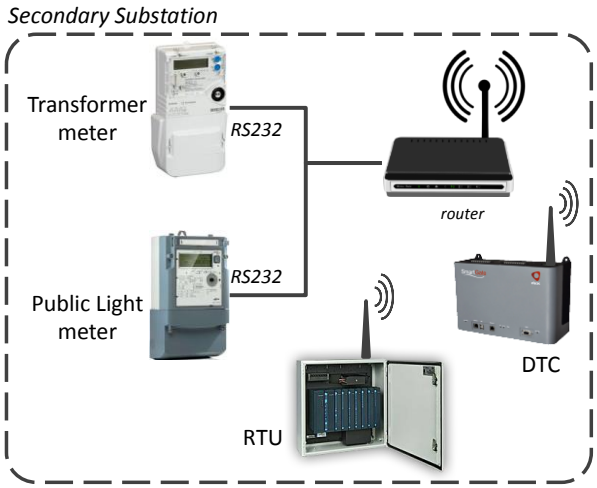

Figure 3 – Initial scenario

As the classical meters' interfaces are of legacy nature, typically RS232, and so fitted for CSD, this imposes that the router shall act as a transparent gateway between the serial domain and the PSD world [2].
On top of it, due to the fact that different, not synchronized, HDLC Primary Stations may access the serial link using a DLMS/COSEM over HDLC protocol stack [3] (Figure 4), the router needs also to control the access to it, limiting to just one active access at given point in time.

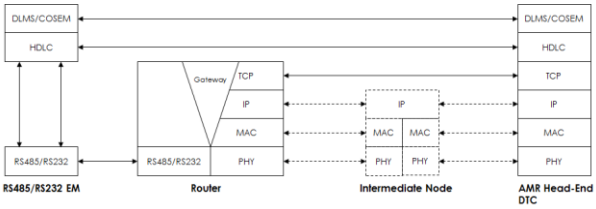

Figure 4 – Protocol Stack

Final scenario

The final scenario, which should be achieved after the smart grid roll-out, encompasses the main services the new and advanced infrastructure is going to integrate, i.e. not only the initial telemetering service but also the latest AMI, grid monitoring and DA services (Figure 5).

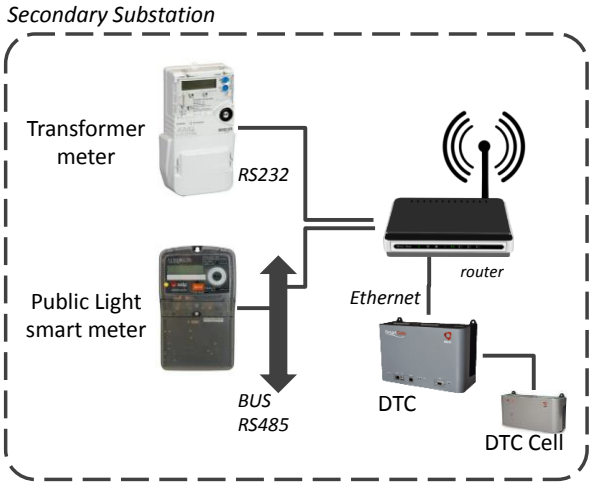

Figure 5 – Final scenario

Besides the expected communication flows between the central systems and devices inside the secondary substation, the router also allows and manages communications between devices that are within the secondary substation, namely between Distribution Transformer Controller (DTC) [1] and meters.

Major requirements

These two last evolution scenarios define the main high level requirements for the front-end router. Namely, the interfaces and the system level aspects. Regarding the former, one has the WAN interface that should be delivered, most of the cases, through an integrated 2G/3G cellular modem. For alternative and evolutive options for connectivity an ethernet WAN port is also allotted. The local interfaces are composed by the serial interfaces and LAN ethernet ports. The first for the meters, RS232 for the legacy ones, RS485 for the Transformer Area Network (TAN) smart meters. The number of LAN ethernet ports is directly related to the number of transformers, as each transformer will call for a DTC. Additionally, sensors deployed in the secondary substation may be connected to the router in order to inform alert the central systems. Different types of sensors are being studied (oil and environment temperature, open door, water flood, etc.).
At system level, the support for Networking and Security protocols are of paramount relevance because these are the enablers for the new tools, which will bring in higher Quality of Service.

