



# LV ENGINE

**Recommendations on Field Communication  
Requirements for the LV Engine Smart Control System**



### About Report

Report Title : Field Communication Requirements for the LV Engine Smart  
Control System

Report Status : Draft

### Report Progress

Created by : Kinan Ghanem 14/10/2019

Reviewed by : Ibrahim Abdulhadi, Ali Kazerooni 23/10/2019

Recommendations by : Simon Hill 06/12/2019

Approved by : Ali Kazerooni 02/03/2020

Signed-off by : Michael Eves 02/03/2020

### Report History

| Date       | Issue         | Status             |
|------------|---------------|--------------------|
| 20/09/2019 | V0.4          | First issued draft |
| 25/10/2019 | V1.0          | First issue        |
| 06/12/2019 | V2.0          | Second issue       |
| DD/MM/YYYY | <Insert Text> | <Insert Text>      |
| DD/MM/YYYY | <Insert Text> | <Insert Text>      |
| DD/MM/YYYY | <Insert Text> | <Insert Text>      |



## Disclaimer

This report has been prepared as part of the LV Engine project, a globally innovative project to demonstrate the functionalities of a Smart Transformer, funded by Ofgem through the Network Innovation Competition mechanism. All learnings, outcomes, models, findings information, methodologies or processes described in this report have been presented on the information available to the project team at the time of publishing. It is at the discernment and risk of the reader to rely upon any learnings outcomes, findings, information, methodologies or processes described in this report.

Neither SPEN, nor any person acting on its behalf, makes any warranty, representation, undertaking or assurance express or implied, with respect to the use of any learnings, outcomes, models, information, method or process disclosed in this document or that such use may not infringe the rights of any third party. No responsibility or liability is or will be accepted by SPEN, or any person acting on its behalf, including but not limited to any liabilities with respect to the use of, or for damage resulting in any way from the use of, any learnings, outcomes, models, information, apparatus, method or process disclosed in the document.



## Executive Summary

This Report describes the main requirements for enabling the communication between the LV Engine Smart Control System (SCS) components. It particularly focuses on the communication between SCS field components and integration between the SCS and SPEN enterprise network. Based on the Smart Transformer (ST) and SCS technical specifications, the activity reported on here identified the data flows required to perform the required SCS functions. This has formed the basis for determining the bandwidth and latency requirements for this data exchange and subsequently the available communication technology options that are most suited for this application – highlighting advantages and limitations of each option. Learning from previous relevant innovation projects as well as future secondary substation functionality was also taken into account when defining the communication requirements.

This report focuses on answering the following three questions:

- What are the recommended technology options to be used in LV Engine SCS field communication?
- What are the bandwidth, latency and security requirements to enable the functionality of the LV Engine SCS underpinned by reliable communications?
- What are the main communication interfaces and equipment requirements for SCS connectivity in the secondary substation?

This activity identified Private Long Term Evolution (LTE) and Broadband over Powerline (BPL) based communication solutions as the two most suitable technologies that meet the project requirements, as well as the provision of additional headroom for future secondary substation communication requirements. However, additional experimental verification is required to ensure that reliable communications can be established with these technologies to subterranean LV link boxes.



## Contents

|  |    |
|--|----|
| Executive Summary .....  | 3  |
| 1 Introduction .....   | 6  |
| 2 Summary of Key Communication Technology Learnings from LV Monitoring and Automation Projects ..... | 6  |
| 2.1 OpenLV Project .....   | 6  |
| 2.2 LVPaC Project .....  | 7  |
| 2.3 SSEN LV Monitoring .....   | 7  |
| 2.4 Net2DG Horizon 2020 Project .....  | 7  |
| 2.5 UKPN Active Response .....   | 7  |
| 3 High Level Requirements and Functionality of the Field Communication Network used by the SCS ..... | 8  |
| 4 Data Flow and Bandwidth Requirements .....   | 10 |
| 4.1 Bandwidth calculations .....   | 10 |
| 5 Review of Relevant Standards and Telecommunications Technology Options .....                       | 12 |
| 5.1 Low Power Wireless Access Networks (LPWAN) .....   | 12 |
| 5.2 Mobile networks .....  | 13 |
| 5.3 Wireless mesh networks .....   | 14 |
| 5.4 Power-line communication .....   | 14 |
| 5.5 M2M/IoT satellite communication: .....   | 15 |
| 6 SCS Architecture .....   | 16 |
| 7 Cyber Security Considerations .....  | 18 |
| 8 Recommendations, Observations and Lessons Learnt .....   | 20 |
| 8.1 Bandwidth .....  | 20 |
| 8.2 Communication technology .....   | 20 |
| 9 References .....   | 22 |
| 10 Glossary of Terms .....   | 24 |
| 11 Appendix: IEC 104 and DNP3 Message Size .....   | 25 |



## 1 Introduction

This document presents the requirements for the communications links necessary to enable the functionality of the LV Engine Smart Control System (SCS). Information in this document is intended to support the procurement of the SCS as well as inform SP Energy Networks (SPEN) internal stakeholders (e.g. IT/OT engineers) to specify field and corporate communications infrastructure that is fit for purpose.

