SMART GRID PROTECTION AND AUTOMATION ENABLED BY IEC 61850 COMMUNICATIONS OVER 5G NETWORKS

Ana ALEIXO
Efacec – Portugal
ana.aleixo@efacec.com

José CABAÇA
Altice Labs - Portugal
cabaca@alticelabs.com

Pedro Miguel NEVES
Altice Labs - Portugal
pedro-m-neves@alticelabs.com

Rui DIAS JORGE
Efacec – Portugal
rdjorge@efacec.com

Rogério DIAS PAULO
Efacec - Portugal
rdpaulo@efacec.com

Alberto RODRIGUES
Efacec - Portugal
arodrigues@efacec.com

ABSTRACT

The present paper is centred on the ongoing work that is currently being carried out by Efacec and Altice Labs within the scope of the H2020 5G-PPP SliceNet project [1]. SliceNet aims at designing and developing a vertical-business-oriented 5G framework capable of addressing the demanding requirements of future network services. Efacec is contributing, with the collaboration of Altice Labs, with a practical use case that settles on distributed coordinated protection and self-healing solutions for energy distribution networks, based on IEC 61850 device-to-device (D2D) communications.

INTRODUCTION

The increasing demand for power supply Quality of Service (QoS) has motivated utilities to extend Protection, Automation and Control (PAC) beyond the substation, increasing the number of devices with monitoring and protection capabilities deployed along the power distribution network, and using such devices to implement protection and self-healing schemes. The lack of a high-performance, reliable, and cost-effective wireless network with the required geographical coverage has been one of the major barriers to the implementation of very-high-speed protection and automation schemes outside contained substation environments.

5G-PPP states that 5G communication technologies will be focused on providing high Quality of Experience (QoE) not only for consumers, but also for industrial stakeholders with specific needs regarding wide-area communications [2]. The 5G infrastructure will be designed with native support for mission-critical services with high-demanding needs such as very high bandwidth, very high reliability, very low latency, and/or massive machine communications.

The SliceNet project aims not only at developing a vertical business centred communication infrastructure, but also at designing highly customizable Plug & Play (P&P) services that will enable a straightforward deployment of the vertical solutions and will substantially increase their scalability and reduce operational efforts. Integrating PAC Intelligent Electronic Devices (IED) in a controlled 5G ecosystem will provide an opportunity for exploring the viability of using these state-of-the-art communication technologies for demanding distributed PAC algorithms based on mission-critical low-latency communications.

Since the presented use case relies on using Internet Protocol (IP) layer 3 extensions of widely used IEC 61850 protocols for D2D communication, such as Routable-Generic Object Oriented Substation Events (R-GOOSE) and Routable-Sampled Values (R-SV) [3], it will be possible to analyse the feasibility of using these protocols, which were originally designed for Ethernet layer 2, in a Wide-Area Network (WAN) that boasts being capable of supporting ultra-Reliable Low-Latency Communication (uRLLC) across multiple domains. Furthermore, testing Distribution Automation (DA) solutions in this laboratory-based framework will allow measuring and monitoring QoS/QoE under simulated extreme network conditions.

The use of 5G technologies will propel the implementation of advanced distributed solutions reliant on the high-speed transmission of power system quantities, such as line current and voltage values, that are currently dependent on the existence of a physical communication infrastructure.

The work being carried out by Efacec and Altice Labs in the scope of the SliceNet project will study the viability of using 5G networks for demanding communication-based DA algorithms that include Phasor Measuring Unit (PMU) based differential protection and high-speed protection coordination.

This paper centres on presenting the ongoing work, on describing the smart grid self-healing use case and lab-based testbed in which these DA solutions are being simulated and validated, and on exposing the outcome expected from the upcoming project phases.

USE CASE DESCRIPTION

The Smart Grid Self-Healing use case brought forth by Efacec and Altice Labs in the scope of the SliceNet project centres on distributed automation and protection solutions for the power grid. This vertical sector use case comprises three complementary scenarios, ranging from automatic power grid reconfiguration using IEC 61850 R-GOOSE for IED coordination to PMU-based differential protection.

The use case considers a Medium Voltage (MV) network topology with two feeders connected by a Normally Open (N.O.) recloser. The self-healing scheme includes a total of five IEDs: two multi-function relays controlling substation circuit breakers and three recloser controllers placed along the feeders. This setup will be reproduced in a laboratory environment and will be used for testing and validating three different DA applications, that are further described in three scenarios. Figure 1 portrays an example of the MV network topology considered for the use case.