PROJECT DEVELOPMENT

From the main requirements enunciated in the previous section, a short-list of potential routers was chosen for a Proof of Concept. This was carried in EDP's smart grid laboratory in Lisbon. A reference scenario (Figure 6) and a test protocol were defined in order to have solid and comparable results. The laboratory stage has proven to be fundamental, not only to better assess the different solutions at stake but also to capture more knowledge in a new frontier.

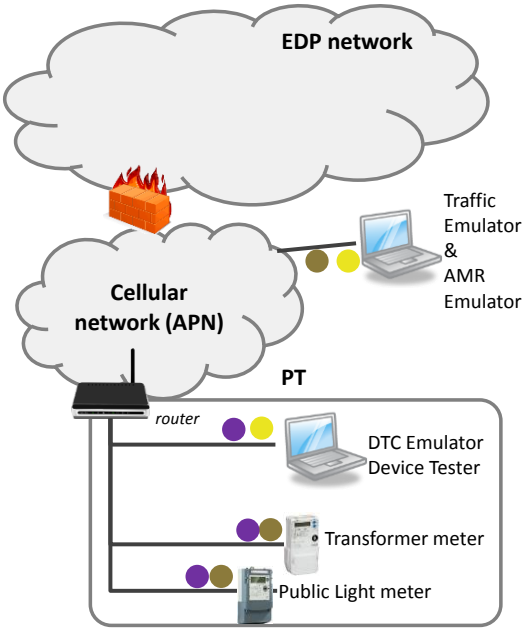

Figure 6 – Proof of Concept scenario

Additionally, it has allowed the task force to choose the different equipment that are now being deployed in real secondary substations in the field as part of a Field Trial that will look in more detail to the Network level as well as to the robustness angle (Figure 7).

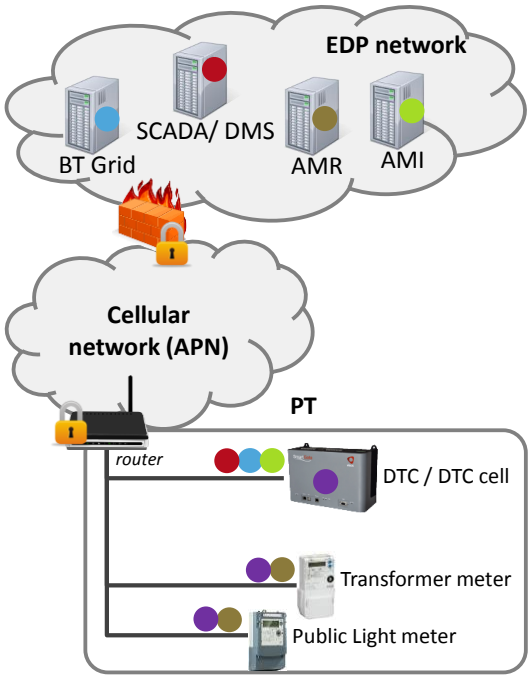

Figure 7 – Field Trial scenario

Network Architecture and Security

Smart grid's systems, AMI, monitoring and DA, require communications to come to the secondary substation level in order to provide advanced functionalities that enhance network visibility and the grid automation level. However, while contributing to increasing operational effectiveness and network efficiency, these developments add new equipment and information flows, valuable assets that broaden the network's attack surface area and raise new security concerns, especially if implemented in classical silo mode. Therefore, new security requirements are necessary in order to strengthen network security at secondary substation level. These can be better attained with an integrated architecture, where the front-end would have enhanced security and networking capabilities.

Traditional service implementation, as it was introduced at an earlier point, consists of several parallel solutions each with its own dedicated communications module. The different network solutions have different characteristics and priorities that require different security approaches. Incorporating all these network equipment presents security limitations, which constrains compliance with the new security requirements.

The network architecture presented in this paper, supported over a router, allow to overcome these constrains. The chosen communications module, i.e. the router, supports additional security features. Human and machine authentication uses access control security policies. WAN communications between the router and the central systems are protected through secure channels using VPN technology, namely IPSec, over a private APN (Figure 8). Different VPN configurations are being tested during the Field Trial. Also, different technologies are being studied like DMVPN and OpenVPN.

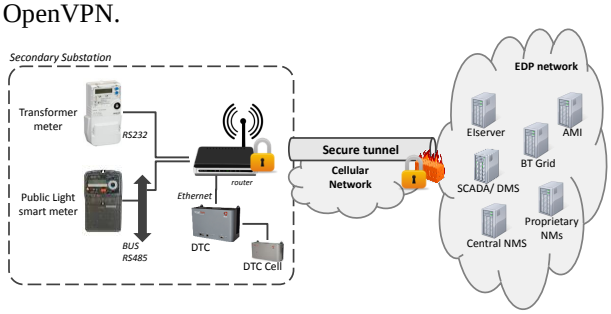

Figure 8 – Reference Architecture

This is a scalable security solution from which resulting security requirements and reference architecture for distributed network equipment should be captured to be translated into future network developments.

