COMMUNICATION REQUIREMENTS FOR FUTURE SECONDARY SUBSTATIONS TO ENABLE DSO FUNCTIONS

Kinan Ghanem[1], Ibrahim Abdulhadi [1], Ali Kazerooni[2], Chris McGookin [2]

[1]Power Networks Demonstration Centre, Glasgow, UK
[2] SP Energy Networks, Glasgow, UK
kinan.ghanem@strath.ac.uk

Keywords: LV DISTRIBUTION, DSO FUNCTIONS, SECURITY, COMMUNICATION REQUIREMENTS.

Abstract

Reliable and scalable communication technologies are required to securely integrate and utilise the flexibility offered by different smart grid solutions. Smart secondary substations can play a critical role in enabling the flexibility services for the DSO with more monitoring and control functions being deployed at these substations. However, there are a number of challenges associated with the deployment and integration of communications to enable future DSO functions. This paper defines the key requirements for future secondary substation communications and provides a number of recommendations to address future operator needs. A case study related to the deployment of a Smart Transformer for better utilisation of network assets and voltage regulation is presented to illustrate the applicability of aforementioned requirements.

1 Introduction

Smart secondary substations can significantly enhance the controllability and flexibility that may be required for day to day network operation. This may be required to facilitate the growing connection of low carbon network technologies (LCT) and distributed energy resources (DER). Secure and scalable communication between these secondary substations and the Distribution System Operator (DSO) enterprise and operational communication networks is key to enabling the delivery of reliable flexibility functions. However, there are number of challenges that need to be addressed such as the reliability, security, availability and cost effectiveness of communication between the DSO control centre and secondary substation field devices.

Various communication technologies (wireless and wired) such as Power Line Communication (PLC), fibre optic communication, ADSL, Narrowband Internet of Things (NB-IoT), mesh networks, microwave networks and mobile technologies (GSM, 3G, 4G/LTE) have been trialled and deployed by DSOs to enable different flexibility functions [1]. UHF telemetry is widely deployed by DSOs worldwide as a means for SCADA communication to control and monitor reclosers and switches. Recently, some DSOs have deployed BGAN satellite technology to remotely control and monitor these distributed assets [2]. All aforementioned technologies have some limitations. Some are not cost effective, whereas others are not scalable and such cannot support the connectivity of an increasing number of controllable assets to realise new critical applications (e.g. smart electric vehicle charging, energy storage and microgeneration control, and demand response). Security of a communication system fulfilling the confidentiality, integrity and availability requirements are becoming more important. The security overhead needed to support the authentication and encryption for the connected devices must be considered in the communication network design. This is an important requirement as Internet Protocol (IP) based communication will underpin the future DSO connectivity in most adopted communication technologies.

Currently, most DSOs globally use a mix of communication technologies to connect the field devices to the control centre depending on application, availability and performance requirements. Utilising wireless technologies is reliant on spectrum and its availability, which in turn dictate the bandwidth and latency that that is available for use by DS applications. With sufficient spectrum using a suitable band, communication coverage in rural areas and the communication capacity required for urban areas can be satisfied. DSOs require a low band spectrum below 1 GHz to enhance the coverage in rural areas and achieve better signal reach for their remote sites. However, the available bandwidth below 1 GHz is very limited and only few narrow frequency band solutions are available. Meeting the coverage and capacity requirements are crucial for future wireless technologies that meet the needs for future DSO flexibility functions. This paper presents the main outcomes of a number of projects that developed bandwidth, latency, security and architecture requirements for communication with UK secondary substations (11kV/0.4kV) for various monitoring and control applications deployed to enhance the distribution network operation flexibility. This paper, firstly focuses on the development of the DSO use case driven communication data flows, which provides the baseline for determining required bandwidth and latencies for data

exchange. Secondly, the mapping between these data flows and feasible communication technologies is presented for different control functionalities at secondary substations. Thirdly, suitable strategies for secure communications in accordance with IEC 62351 and the UK Energy Network Association's "energy delivery systems – cyber security procurement guidance" are outlined, while considering available bandwidth constraints. Finally, a number of recommendations will be drawn in relation to required RF spectrum, feasible communication technologies, interoperability with legacy systems and end-to-end communication testing requirements.