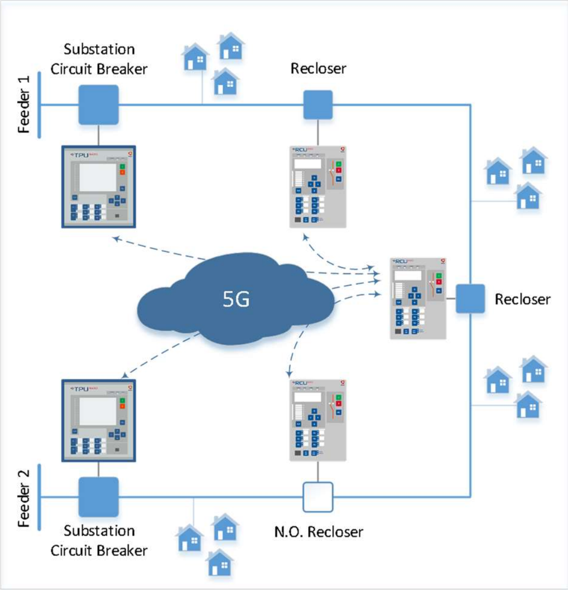


Figure 1. Smart grid topology considered for the use case.

The DA algorithms considered for all use case scenarios are fully distributed and rely solely on D2D communication, thus taking full advantage of the 5G technologies being developed in the SliceNet project. It is noteworthy that a significant set of the requirements imposed by these applications is not complied by currently available WAN radio technologies, including 4G, and thus 5G will allow utilities to explore and implement other solutions besides the centralized or semi-decentralized algorithms running in the command centre and/or substation.

Scenario 1: Protection Coordination

Protection coordination throughout the power system is of paramount importance to ensure reliable, secure and selective fault detection and clearance. Most coordination schemes implemented in power distribution networks do not include the exchange of information between PAC devices due to the absence of an adequate communication infrastructure. Coordination is typically achieved based on time grading and/or analogue measurements analysis with obvious shortcomings, including higher fault clearance time and difficult deployment for complex power system topologies.

The first scenario introduces a communication-based coordination scheme that relies on IEC 61850 R-GOOSE for exchanging messages between smart grid IEDs.

When a fault is detected in the power line, a blocking signal is immediately transmitted to all upstream devices. Consequently, the protection functions in all upstream devices are promptly inhibited, except for the ones running on the device closest to the fault (*n.b.*, this is the sole device that remains unblocked after detecting the fault). This device operates after a parametrized delay, clearing the fault while leaving all healthy upstream line sections energized. The described workflow is represented in Figure 2.

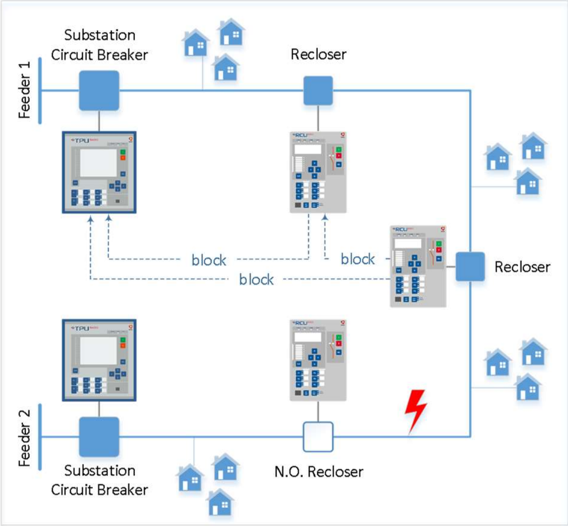


Figure 2. Example of communication-based protection coordination.

In order to ensure selectivity, it is crucial that the upstream devices receive and process the blocking signals before the protection functions operate. Consequently, it is imperative that the D2D communication is not only low-latency but also deterministic.

Scenario 2: Automatic Network Reconfiguration

Automatic power network reconfiguration applications are the core of smart grid self-healing strategies. The main purpose of these applications is to automatically re-energize healthy sections of the power grid from an alternate power source after permanent faults have been detected and cleared.

The second scenario presents a distributed self-healing solution that resorts to IEC 61850 R-GOOSE messaging for high-speed MV loop scheme reconfiguration.