Network Management

Regarding the Network Operations Center (NOC), routers will be visible to a central Network Management System (NMS), allowing overall supervision. This system will receive messages from proprietary NMSs or directly from routers. The usage of proprietary NMSs allows the NOC to retrieve additional information useful for management. The messages between routers and the NMSs will be exchanged over Simple Network Management Protocol (SNMP), being it for events (traps) or for configuration (get/set commands) (Figure 9). In addition the Field Trial will allow to better define the final list of interesting traps, as well as to better define the final Management Information Base (MIB).

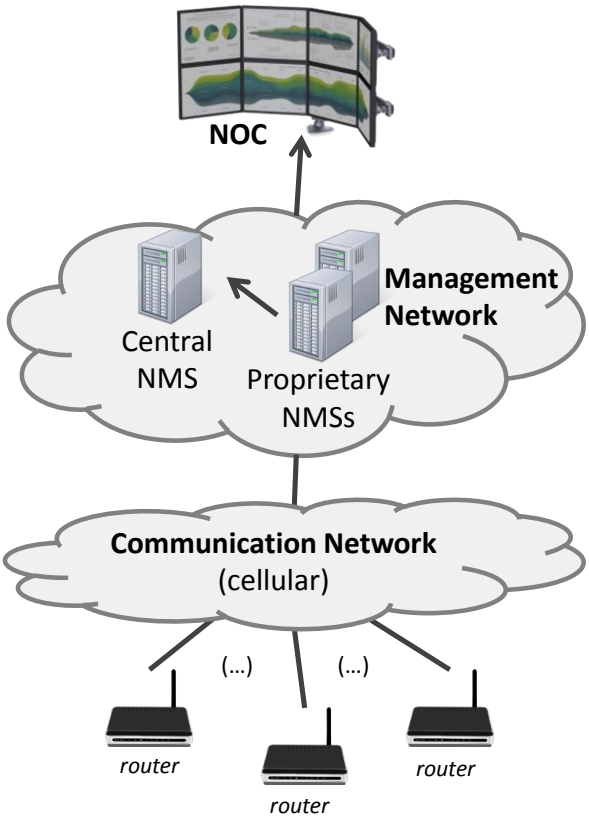

Figure 9 – Network Management Architecture

The NOC will monitor, amongst others, link status and cellular connections. It's important to identify if carriers are delivering a good level of service, that is, availability and bandwidth are according to the SLAs.
The NOC should be able to identify communication problems between the router and the linked equipment. Therefore, supervision is extended to the devices that are inside the secondary substation giving NOC the option to remotely actuate when possible. Security is a top concern and, despite IPSec connections, the physical ports from the router are being monitored in order to identify unauthorized connections. Additional information from the router is planned to be retrieved for integration with a Security Information and Event Management system to analyze and identify unexpected behaviors and patterns.

Next steps

A public tender is expected to be launched during 2Q2014 for routers acquisition. Specifications are going to be concluded after retrieving and analyzing Field Trial results. Routers must fit technical and environmental requirements. There are a few points to be assessed and closed as for instance the power supply specification, which must be reliable enough to bear strong discharges/surges. Another point is the antenna side, which also encompasses cables and accessories, this is necessary to ensure a strong cellular signal quality.

CONCLUSIONS

Being a forefront runner makes this a very innovative project, but in addition it also brings many interesting challenges. It calls for the coexistence of legacy and leading edge equipment, for new ways of mass deployment, for integration with several central systems, for advanced security mechanisms and for new management platforms and processes.
The router will replace up to 3 modems per secondary substation. A reduction in operational costs (OPEX) is expected as well as for maintenance costs through a better supervision and management over the communications between the secondary substation and the central systems. Additionally, a new layer of security will bring robustness and reliability while ensuring privacy and protection for automation and metering data.

REFERENCES

[1] F. Melo et al., "Distribution Automation on LV and MV using Distributed Intelligence", Proceedings CIRED Conference, 10-13 June 2013, Stockholm, Sweden.
[2] A.F. Molisch, "Wireless Communications", 2005, John Wiley, Chichester, UK
[3] DLMS User Association, "Device Language Message Specification".