24th International Conference & Exhibition on Electricity Distribution (CIRED)

12-15 June 2017

Session 3: Operation, control and protection

Improving actionable observability of large distribution networks for transmission operators to support improved system control, fault detection and mitigation

ISSN 2515-0855
doi: 10.1049/oap-cired.2017.1199
www.ietdl.org

Corinne Shand[1] ✉, *Gareth Taylor*[1], *Emma Stewart*[2], *Ciaran Roberts*[2], *Alan Mcmorran*[3], *Priyanka Mohapatra*[4]

[1]*Brunel University London, Electronic and Computer Engineering, London, UK*
[2]*Lawrence Berkeley National Laboratory, Grid Integration Group, Berkeley, CA, USA*
[3]*Open Grid Systems Ltd., Glasgow, UK*
[4]*SP Energy Networks, Glasgow, UK*
✉ *E-mail: corinne.shand@brunel.ac.uk*

Abstract: The widespread introduction of phasor measurement unit (PMUs) in transmission networks is well understood and has improved visibility enhancing grid stability and avoiding low probability events such as blackouts. For many transmission system operators, there is little-to-no visibility of the real-time state of distribution networks beyond the grid supply points. With the increased penetration of distributed energy resources on low- and medium-voltage networks of the state, and thus behaviour, of the distribution network cannot be assumed to follow historical patterns. The future transition to distribution system operator concept requires better visibility, especially around grid supply points, for deploying wide-area control strategies and active network management schemes. This implies active sharing of data between transmission and distribution monitoring systems. There are a number of challenges in extending the use of PMUs to distribution networks. Many of the lessons and best practises at transmission do not translate to the operation of distribution networks, as an exponential increase in network complexity makes it infeasible to perform complex analysis of the complete network model in real time. This paper presents a methodology for addressing the problems faced in deploying microPMUs at the distribution level.

1 Introduction

Power systems in Great Britain (GB) and worldwide are facing the challenges associated with the transition to a low carbon/high reliability future including:

- Fast changes in generation mix.
- Slowly evolving network components.
- Relatively high cost of upgrades per capita.
- Environmental impact of adding equipment.
- The increase in frequency/impact of severe weather events [1].

Enhanced monitoring is required both at transmission and distribution voltage levels to manage the impact of emerging system dynamics, provide essential network services and safely direct power from lower-voltage levels through the interconnected transmission network to areas of demand.

An increasingly complex distribution network in GB will require higher levels of monitoring beyond the current substation boundaries. Additional load points and meshed networks being added to an ageing distribution grid will require more complex monitoring. Data will need to be collected at key network locations and at a higher frequency and granularity, both in relation to real-time system operations and longer-term network planning.

Current practises of real-time monitoring must expand beyond the substation to strategic locations, service providers and distributed energy resource (DER) installations. The ability to control the network, take actions and react to wider system events through the use of enhanced monitoring solutions will aid the ability to detect issues directly impacting network performance, system stability and ensure GB distribution network operator (DNOs) maintain a safe and reliable network. New sensors, communication equipment and information technologies promise to improve efficiency, reliability and power quality of the distribution system, improve the quality of service and enabling increased DER penetration and improved customer choice.

The University of Texas at Austin has previously created an independent synchrophasor network [2]. This is a network that uses PMU measurements at the distribution level from sites across the state of Texas. The aim of their research was to validate the quality of the PMU measurements and to show that they are acceptable for power system analysis, by comparing them to measurements taken at the transmission level. Using three weeks of measurements, the data from both voltage levels are closely matched.

Where communications infrastructure is restricted, operators do not necessarily need 100–200 samples/s but they do need the outcome of analysis in order to respond to network events. Investment into distribution management centres and widespread sensing would provide operational visibility; however, the data communication and analytics infrastructure investment is limited, with little-to-no visibility for the transmission system operator of faults and outages beyond the grid supply point. This paper is considering microPMUs (μPMUs) as part of a bigger data framework along with communications and analytics frameworks. The information that is visible would need to be prioritised for both communications and the system operators. Each operational area would potentially require the data to be filtered and translated into something they will understand – some operators would not want to see a phase angle measurement but rather the action that should be taken when the phase angle deviates.

This paper will look at the main challenges faced by transmission operators when observing large distribution networks and the challenges for installing µPMUs in resource constrained areas. This paper presents a methodology for addressing problems faced in deploying µPMUs on the distribution network by leveraging trusted cloud computing platforms and encrypted communications over public telecommunications networks to provide an adaptable, secure platform for devices to automatically authenticate, coordinate and store data.