Figure 3 summarily illustrates a loop scheme automation sequence that is initiated after fault detection and clearance, in which IEDs located along MV feeders exchange R-GOOSE messages containing switchgear open and close commands with the purpose of isolating the faulty line section and closing the N.O. point and thus connecting the healthy line sections to the second feeder.

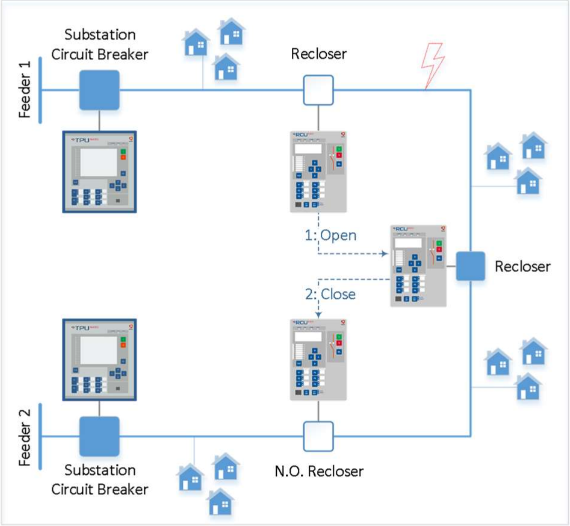


Figure 3. Example of communication-based automatic network reconfiguration.

Scenario 3: Differential Protection

The third scenario presents a differential protection solution that may be regarded as an alternative to the protection coordination strategy presented in the first scenario. Aside from improved accuracy and higher operation speed, differential protection schemes provide an efficient solution for the protection of closed loop topologies in MV networks that otherwise require complex protection engineering. However, these algorithms are computationally demanding and have extremely ambitious communication requirements which presently are not covered by public wide-area radio networks.

The operation principle of differential protection rests on the assumption that, under normal operation conditions, the current that flows into the protected object (*e.g.*, a line section) is equal to the current that flows out of it. This property makes differential protection schemes inherently selective, since the protected zone is clearly limited by the current sensors (*i.e.*, faults outside an IED's protected zone are not detected by that IED).

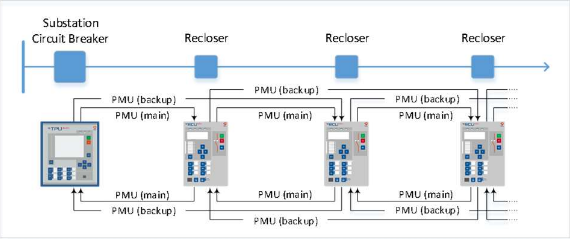


Figure 4. PMU-based differential protection scheme.

The solution exploited in the SliceNet project uses PMU transmitted over IEC 61850 R-SV for the IEDs to compare locally measured phase currents (magnitude and angle) with the values measured by devices located further along the line.

As depicted in Figure 4, all devices that are part of the differential protection scheme are continuously streaming phase current values to the nearest device(s). The solution also considers a backup protection scheme that requires all devices to stream the line current values to other devices that are located further down the line. The backup protection will operate after a small delay if a fault is detected and the main protection fails to act. Failures in the main protection system may result of several causes, such as device malfunction, communication failure, or time synchronization failure.

Communication requirements

The main benefits that smart grid DA applications are expected to attain from the 5G framework and services that are being developed in the scope of the SliceNet project are:

- Ultra-reliable communication infrastructure;
- Low-latency D2D communication;
- Deterministic communication;
- Secure communications between smart grid devices, focusing on the Operational Technology (OT) cybersecurity principles that favour availability and data integrity over confidentiality;
- QoS and QoE under all network conditions.

The analysis of the proposed use case scenarios resulted in a set of requirements for the 5G communication network intended to support the corresponding DA applications.

Table 1 includes the requirements considered of greater relevance for event-driven R-GOOSE communications and for synchrophasors transmitted over R-SV.

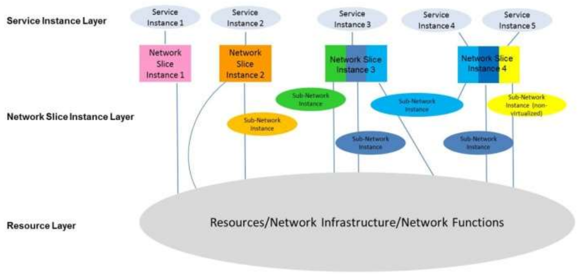
Requirements	**Event-driven**	**Synchrophasors**
Availability/reliability	99.999 %	
Wide-area coverage	Yes	
Connection density	< 0.5 devices/km^2	
Multi-domain slicing	Yes	
Mobility	No	
E2E latency	≤ 10 ms	≤ 5 ms
Data rate, per device	< 20 Mbps	< 2 Mbps

Table 1. Summary of use case communication requirements.