2 Communication challenges and requirements for DSO functions

DSO functions require real-time, reliable and secure two-way communications networks that maintain required performance and reliability as dictated by the DSO functions and the criticality of the connected substations and flexibility assets [3]. To determine which communication technologies are appropriate for enabling DSO functions, the basic requirements of communication infrastructures in terms of bandwidth, latency and security should be met. Additionally, the reliability of a chosen communication technology for secondary substations providing DSO services should minimise the rate of outages and ensure high performance data exchange for existing and future operational requirements [4]. Additional performance metrics that need to be considered in the network design and technology selection are availability, accessibility, Quality of Service, maintainability and resilience [5]. Furthermore, a communication technology that is fit for purpose is also highly dependent on affordability, which should be considered for large-scale field deployments and how cost-effective their integration with existing systems (e.g. enterprise network) is along with the lifetime cost of operating the communications solution.

Moreover, power backup should be considered based on the availability requirements of a communication technology. The Energy Networks Association (ENA) Engineering Recommendation ER G91, issue 1, 2012 specifies that substation batteries should have enough capacity to meet the standing demand for at least 72 hours for those substations that would require to deliver black start services [6]. In secondary substation applications, 24 hours of backup power could maintain the operation during unexpected loss of power scenarios.

Considering the above communication requirements, several implementation and integration challenges exist. Most wireless technologies used to connect secondary substations face the following challenges and limitations:

- Integration with legacy communication equipment, some existing hardware have limited capabilities in supporting new communication protocols and security features.
- Interoperability between secondary substation communication and different vendor monitoring and control equipment, for example an LV monitoring system may not employ standard communications.
- Secure remote access to secondary substation functions by the DSO and third party service providers. A particular challenge is the overhead needed for secure communications using bandwidth constrained legacy communications.
- Limitations with licenced radio frequency (RF) spectrum available to DSOs for secure exchange of data with secondary substations, particularly when considering data-rich applications such as power quality monitoring and asset condition diagnostics.
- Reach and penetration of communication technologies for hard to reach areas such as underground LV link boxes.

Current arrangements for secondary substation automation varies between the DSOs, and the bandwidth requirements (for several DSOs) are in the range 3 – 5 kbps per site to remotely control and monitor their MV switching units and automation nodes. Some of the communication channels which may be still used in the secondary substations (i.e. UHF telemetry) are narrowband and limited in bandwidth which cannot be deployed for applying some security measures. Furthermore, extra communication bandwidth is required for voice services to support the DSO during black start scenarios in case DSO private communications should be used where mobile network operators lose power during a blackout. Moreover, new connected distributed assets such as charging points, LV monitoring and control functions and integration of DER may demand more bandwidth, particularly if they rely on communication with or via the substation.

3 Data Flow and Methodology for Bandwidth Calculations

In order to determine the bandwidth requirements for the secondary substations of the future, the DSO use cases considering the number of communicating nodes, measurement and control points and connected field devices in each secondary substation should be specified. Subsequently, the data flow between the communicating entities can be defined. This is practically the distribution management system (DMS) polling the RTU measurements and the protocol used to communicate between the RTU and DMS. It is assumed that future deployment of RTU connectivity will comply with IEC 62351, which is the data and communication security standard for power systems management and associated information exchange, including IEC 61850, DNP3 or IEC 60870-5-104 [7].

3.1 LV Engine smart control system use case architecture

The LV Engine project is a national innovation project led by SP Energy Networks and funded by the UK regulator Ofgem to design and trial a power electronics based Smart Transformer (ST) that performs a number of flexibility

functions including: power flow control and transformer load sharing; LV feeder voltage regulation, MV reactive power compensation and provision for DC loading. The smart functions of the ST are controlled and coordinated through a Smart Control System (SCS), which communicates with the ST, DMS and controllable LV linkbox switches (C_LVS).It also has access to LV and MV metering data. The SCS architecture design for LV Engine is based on integrated communications between a regional smart controller (RSC) and local smart controllers (LSC). This architecture (shown in Fig 1) is specified by SP Energy Networks [8]. The LSC communicates with the ST, C_LVS and RSC via the master gateway (RSC and the master gateway reside within the SP Energy Networks operational management zone). The RSC also has access to smart metering data, integrates with the DMS and LCSs deployed in secondary substations.

