CHALLENGES AND OPPORTUNITIES OF 5G IN POWER GRIDS

Gargi BAG
ABB Corporate Research - Sweden
gargi.bag@se.abb.com

Linus THRYBOM
ABB Corporate Research - Sweden
linus.thrybom@se.abb.com

Petri HOVILA
ABB Oy - Finland
petri.hovila@fi.abb.com

ABSTRACT

This paper is based on the ongoing evolution of the power grid for supporting a much more flexible and dynamic grid with a high penetration of renewable energy sources and storages. The foreseen applications required for controlling and protecting this new grid is further mapped against the emerging 5G technology, identifying both the challenges as well as the opportunities, by assessing the power grid requirements versus the envisioned 5G technology and functionality.

INTRODUCTION

The power grid which we know today as a traditional one way power flow, where the power is generated by a few large power plants, transferred via HV transmission and finally transformed and distributed to the consumers in the end of the grid, is now fast evolving. The new power grid needs to support a bi-directional power flow due to the increasing number of both small scale as well as large scale DER (Distributed Energy Resources).

This paper uses the evolving power grid as a starting point for identifying the new control, protection and monitoring applications needed, and focus the analysis on the derived communication aspects and requirements. Especially the emerging fifth generation of mobile networks, 5G, is targeted in the analysis since it is just being defined, with the expressed vision to support vertical industry needs in e.g. the energy domain. This concurrent evolution gives a good opportunity to synchronize these two domains, providing use cases and requirements from the energy domain, into the 5G domain. In this paper the communication requirements related to power grid protection, control as well as monitoring are presented, identifying the challenges such as latency, reliability and time synchronization that needs to be addressed. The paper also discusses the opportunities which open up due to the flexibility which is provided by wireless technologies.

FROM TRADITIONAL TO SMART GRIDS

The power grid is transforming into a bi-directional power flow, whereby some of the traditional consumers are also becoming producers i.e. prosumers. The new grid has a large quantity of DER, typically renewable energy sources which often are intermittent by nature. Small-scale DER units are mainly connected to the distribution grids and larger wind / solar parks with multiple DER units to the transmission grids.

This evolving new power grid provides also the basis for a large scale deployment of microgrids, where a part of the grid, with DER, is disconnected for example in case of disturbances from the main grid and operated intentionally as an islanded grid. Fig 1, shows the power grid with addition of DER.

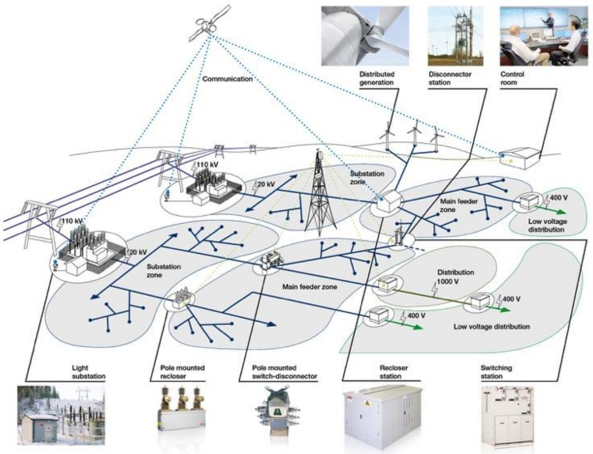

Fig 1: Grid automation

Within the distribution grid there will be need of wide area monitoring using for example Phasor Measurement Units (PMUs) and additional types of sensors, for monitoring not only the phasors but also information such as temperature, vibration etc. for the devices in the grid. Similarly, with addition of renewables in the grid, more and more control functions related to power balancing, voltage and frequency control are also required from the DER units by the grid codes or in the future by technical service markets. These DER units need to communicate decentrally or centrally to execute the control applications.

However, it is not only the infrastructure of the grid that is changing, but also its electrical characteristics (e.g. dynamics due to less inertia) is changing due to the fact that modern power electronics are used in connecting the DER units with different fault behavior and fault current feeding capability than traditional synchronous generators. Therefore, new protection methods and schemes needs to be developed for both grid-connected and islanded operation in order to detect the limited fault current. Since the current flow will be bi-directional, directional protection will be needed in many cases. Also other schemes, such as line differential protection, can be used to enhance the protection sensitivity.

The conclusion is that the transformed power grid will necessitate more control, coordination, and monitoring functionalities, thus a higher degree of grid automation including communication [1]. Due to its scalability and flexibility, as well as cost efficient deployment, wireless communication is a suitable candidate for providing the communication infrastructure for the emerging power grid. The need for wide area coverage, as well as high performance are two identified reasons [2] why cellular technologies are suitable to facilitate the communication needs for the power grid. The use of the emerging 5G, which is envisioned to support both massive machine type communication as well as ultra-reliable and low latency communication, will further make the case stronger for using wireless communication for grid automation.