Section 2 will discuss the current use of wide area monitoring schemes (WAMSs) at the transmission level, with an insight into why it is needed at the distribution level. Communication technologies and secure communications are considered in Sections 3 and 4. Section 5 covers trusted cloud platforms and Section 6 looks at the encryption and synchronisation of µPMUs.

2 Transmission WAMS

WAMS incorporate wide-area synchronised phasor measurements, produced at a rate of 50 fps, which provide unparalleled monitoring and understanding of the dynamic behaviour of large electrical systems, when compared with unsynchronised supervisory control and data acquisition (SCADA) data that is sampled at 1 fps. On the GB network, visualisation of real time system dynamics using enhanced monitoring (VISOR) [3, 4] is a network innovation competition project to show how this radical change in power system monitoring can be exploited to reduce both operational and capital expenditure through maximising asset utilisation, and to increase resilience against high impact, low probability events that can cause network disruption, plant damage or even blackouts.

This goal is being realised through the novel use of emerging monitoring, analysis and visualisation techniques to better understand the true capability of the power system and to determine in real time how close the system is being operated to this maximum capability. Through this improved understanding, WAMS can provide operators/planners with greater confidence to fully exploit this capability when facing new challenges. Using real-time measurements to identify threats in advance can enhance network security. Whilst WAMS can offer a wide variety of benefits to power system operators and planners, VISOR is focusing on the following key areas that are expected to be of the most benefit to the GB system in the short-to-medium term:

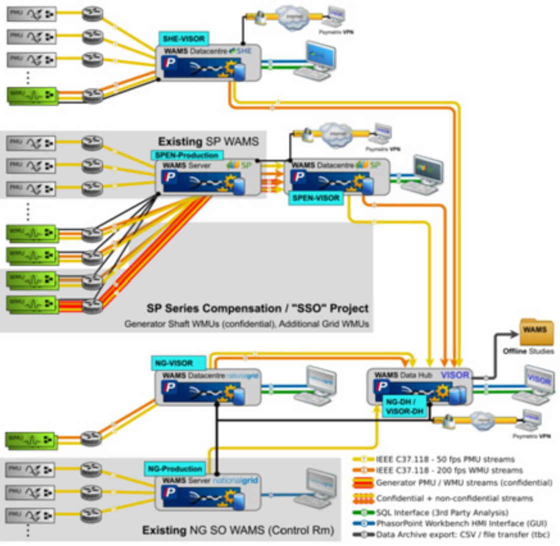
- Real-time monitoring and alarming of sub-synchronous oscillations (SSOs) in the range 0.002–46 Hz.
- Dynamic model validation using post-mortem analysis of WAMS data.
- Hybrid state estimation.
- The potential use of angle-based security limits to increase power flow on the B6 boundary between Scotland and England [3].

2.1 Current GB WAMS

The GB power system is currently using wide-area monitoring to improve transfer capabilities and monitor interactions and resulting oscillations.

Existing GB transmission WAMS brings together wide-area monitoring data from the three GB transmission owners: scottish power (SP) energy networks, national grid and Scottish hydro electric; and the GB system operator. The first integrated GB WAMS focuses on three key areas, each incorporating the planning, real-time and event/trend analysis domains:

- *Management of system risks and events*: Early warning, response and analysis.
- *Reducing uncertainty*: Improved situational awareness, confidence in system models and limits.
- *Maximising assets*: Efficient and effective use of WAMS and transmission infrastructure



PMU
WMU
SHE-VISOR
WAMS Datacentre SHE
Paymetrix VPN
Existing SP WAMS
SPEN-Production
WAMS Server SP
WAMS Datacentre SP
SPEN-VISOR
SP Series Compensation / "SSO" Project
Generator Shaft WMUs (confidential), Additional Grid WMUs
WAMS
Offline Studies
NG-VISOR
WAMS Datacentre nationalgrid
WAMS Data Hub VISOR
NG-DH / VISOR-DH
NG-Production
WAMS Server nationalgrid
Existing NG SO WAMS (Control Rm)
IEEE C37.118 - 50 fps PMU streams
IEEE C37.118 - 200 fps WMU streams
Generator PMU / WMU streams (confidential)
Confidential + non-confidential streams
SQL Interface (3rd Party Analysis)
PhasorPoint Workbench HMI Interface (GUI)
Data Archive export: CSV / file transfer (tbc)

Fig. 1 *Critical infrastructure of the GB transmission WAMS*

The critical infrastructure of the GB transmission WAMS includes three regional WAMS ‘Datacentres’, a central WAMS ‘Data Hub’ server and the deployment of PMUs and waveform measurement units (WMUs) across the GB transmission network as shown in Fig. 1 below.