This document first of all summarises the main lessons learnt from the previous UK funded projects related to the communications for LV network automation functions. The document then presents the methodology for calculating communication bandwidth requirements based on a set of defined data points and agreed communication protocols that the SCS is expected to use. An accompanying bandwidth calculation tool is supplied with this document. The document also presents communication technology options that can be used to exchange data between the SCS components. Advantages, disadvantages and relative costs of each of the technology options is also presented. Finally, recommendations for the communications architecture (including inside the secondary substation) are provided.

This document assumes prior knowledge of the LV Engine ST technical specification [1] and communication and data management requirements [2]. The information is also presented to an audience with IT/OT experience, so fundamentals of communications and protocols will not be explained.

## 2 Summary of Key Communication Technology Learnings from LV Monitoring and Automation Projects

This section summarises the key learning captured from recent UK innovation projects about the communication technologies that enable LV automation and monitoring. Progress and closedown reports related to these projects have been reviewed, which mostly can be found on the ENA smarter networks portal<sup>1</sup>. First-hand experience with some of these projects is also reported.

### 2.1 OpenLV Project

The OpenLV project led by WPD (funded under Ofgem's NIC scheme) covers the specification, design and testing results of a secondary substation based LV monitoring and automation platform [3]. The main learnings encompass applications relating to communications between the deployed trial platforms as well as between the deployed platforms and remote data servers/cloud based management servers. The wide area communications links for the OpenLV project are provided over secure 3G/4G mobile data networks, where a dedicated private access point is set up for the project trials to support roaming between three UK mobile operators (to ensure the availability of mobile network coverage).

The main learning from the project covered areas such as technology and equipment, IT and telecommunications and processes and procedures. The main communications related learnings are:

- A dedicated private Access Point Name (APN) for the OpenLV project trials is recommended. This works as a gateway between the mobile network and IoT devices, rather than using a shared private APN, which improves the security of the overall solution.

---

<sup>1</sup> <https://www.smarternetworks.org/>



- An adequate 3G/4G signal strength at a site to ensure reliable communications is essential. If there is an issue with the signal strength and its quality, then deploying an outdoor antenna to improve signal strength is recommended.
- Monitoring of sites to ensure regular communications is occurring, with alarms set up to flag any issues. This is vital as several hardware issues, particularly with routers, have been detected and rectified.

Further learnings that encompass the technology, primary plant as well as processes and procedure can be found in [4, 5].

## 2.2 LVPaC Project

Electricity North West led a project called LVPaC that considered the LV protection and the required communication technology to connect with LV switches for active network management. Remote modification of the LV switch device installed inside the LV link box was possible via a communication gateway. The main findings from the project demonstrated enhanced protection functionality of the LV devices. Moreover, the project implemented DNP3 communications between the LV active network management (Lynx devices) and the Electricity North West control room. A flexible scanning mechanism was implemented to poll a number of signals from single and multiple devices on the LV network. One of the key learnings from the project was that the gateways require a live connection to the Kelvatek server. If the server is not available, scanning on the gateway which communicates via the Electricity North West Vodafone 3G/GPRS Access Point will stop. Furthermore, if the gateway loses power, it requires 60 seconds to restore the connection. This has been solved via installing a battery backup for the gateway. More details about the project can be found in [6].

## 2.3 SSEN LV Monitoring

SSEN published a report titled “Demonstrating the Benefits of Monitoring LV Networks with embedded PV Panels and EV Charging Point (SSET1002)”, which considered communications requirements for transmitting LV monitoring data back to the DNO [7]. The technology mainly used in this SSEN project was GPRS/GSM. The recommendations from the report suggest using alternative communications solutions as the use of GPRS / GSM communications may not be suitable in all installation locations. The project did not seek to analyse different communications technologies. Moreover, the project confirms that communication and transmission of the collected and measured data can be achieved by means of GPRS. And if signal strength is an issue, then this can be resolved by extending the antenna.

## 2.4 Net2DG Horizon 2020 Project

The Net2DG Horizon 2020 project funded by the EC demonstrated a solution that correlates data from smart meters, smart inverters and information from the DSO, which enables the development of novel LV grid observability applications for voltage quality, grid efficiency, and LV grid outage diagnosis [6]. RF MESH communication combined with 3GPP based WAN connection is used as the communications solution.