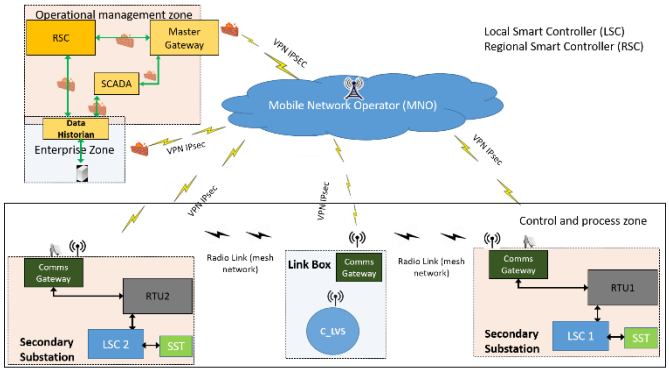

Fig. 1 LV Engine SCS high Level communication architecture

The C_LVS requires a communication gateway to enable data exchange with the LSC in the secondary substation. The gateway should have at least an Ethernet and radio interface for RTU and wireless network integration respectively. The communication and data integration between the components of the SCS and selection of suitable communications technologies requires further consideration of bandwidth and cyber security. The required bandwidth is to exchange messages between field device and control centre whereas, cyber security is to ensure the encryption for the data and establish secure connection by authentication. The secondary substation gateway will collect data and measurements from the C_LVS and LSC and communicates to the master gateway, which in turn forwards the messages to be processed, analysed or archived centrally.

As shown in Fig 1, the secondary substation gateway communicates to the master gateway via public mobile radio technology such as 4G/3G/GPRS access point that supports the DNP3/IEC104 protocols or via a private wireless technology deployed by the DSO such as private LTE. The gateway should be configured to send/receive data to/from three locations (master gateway and the LSC and NOP). The C_LVS gateway should be equipped with a radio and an Ethernet interface. The transmitted data from the C_LVS in the link box to the LSC via third party networks such as public 3G/4G technology should be sent via an Encapsulating Security Payload (ESP) within the IPSec protocol suite, which provides authentication, integrity, and confidentially of network packets data/payload.

3.2 LV Engine SCS data flows

The first step to determining the bandwidth requirements for the LV Engine SCS, is to identify the data flows between communicating components as identified in the section 3.1. Namely the Normally Open Point (NOP), Local Smart Controller (LSC) and Regional Smart Controller (RSC). These data flows and subsequent bandwidth calculations are needed for any future deployments of communications between the DSO control centre and secondary substations. The bandwidth calculations assume the use of DNP3 or IEC 60870-5-104 (IEC104) protocols as specified by SP Energy Networks which is based on their outlook for using these protocols for new communications hardware. The results showed in this paper are based on the following assumptions:

- The message size for each protocol and the estimated polling rates are based on empirical experience from previous and ongoing projects at the PNDC that tested off the shelf communication equipment (e.g. RTU).
- The security overhead is based on 2 levels of security for IEC104 (i.e. IPsec and TLS) whereas for DNP3 calculations are based only on IPsec level of security which follows industry practice.
- The maximum latency requirement of the LV Engine (according to the ST technical specification) is 10s for DC, HV, LV AC voltage set point and LV active and reactive power set points.

4 Bandwidth requirements

The calculated bandwidth for the LV Engine based on un-batching polling messages (for IEC 104) and no class reporting (for DNP3) are shown in Table 1 and Table 2. Monthly data usage is also provided. It is assumed that an RSC is connected to 18 LSCs when the RSC is located in the primary substation (in line with typical maximum connectivity possible via UHF/VHF radio communications currently used for secondary substations as advised by SP Energy Networks). It is possible that the RSC is located in the primary substation – at which point a risk-based decision will need to be made with regards to how many LSCs the RSC should communicate with taking into account the impact of RSC loss on the performance of LSCs and subsequent impact on the performance on the LV Engine SCS and control objectives.