The datacentres and data hub provide data aggregation as phasor data concentrators, in addition to providing storage, analysis and visualisation of WAMS data over their respective areas of coverage.

WMUs are similar to PMUs in that they also provide synchronised measurements of voltages and currents and utilise the same IEEE C37.118-2 [5] communications mechanism. Unlike PMUs however, WMUs report point-on-wave measurements of the voltage or current waveform at a 200 Hz sampling and reporting rate. This provides extended visibility from the present PMU capability of around 10 Hz, up to 46 Hz to fully cover SSO behaviour involving series capacitors, generator torsional behaviour and power electronic systems.

2.2 Extending WAMS to distribution

The changing network and increased DER mentioned in Section 1 is creating unprecedented challenges for network owners and system operators.

In an ideal scenario-enhanced modelling capabilities will include wide-area monitoring at all voltage levels, and digital computing should be able to safely enable system services, transfer power and enable the operator to utilise the existing system safely to its maximum capacity. However, there are a number of challenges in deploying PMUs on the distribution network [6] secure and reliable communication is not present in all parts of the network and is especially poor in distribution network; low-latency, high-bandwidth communications cannot be assumed. The challenges for network owners lie in improving the existing communications infrastructure to enable data flows, merging of information technology (IT) systems, and ensuring cyber security. It is key that the right information is provided to the right people at the right time irrespective of whether they are the distribution or transmission system operator.

Economy is important for the distribution grid. If smart meters were used for WAMS, thousands would be required to report limited information, while one or two µPMUs on the same network could report more useful highly accurate, high fidelity information.

Assuming 1000 customers reporting single-phase phasor data at a frequency of 1 Hz, this would produce 2.2 GB of data each day (four phasors, frequency, rate of change of frequency, timestamp and status with 32 bit floating point precision, 64 bit time stamps and

2 B status), whereas two μPMUs collecting three-phase data at 50 Hz would produce 285 MB of data each day (assuming 12 phasors and the same precision). The μPMUs would be collecting less data by volume but with higher fidelity data.

3 Communication technologies

Transmission system operators are in a position to install and manage their own dedicated, secure, high-bandwidth, low-latency communications network connecting their primary substations to the control room. When installing a PMU in a transmission substation, this existing communications network is generally used.

When installing PMUs on the distribution network, however, it is less common to find a dedicated communications network installed across the DNO's service territory. Instead any communications links are over public networks such as cellular network services, fixed-line telephone/broadband connections or wide-area radio networks. The performance of such networks can vary widely depending on the location of the substation and local availability of communication services.

The installation of PMUs across a distribution network must therefore deal with a number of issues when using these communication links:

- Reduced and/or unpredictable bandwidth and latency.
- Restrictions in cumulative transmission of data (e.g. monthly usage caps on the amount of data that can be sent/received).
- Use of an insecure public communications network.
- Lack of control when a network goes down (e.g. it is harder to control the reliability of something that is owned by someone else).

The advantages and disadvantages of different communications technologies have been analysed previously [7]. The performance of modern cellular networks, especially in areas covered by the latest fourth generation technology, can provide sufficient bandwidth for PMU communications; however, the cost of a contract to provide sufficient capacity to transmit all data collected by a PMU can be prohibitive and the latency, bandwidth and being a public network, the availability of the communications link can be impacted by other users.

4 Secure communications

4.1 Direct access via virtual private networks

Virtual private networks (VPNs) [8] are widely used in multiple industries and have been used previously within the power industry in conjunction with cellular communication networks [9] to enable secure access over public networks. Transport layer security [10] cryptographic protocols allow for secure, encrypted communications over networks. Standard data communications protocols such as hypertext transfer protocol secure [11] are built on transport layer security (TLS) and are widely used for web browsing as well as machine-to-machine communications. Previous work [12] has looked at the security of the smart grid and how public key infrastructures can be used on top of existing mechanisms such as TLS to enable secure communications.