Apart from the presented End-to-End (E2E) latency and bandwidth requirements, these smart grid mission-critical applications require an ultra-reliable communication infrastructure. It is important to take into consideration that the electric power distribution network extends over a wide geographical area. The IEDs that implement the referred DA solutions are sparsely distributed along the power grid and some are placed in areas with sub-optimal communication network coverage. The SliceNet project is tackling these needs by designing a multi-domain slicingfriendly infrastructure that will rely on active QoS monitoring in order to ensure the best possible communication network conditions under all scenarios.

NETWORK SLICING

One of the definitions that shows more clearly the Network Slicing concept is the one presented in [4], where it is stated that the network slicing concept consists of three layers: 1) Service Instance Layer, 2) Network Slice Instance Layer, and 3) Resource Layer.



Source: NGMN Alliance

Figure 5. Network Slicing Concept.

1) Service Instance Layer – represents the services which are to be supported. Each service is represented by a Service Instance. Typically, services can be provided by the Digital Services Provider (DSP), that can also take the role of the Network Services Provider (NSP) or a third party entity (*e.g.* a Mobile Virtual Network Operator).

2) Network Slice Instance Layer – a network operator uses a Network Slice Blueprint to create a Network Slice Instance. A Network Slice Instance provides the network characteristics which are required by a Service Instance. A Network Slice Instance may also be shared across multiple Service Instances provided by the network operator. The Network Slice Instance may be composed by none, one or more Sub-network Instances, which may be shared by another Network Slice Instance.

3) Resource layer – represents all the resources, physical and/or virtual, that will enable the creation of the Network Slice.

VERTICAL BUSINESS ORIENTED 5G FRAMEWORK AND SERVICES

Verticals often have diverse and sometimes critical needs, which pose strict and challenging requirements to network operators and service providers on their control and management frameworks for the provisioning of suitable slices and services. Customization is therefore a key aspect for 5G network slicing to offer tailored services, and requires high degrees of programmability and flexibility of the slicing framework. Some of the novelties in the new network slicing concepts are the One Stop API (OSA), the Plug&Play (P&P) and the QoE optimizer that together can enable the E2E slice design/runtime customization and guarantee that the QoE is under the Service Level Agreement (SLA) with the vertical.

The OSA is conceived as the main entry point of the slicing framework. It is the enabler for the engagement of verticals into slice design and provisioning, and it reflects the overall outcome of the multi-domain slicing concept as this is tailored to the requirements for the support of “Verticals-in-the-loop” concept. The diversity of functional, performance and security requirements that may relate with a vertical, necessitates the support of a level of abstraction offered through the OSA. The abstraction aims at enabling verticals express accurately the particular communication/service/application requests that are considered important for the delivery of the end-to-end functionality.

The main goal of the P&P is to expose dedicated and vertical customized control features and capabilities per network slice instance. This will function as a key enabler for the “Verticals-in-the-loop” runtime approach which enables verticals to plug their own control logics and specialize their slices according to their needs, offering significantly enhanced degree of flexibility for tailored services to end users.

The QoE optimizer is conceived as a per-slice optimization framework in which QoE/QoS performance metrics are monitored to measure the delivered quality and determines the actions needed to be taken to re-establish desired quality levels, and enforces them through vertical-informed actuators, which, in turn, interact with the slicing functionalities to trigger the necessary actions at the underlying infrastructure level (physical and/or virtual).

USE CASE TESTBED

The use case will be prototyped, tested, and validated in laboratory environment. The testbed will be set up in two different sites, both in Aveiro, Portugal. One site hosts the 5G network management, the other the 5G network infrastructure. The Efacec IEDs and the power system simulator will be installed in the latter site.

The Smart Grid testbed represented in Figure 6 shows the Vertical, DSP and NSP actors. Each of these actors will have its own hardware and software to accomplish their roles in the Smart Grid testbed environment. In the figure the Vertical is represented in purple, the DSP and NSP1 are the same entity, represented in yellow, and the NSP2 is represented in blue.