Use cases and Requirements

Table 1, gives a high level overview of different application requirements in terms of latency and availability in grid automation. However it is to be noted that the figures for latency presented below is generalized and the exact requirements are application dependent.

Application	Latency	Device	Availability
Teleprotection	Low < 10ms	Breakers	Very high
Tele-interlocking	Low < 10ms	Breakers Reclosers	High
Control	Medium <~100ms	Switches Reclosers DER units	High
Video	High <~1000 ms	Remote sites	High
Monitoring and diagnostics	High <~1000 ms	Smart meters Condition monitoring devices	Medium

Table 1: Application requirements

Protection

For protection applications the limited fault current of the used power electronics converters is a challenge to detect using existing methods. Line differential protection can be considered in this case as one very potential alternative, relying on high-speed communication of measurements between two points of the distribution or transmission line to detect a fault. As shown in Fig 2, in line differential protection two relays monitors a section of the distribution line such that they sample the current following the line at certain intervals of time and send the measurements to each other for comparison. If there is no fault in the network, the two measurements must match for a time instant, if not then a fault is detected in that line segment, whereby the relay sends a trip command to the breaker.

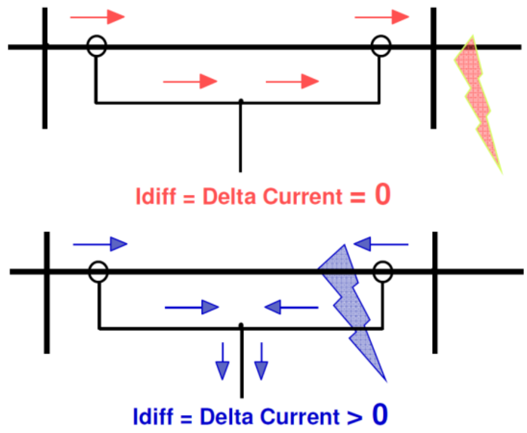

Fig 2: Line differential protection principle

In the present scenario, wired communication such as fibre optics is used between two points, which can be expensive, especially when deployed in the distribution level in large scale. Here a cost efficient wireless solution would be desirable which is also scalable and flexible.

The protection applications put the highest constraints and requirements for the communication network. These requirements are defined below in Table 2.

Requirements Category	Definition
Coverage	Urban and sub-urban areas need coverage. Nearby substations may be distributed up to 50 km apart.
Security	Message authentication and integrity, partly encryption.
Redundancy	Disjoint redundant paths between substations. Avoid single point of failure.
Latency	Application specific, <10 ms.
Reliability	99.99%
Time synchronization	< 20 us between substations.

Table 2: Protection requirements

As can be seen from Table 2, the relays will be deployed over wide areas, thereby needing wide area communication. Even if the distribution part of the power grid is mainly located in urban and sub-urban areas, there are as well cases of rural deployment of substations, however for these substations the requirements may be slightly more relaxed. It is also imperative to support redundant communication paths between substations to avoid a single point of failure, even though the level of redundancy depends on the cost, the estimated impact and the probability of a failure. Cyber security is a major concern for all power utilities, and it will be of increasingly importance as the power grid relies more and more on communication networks. Message authentication and integrity are here the main needs for protection applications to avoid improper operations due to false data. Loss of communication, denial of service as well as jamming of radio signals must also be cared for by the infrastructure, even if the protection applications always have a backup method in order to mitigate a communication loss.

The protection applications have the most stringent communication requirements. The communication latency, <10 ms for some applications, in combination with high reliability, >99.99%, meaning that at least 99.99% of the messages should arrive within its time deadline. One requirement closely related to the communication infrastructure is time synchronization. Many protection applications depends on highly synchronized clocks among the substations in order for the protection algorithm to operate efficiently. In today's protection applications based on wired communication, time synchronization is often provided by GPS clocks, and are distributed within a substation using protocols such as IEEE1588 or similar protocols assuming very low jitter. In an expanding distribution grid a different approach is needed for time synchronization of the substations and devices.

Control and Grid Automation

In the evolving power grid, with the high renewable penetrations at various voltage levels, new control requirements are essential both in transmission and distribution levels.

The larger integrations of wind or solar at transmission level impose control requirement related to power balancing, voltage control and frequency regulations. The role of renewables during normal and system contingencies (related to grid support and ancillary services) demand control actions based on different communicated measurements, controllable switch status and system events. Similarly in the distribution grid, with high penetration of renewable sources, state of the art system control, e.g. voltage profiling, requires much more information or measured values from different part of the network.