For PMUs deployed at distribution using public communication networks, the architecture for receiving commands/data and providing the data collected can vary depending on security requirements and the parties requiring access to the data. A VPN can be configured to allow the PMU to communicate with systems within the DNO's own internal network directly. Any further sharing of the data with other parties such as the transmission system operator (TSO) would then require additional links between the DNO and TSO to be established.

The advantage to this approach is that the systems requiring the data can communicate directly with the devices in the same manner as those deployed at transmission. There are some potential issues with this approach. The devices in the field are unattended and connected to a public communications network with a trusted VPN connection. This has already been identified as an avenue of attack [11] for third parties to gain access to an internal network. There is a risk that a misconfigured VPN connection or unknown vulnerability would provide an avenue into the DNO's internal network, either physically via the device or from unauthorised access via the public communications network. This also requires the DNO to set up data sharing with the TSO via another mechanism, adding complexity and latency.

4.2 Distributed access using cloud computing

A second approach is for the PMU to communicate with a cloud system that then stores the data and shares it with authorised parties [13]. A cloud architecture would have both the PMU and the cloud server connecting to the public network, then users within the DNO and TSO would pull data from this cloud server directly. The cloud server would be installed within a data centre with an 'always-on' connection but for devices with low bandwidth communication links, they would connect and push data only when required.

This offers advantages in that the users within a secure TSO and DNO network are only 'pulling' from the cloud server, it does not need a VPN or 'push' connection into the secure TSO/DNO network. Where the cloud server to be compromised, then the attackers would have access to the data but not into the secure networks. The PMU devices in the field can similarly only connect to the cloud server and do not have any connection into the TSO/DNO network.

The disadvantage is that the system would be storing potentially sensitive real-time sensor data on a server connected directly to a public network. If properly configured [8], these risks can be mitigated but recent cyber attacks [14] have shown that it is difficult to robustly secure systems. The priority should be to mitigate the risks to the secure, internal networks if a remote device is compromised.

5 Trusted cloud

Cloud computing allows relatively cheap access to huge amounts of processing power, without investing in dedicated computing facilities, which is ideal for the analysis of lots of data. If required, resources can be scaled up to deal with a large influx of data, and then reduced if the input returns to normal levels [15].

Trusted clouds are a development of private clouds. They allow only specified people or organisations to use the cloud and to verify that the image used to instantiate the virtual machines has not been modified since its creation. This provides an additional layer of trust and security for the data and applications deployed in the cloud, providing a more reliable and secure platform. As with all cloud platforms, different levels of accesses can also be created, so an administrator can access the underlying infrastructure of the cloud, while end users can only view the data or results stored [16].

It allows measuring of the collective integrity of the hardware platform, firmware and operating system components responsible for booting. Integrating trusted cloud implementations would allow cloud administrators/system operator (SOs) to measure and verify infrastructure integrity; however, the end-user integrity measurement/testing of the underlying infrastructure will require some additional mechanism such as a secure channel for end users to access the cloud platform [12, 17].

A challenge is the additional software that will be required to enable the connecting PMUs to automatically authenticate, integrate and communicate with a trusted cloud platform. The cloud-based platform must meet the specific utility's requirements for security, and verify that the connecting PMU is trustworthy when it is connected to the network. The PMU must also verify that it is communicating with a known, trusted platform [15].

A cloud-based system will allow multiple μPMUs to automatically connect, authenticate, integrate and send their data to the back-end system. A trusted cloud [16] platform can help to ensure the connection and data is secure. In such an environment, the integrity of the entire GB power system would depend on the ability of DNOs/TSOs to update and maintain only sections of data related to their equipment/network.

6 UPMU synchronisation/triggers

By using encrypted communications over public communication networks μPMUs can be quickly connected, with the platform managing the device coordination. Where devices are operating in low bandwidth environments, it is not feasible to provide full 50–200 Hz data, instead they would reduce the synchronisation frequency of data to regular intervals unless triggered by configurable metrics.

These localised triggers can be set based on the device's position on the network with pre-defined metrics. For example, WAMS at transmission may automatically trigger alarms when pre-defined condition such as a rate of change of frequency is exceeded. Similarly, a change in magnitude or angle may go above or below a defined maximum/minimum.

These events are then sent to the cloud platform, allowing it to request all other devices to force a synchronisation of their data to allow a centralised analysis of the data. A notification to any subscribers (e.g. the distribution and transmission system operators) about the change in network conditions would also occur.