The Vertical will have field IEDs, which will be directly connected to User Equipment (UE) registered to the 5G network, substation IEDs connected to a Local Area Network (LAN) which is also connected to the 5G network, and a substation server containing an engineering tool and Supervisory Control And Data Acquisition (SCADA) server.

Horizontal communication between IEDs will be made via R-GOOSE and/or R-SV, depending on the use case scenario. With the goal of creating a more realistic environment, during the use case testing and validation the IEDs will also be communicating with the SCADA via

IEC 61850 Manufacturing Message Specification (MMS) and will be accessible for remote engineering and diagnostic.

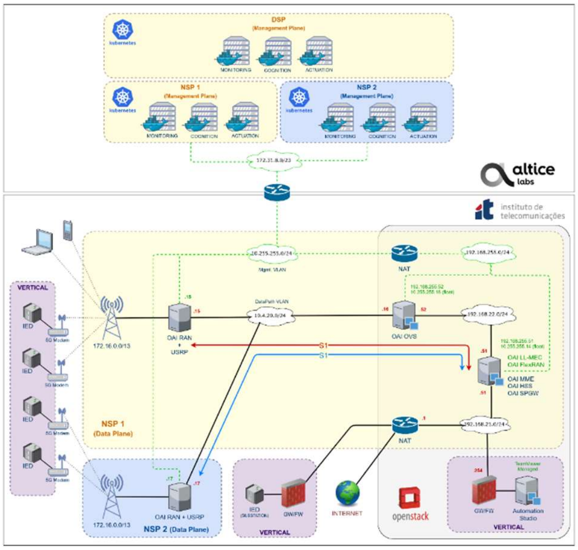


Figure 6. Use case prototyping and validating testbed.

The DSP will provide the 5G Modem and the respective Subscriber Identity Module (SIM). The DSP control plane will also ensure the E2E slice "integrity", by using a runtime QoE optimization workflow that has the ability to replace faulty/degraded Network Subnet Slices (NSSs), in order to maintain the contracted SLA with the Vertical.

The NSP will provide all the remaining resources for the creation of the network slice, these include the Universal Software Radio Peripheral (USRP) and the service that controls it, Open Air Interface Radio Access Network (OAI RAN), OAI OVS (Open Virtual Switch), OAI SPGW (Serving Packet Gate Way) and the control plane components OAI MME (Mobility Management Entity), OAI HSS (Home Subscriber Server). OAI FlexRAN and OAI LL-MEC (Low Latency-Multi-access Edge Computing).

For the DSP and NSP management plane we will use containerized software by using Docker containers and Kubernetes as the container orchestrator. This approach will be applied to the Monitoring, Cognition and Actuation sub-planes.

In order to test the network slice multi domain concept and also the replacement of a faulty/degraded NSS from one NSP with a "healthy" NSS of the other NSP we have two NSPs in our Smart Grid Testbed.

CONCLUSION

5G wide-area communication networks are expected to act as key enablers for power distribution grid applications. Having access to a secure cost-effective ultra-reliable low-latency communication infrastructure will presumably boost the development of smart grid distributed applications that would otherwise be technologically or economically impracticable.

The 5G framework and vertical-business-oriented services currently being designed and developed in the scope of the SliceNet project will provide a valuable opportunity for developing state-of-the-art communication-based smart grid applications and validating them in a realistic environment.

There is a phased iterative plan, already ongoing, for the SliceNet Smart Grid Self-Healing use case testbed deployment, vertical integration, and validation tests. Future prototyping and validation activities are anticipated to provide data that will allow the viability analysis of the DA algorithms described throughout this paper and will enable studying the impact these applications have on the communication network. This work is also expected to provide a more accurate idea of the advantages that can be obtained from 5G networks compared to the WAN radio technologies available today.

Acknowledgments

This work has received funding from the European Union's H2020 program, under grant agreement No. 761913. The authors wish to thank all SliceNet partners for their support.

REFERENCES

[1] 5G-PPP SliceNet Project, "End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks" (H2020-ICT-2016-2/761913), [Online] available at https://slicenet.eu/.

[2] 5G-PPP, "5G empowering vertical industries", Feb. 2016, [Online] available at https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf.

[3] IEC, "IEC TR 61850-90-5 Ed.1: Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118", 2012.

[4] NGMN Alliance, "Description of Network Slicing Concept", [Online] available at https://www.ngmn.org/fileadmin/user_upload/160113_Network_Slicing_v1_0.pdf