The bandwidth calculations included the overhead of security requirements applicable to DSOs, which aim to provide an adequate mutual authentication and encryption layer above the TCP/IP layer and over the transport security layer (TLS) protocol. Based on the IEC 62351 security standard, DNP3 and IEC 60870-05-104 should be secured with two levels of security. Security through authentication and encryption are required and the DSO should comply with these requirements. In the bandwidth calculations, two levels of security have been

applied to the connection and the transmitted data. The first level is through the device itself and the second level of security is from the IPsec through a VPN between the routers. The number of analogue data points communicated by the C_LVS and LSC are 12 and 87 analogues respectively based on the data flow analysis. Whereas, the number of digitals are 2 and 23 digitals respectively. The polling time is considered as 90 seconds, which is typical for the DSO.

Table 1 Calculated bandwidth for secure IEC104 (un-batching)

Secure IEC104	Required data rate (bps)	monthly data with IPsec (Mbyte)
C_LVS	588	190
LSC	3979	1290
RSC	71620	23205

Table 2 Calculated bandwidth for DNP3 protocol (un-batching)

DNP3 with IP security	Required data rate (bps)	monthly data with IPsec (Mbyte)
C_LVS	563	183
LSC	3379	1095
RSC	60806	19701

Results analysis show that the overhead caused by the IPsec will vary based on the message size. Smaller message sizes will result in a higher overhead in terms of bandwidth needs. Bandwidth characterisation of RTU traffic carried out at the PNDC indicates that the message size is a significant factor influencing the security overhead as a percentage of the packet caused by the IPsec through a VPN. The security requirement for LV Engine with un-batch reporting may cost (22 - 28%) of the total required bandwidth. Remote access for reconfiguration and maintenance can be bursty and bandwidth consuming, as two levels of security for authentication and encryption could increase the current bandwidth requirements by 2 to 3 folds. The configuration of each protocol (DNP3 and IEC104) will determine the exchanged messages size and their required polling, which in turn affects the bandwidth. DNP3 and IEC 104 can support batch reporting which enables the DNP3/IEC104 packets to contain several measurement points in the same message, and as result decrease the required bandwidth.

5 Conclusion

Sufficient spectrum in a suitable band (below 1 GHz) is required to enable a secure wireless communication technology between the secondary substation and the DSO enterprise network. Enhanced security is needed to enable new functionality in a connected secondary substation and fulfil the requirements of the future DSOs. The security overhead represents an average of 2-3 fold increase in bandwidth if both IPsec and TLS are deployed to secure the connected asset. The configuration of DNP3/IEC-104, frequency of analogue/digital polling and the level of implemented security for authentication and encryption are the main factors that affect the bandwidth. It is recommended for the purposes of saving bandwidth to use batching polling messages (for IEC 104) and class reporting (for DNP3). Medium and long-term RTU connectivity should meet LV monitoring requirements (i.e. suitable interfaces and standard communication standards). The communication technology for LV substation monitoring should not be considered as a standalone service. DSOs should consider, in detail, the appropriate communication technology that can meet the requirements of the LV monitoring in addition to secondary substation functions such as monitoring and MV control. A private network operated by the DSOs is thought to offer the best compromise option to meet the current and future DSO needs and effectively recover from a black start scenario.

6 Acknowledgements

This work is part of the LV Engine project led by SP Energy Networks and funded as under the Ofgem Network Innovation Competition.

7 References

[1] Andreadou, N., Guardiola, M.O. and Fulli, G., 2016. Telecommunication technologies for smart grid projects with focus on smart metering applications. Energies, 9(5), p.375.

[2] Kinan G, Federico C., and James I., “The reliability and optimal data usage of BGAN Satellite Communications for Remote Outstations,” 2018 International Conference on Smart Applications, Communications and Networking, SmartNets 2018, 2018.

[3] Rossella M. and Konstantinos M., ENISA, “Communication network interdependencies in smart grids”, European Union Agency For Network And Information Security, (ENISA), 2015.

[4] Celli, Gianni, et al. "Reliability assessment in smart distribution networks." Electric Power Systems Research 104 (2013): 164-175.

[5] IEEE, “Recommended Practice for Collecting Data for Use in Reliability, Availability, and Maintainability Assessments of Industrial and Commercial Power Systems”, IEEE Std 3006.9-2013.

[6] ENA, Engineering Recommendation G91 Issue 1 (2012) - Substation Black Start Resilience

[7] IEC 62351: 2016, “Standards for Securing Power System Communications”, 2016.

[8] SP Energy Networks –LV ENGINE project, https://www.spenergynetworks.co.uk/pages/lv_engine.aspx, accessed 12 March 2020.