With addition of renewable sources in distribution level with variable power output, the key challenge is balancing the supply and demand of power while maintaining the acceptable voltage and frequency regulations.

The microgrid concepts relates to the operation of the distribution network with distributed generations and control of them, either in grid connected or islanded mode. In a microgrid, the distributed resources are required to share the loads depending on their available power and power rating. The power sharing ratios as well as the control strategies for grid voltage and frequency regulations can be decided by a central controller based on power consumption information of the loads in case of a small power park. However for a large microgrid, where the sources and loads are placed far apart, it is not feasible to communicate all the measured electrical values (e.g. voltage, power, frequency) of the loads and source to the central controller. In this case the central controller can provide secondary level system controls (e.g. energy management, voltage profiling) by calculating the reference quantities while the load sharing is achieved with decentralised concepts e.g. droop control.

These differences in control approaches at various level in power grid also implies different communication requirements in terms of latencies and reliability. Some control actions based on communication can be mentioned as:

1. Control actions based on a controllable switch status (e.g. breaker)
2. Control action based on measured voltage or frequency which are not local
3. Control action based on a system events e.g. trip of a distributed generator or line
4. Control action based on loss of power generation in a renewable source

The coverage and security requirements are here same as for the protection applications. Latency and reliability requirements would be more relaxed, allowing around 100 ms latency with a 99.9% reliability. Time synchronization accuracy is also less critical for control applications. Additionally communication of different signals (power, breaker status, trip or voltage) demands various communication ability. For example, secondary level control functions in a large microgrid such as energy management may tolerate a higher latency as compared to for example control action based on system events.

Monitoring and Diagnostics

Monitoring includes monitoring of grid equipment, including real-time situational awareness and supervision of capacitor bank controllers, fault detectors, reclosers, switches, and voltage regulators within substations. The use of Phasor Measurement Units (PMUs) for wide area monitoring of the voltage and current in the grid, is used to detect faults in the grid. In this scenario, the frequency of sending data in this scenario is less compared to protection and also the demand for low latency is less strict however the need of time synchronization, security and large scale coverage becomes extremely important. Other than the PMUs there could be sensors installed on different points in the grid to monitor the temperature, vibration and other physical characteristics of the devices in the grid. Metering devices, which already today are commonly deployed using wireless technologies, can also be a data source for the evolved power grid. Video surveillance of remote substations represents another type of application, with a significantly higher bandwidth need.

The latency requirements is even more relaxed for the monitoring applications, typically 500-1000 ms, and with a reliability of around 99%. Metering applications may on the other hand require data encryption and are also subject to privacy issues.

CHALLENGES AND OPPORTUNITIES

Similar to any other industrial automation control context, the main challenges for wireless communication are: safety, security, availability, latency, system integration, coexistence and interference avoidance [3]. A subset of these aspects are addressed below.

Security mechanisms to provide integrity and authenticity are of highest importance whereas encryption is applicable also in cases like metering. To in first case avoid, and secondly detect and act upon a security threat is necessary for providing a reliable power grid system. Here IEC 61850 defines a set of end to end security principles to protect the data integrity, but the communication infrastructure must in addition provide measures against e.g. jamming of radio signals and unauthorized access to the network and its devices including e.g. denial of service attacks. In practise the communication infrastructure itself must be perceived as a secure network, comparable with a point-to-point fibre or a VPN (Virtual Private Network). The support for a VPN-like service by the 5G system would here be needed, as well as the ability to detect a radio jamming attack.

The low communication latency, in combination with the high reliability required, represents the main challenge for the 5G development since latency in the form of average has been state of practise in the cellular domain. The conceptual change from “average latency” into “worst case latency” is ongoing, and is primarily addressed by the concept of network slicing [4].

The flexibility of providing multiple ways of redundancy in a cellular system is an opportunity which can be further exploited. From using dual end devices, dual operators, dual base stations, use of multicast communication to the use of different diversity schemes such as frequency and time diversity. However, again here practicality and acceptance of using 5G depends on the cost of having dual support in terms of base stations, modems and other techniques for achieving redundancy.

In a cellular system, coexistence is typically not an issue since licensed frequency bands are used. However, in 5G there may also be the possibility to use unlicensed bands, but primarily for off-loading during peak time.

An obvious opportunity for the 5G system is to provide a time synchronization source for the end devices. For the power grid domain it would be of high value if the GPS clock receivers could be replaced by a service in the communication infrastructure. Another opportunity of a 5G communication infrastructure is to provide MEC (Mobile Edge Cloud) services for some of the distributed but still time critical control applications. Direct device to device communication is another feature which likely will be useful for more local communication.