With automated synchronisation, messaging and integration with the underlying network topology, more intelligent local analytics can be used to create dynamic triggers that require the device to use its knowledge of the local topology to determine whether an event has occurred that requires notifications. These triggers can be automatically updated by the cloud server based on its view of the local, regional and overall network conditions.

7 Conclusion and future research

The addition of DER on low- and medium-voltage networks, combined with lack of visibility of the real-time state of distribution networks, makes it difficult for transmission system operators to have visibility of the network beyond the grid supply points. A solution to this is to install μPMUs at the distribution level to provide increased visibility within WAMS. This paper has looked at the challenges involved in this including the challenges involved in secure communications and utilising a trusted cloud platform as a means of allowing devices to automatically authenticate, coordinate, store and share data.

Event triggering is a viable option to reduce the synchronisation frequency of data to regular intervals unless triggered by configurable metrics.

Future work in this area will involve further testing of trigger-based synchronisation such as what an acceptable trigger is and how effectively a network of devices can be synchronised, as well as the integration of μPMUs within transmission WAMS in a functioning network.

8 References

1 USGCRP: 'Climate change impacts in the United States', in Melillo, J.M., Richmond, T.C., Yohe, G.W. (EDs.): 'The third national climate assessment' (U.S. Global Change Research Program, 2014), p. 841

2 Allen, A.J., Sohn, S.W., Grady, W.M., *et al.*: 'Validation of distribution level measurements for power system monitoring and low frequency oscillation analysis'. 2012 IEEE Power Electronics and Machines in Wind Applications, Denver, CO, 2012, pp. 1–5

3 VISOR project: opportunities for enhanced real time monitoring and visualisation of system dynamics in GB

4 SPEN-DSO vision. Available at http://www.spenergynetworks.co.uk/userfiles/file/SPEN%20DSO%20Vision%20210116.pdf, accessed on 08 January 2017

5 IEEE Standard for Synchrophasor Measurements for Power Systems: '*IEEE Std. C37.118.1-2011*' (revision of IEEE Std. C37.118-2005), December 28 2011, pp. 1–61

6 Stewart, E.M., Kiliccote, S., Shand, C.M., *et al.*: 'Addressing the challenges for integrating micro-synchrophasor data with operational system applications', 2014 IEEE PES General Meeting|Conf. Exposition, National Harbor, MD, 2014, pp. 1–5

7 Gungor, V.C., Sahin, D., Kocak, T., *et al.*: 'Smart grid technologies: communication technologies and standards', *IEEE Trans. Ind. Inf.*, 2011, **7**, (4), pp. 529–539

8 Venkateswaran, R.: 'Virtual private networks', *IEEE Potentials*, 2001, **20**, (1), pp. 11–15

9 Zhou, H.J., Guo, C.X., Qin, J.: 'Efficient application of GPRS and CDMA networks in SCADA system'. Power and Energy Society General Meeting 2010 IEEE, 2010, pp. 1–6, ISSN 1944-9925

10 IETF Network Working Group: 'The transport layer security (TLS) protocol version 1.2', August 2008. Available at https://tools.ietf.org/html/rfc5246, accessed on 12 January 2017

11 IETF Network Working Group: 'HTTP over TLS', May 2000. Available at https://tools.ietf.org/html/rfc2818, accessed on 12 January 2017

12 Metke, A.R., Ekl, R.L.: 'Security technology for smart grid networks', *IEEE Trans. Smart Grid*, 2010, **1**, (1), pp. 99–107

13 Andersen, M.P., Culler, D.E.: 'BTrDB: optimizing storage system design for time series processing' (University of California, Berkeley)

14 Lee, R.M., Assante, M.J., Conway, T.: 'Analysis of the cyber attack on the Ukrainian power grid', E-ISAC, 18 March 2016. Available at https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf, accessed on 12 January 2017

15 Shand, C., McMorran, A., Taylor, G.: 'Integration and adoption of open data standards for online and offline power system analysis'. 2014 49th Int. Universities Power Engineering Conf. (UPEC), Cluj-Napoca, 2014, pp. 1–6

16 Wallom, D., Turilli, M., Taylor, G., *et al.*: 'myTrustedCloud: trusted cloud infrastructure for security-critical computation and data management'. 2011 IEEE Third Int. Conf. Cloud Computing Technology and Science, Athens, 2011, pp. 247–254

17 Sule, M.-J., Li, M., Taylor, G.: 'Trust modeling in cloud computing'. 2016 IEEE Symp. Service-Oriented System Engineering (SOSE), 2016, pp. 60–65