The availability of detailed data from different parts of the power grid, together with demand response status, may additionally give rise to new services and business opportunities for the stakeholders such as telecom vendors, network operators, utilities and equipment manufacturers. The consumers which sometime also will act as producers will also play an important role in this future power grid. Given below are some examples of the opportunities of using 5G in power grids, especially in microgrids.

Load Compensation in a Microgrid

A cost effective and deployable communications system is required to provide data links between the remote power generators and the centralized controller as well as between the centralized controller and the loads in a microgrid as shown in Fig 3.

In Fig 3 the two distributed energy (DG) sources provides the real and reactive power denoted by P and Q respectively. In [5] it is shown that with proper reference signals generation, it is possible to compensate for the unbalance load by the compensator and share power among the DGs. In Fig 3, the power consumptions (P_L and Q_L) of the individual loads need to be communicated to the centralized controller (CC), which calculates the averages of P_L and Q_L. Based on these averages (P_{Lav}, Q_{Lav}), and the rating of each DG, the CC determines the load sharing ratio (*R1* and *R2*) for each DG. The average power and the load sharing ratios are then sent from the CC to each DG to calculate the individual references.

When using 5G, cloud based computing functionality at the edge of the network can be suitable in implementing the CC. This will be beneficial considering the availability of scalable computing power and the low latency incurred by the short communication distance.

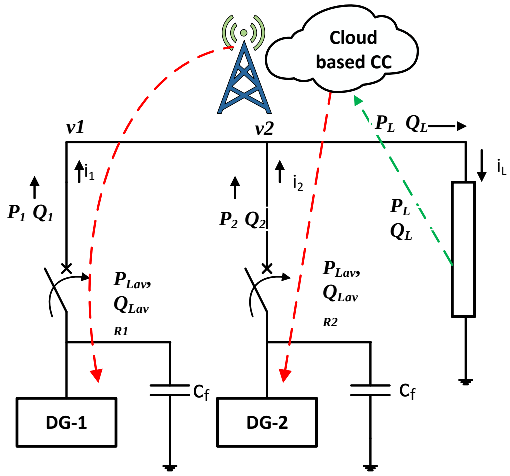

Fig 3: Microgrid

Power Management in a Large Microgrid

In a large microgrid where the distributed sources are far from each other, the low or medium voltage lines are highly resistive and challenging for droop based power sharing. The power sharing can be improved significantly in this conventional decentralized power control scenario by correcting the distributed generators reference signals. The reference signal in this case will consist of the first component, which is derived from the decentralized controller based on local measurements. The second component is derived from the power network parameter or other control constrained and is communicated [5] by other DGs and power measurement units in the lines. This function has low latency requirements, but 5G can be a suitable choice considering the need to cover large distances, providing a secure and reliable communication link.

Protection

As discussed in the previous sections, the need for protection applications increases with more DER connected to the grid. Further, an additional challenge is the detection of the limited fault current. One possible solution is here line differential protection, which has high requirements on the communication infrastructure. Other protection schemas may here also be developed, e.g. taking into account data from other nearby substations. The flexibility of 5G would here allow easy access to this data, and thus enable deployment of new protection algorithms, without the need of a new communication infrastructure.

CONCLUSION

This paper discusses how the power grid is evolving to mitigate outages and support more renewable sources of energy in the power grid. The evolving 5G standard has the potential to become a key enabler for this transformation as it will support wide area communication, low latency, cyber security, highly reliable and scalable communication. It is also foreseen that the increased level of data and its granularity will enable new services and business around the power grid domain. This paper also present examples of functions impacted by 5G, and their main functionality. However the success of 5G will depend on the cost to support features such as security, dedicated QoS, redundancy, and also the regulations.

REFERENCES

[1] A. Timbus, M. Larsson and C. Yuen, "Active Management of Distributed Energy Resources Using Standardized Communications and Modern Information Technologies," in IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4029-4037, Oct. 2009.

[2] C. Kalalas, L. Thrybom and J. Alonso-Zarate, "Cellular Communications for Smart Grid Neighborhood Area Networks: A Survey," in IEEE Access, vol. 4, no. , pp. 1469-1493, 2016.

[3] J. Åkerberg, M. Gidlund and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," 2011 9th IEEE International Conference on Industrial Informatics, Caparica, Lisbon, 2011, pp. 410-415.

[4] P. Rost et al., "Mobile network architecture evolution toward 5G," in IEEE Communications Magazine, vol. 54, no. 5, pp. 84-91, May 2016.

[5] R.Majumder, G.Bag, K.Kim, "Power Sharing and Control in Distributed Generation with Wireless Sensor Networks" IEEE Trans. Smart Grid2012.