## 2.5 UKPN Active Response

UK Power Networks Active Response project deliverable “High-Level Design Specification of Advanced Automation Solution” [9], specifies the LV automation solutions where Link box communications are used for the remote control of LV switches that are installed in link boxes as well as at secondary substations. The project is yet to identify the best method for providing communications links to these sites from wherever their local master RTUs are located. Link boxes are particularly limited in space to anything but very small communications components. The main learning from the project so far was the idea of trying Power Line Carrier (PLC) communications between link boxes and master RTU locations is not recommended based on findings from a previous project (FUN-LV) where the technology was not successful.





Several ongoing projects are considering low power wireless access technologies such as NB-IoT and Random Phase Multiple Access (RPMA). SPEN NIA project “400kV Dynamic Cable Rating Retrofit Project utilising RPMA Communications Technology” that started Jul 2019 aims to investigate the feasibility of using the RPMA wireless technology coupled with point sensors and integrated with a Dynamic Cable Rating (DCR) [10]. Another ongoing SPEN project “Enabling Monitoring and Control of Underground Assets” aims to investigate whether RPMA technology can achieve wireless coverage to the link-box and the communication solution can provide a cost effective technical solution [11]. Additionally, testing the penetration of the NB-IoT technology is part of a current collaboration between SPEN and Vodafone [12]. The main findings from this project will be presented in the LCNI conference in Glasgow in October 2019.

### 3 High Level Requirements and Functionality of the Field Communication Network used by the SCS

The potential SCS architecture envisaged for LV Engine is depicted in Figure 1. This consists of a regional smart controller (RSC) and local smart controllers (LSC). This architecture is specified in [1, 2] based on functionalities expected from overall SCS and initial engagements with SPEN IT/OT departments conducted by LV Engine team. The LSC communicates with the ST, LV normally open point (NOP) and RSC via field online (which resides within SPENs operation management zone). The RSC is assumed to reside within SPENs operation management zone and has access to smart metering data, integrates with the network management system (NMS) and LCSs deployed in secondary substations.



**Figure 1 High-level architecture of the communications technologies enabling the SCS [1, 2]**

The communication and data integration between the components of the SCS and selection of suitable communications technologies requires consideration of:

- The definition of data to be transmitted and its associated bandwidth: the data flows are defined based on the ST technical specifications, taking into account communicating components of the SCS and their integration with the SPEN operational communication network;





- Cyber security: considerations are based on the UK NIS directives<sup>2</sup> and IEC 62351. Two levels of security are considered the preferable option by some DNOs due to the provision of encryption in addition to authentication.
- The communication latency: communication latency for the LV Engine is specified in the communications and data management requirements, where the maximum latency requirement of the LV Engine is 30-60s;
- Communication redundancy: this is not considered a key requirements as the SST will default to local control. Redundant communication with the secondary substation, in general, is governed by SPEN requirements;
- Overall system reliability and optimum performance of the communication technology: The performance of any chosen unproven communication technology should be tested prior to any field development. The communication technology should comply with the Ofcom regulations in terms of the available spectrum and operating frequency as well as meet the requirements from the communications act (i.e. The Electronic Communications Code<sup>3</sup>).

The requirements in terms of the bandwidth, cyber security and the latency will be covered in the following sections and further explained in the supported bandwidth calculations.

The reliability of any chosen communication technology for the LV Engine should ensure the following:

- Availability: the service/network should be available on demand and it is guaranteed 24 hours for control applications.
- Accessibility: the field device can use the network to send the required message to the control centre or destination. For wireless communications, the accessibility means there is enough bandwidth for the device to transmit data through the link.
- Quality of Service: any communication technology should be able to manage and exchange high quality data (i.e reduce packet loss, latency and jitter).
- Maintainability: the technology should be able to be repaired in a suitable time frame.
- Resilience: the technology should be able to recover any connection failure rapidly.

Moreover, communication technology selection is also dependent on affordability, which cannot be ignored for large scale field deployments and how cost-effective their integration with existing systems (e.g. enterprise network) is as well as the lifetime cost of operating the communications solution.

Finally, power backup should be considered for any deployed communications technology in the power utility. ENA Engineering recommendation G91, issue 1, 2012 require that substation batteries should have enough capacity to meet the standing demand for 72 hours. This will ensure that there is sufficient backup power for the site to remain in operation for 72 hours after a power supply loss to ensure that auxiliary systems and command and control structure remain unaffected after grid failure (i.e. black start procedure after a blackout) [26, 27].

<sup>2</sup> <https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018>

<sup>3</sup> <https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/electronic-comm-code>



## 4 Data Flow and Bandwidth Requirements

In order to determine the bandwidth requirements for the LV Engine SCS, the first step is to identify the data flows between communicating components, namely the Normally Open Point (NOP), Local Smart Controller (LSC) and Regional Smart Controller (RSC). These data flows and subsequent bandwidth calculations are summarised on an accompanying calculation spreadsheet. The bandwidth calculations assume the use of DNP3 or IEC 60870-5-104 (IEC104) protocols as agreed with SPEN which is based on their outlook for using these protocols for new communications hardware. Prior to consulting the spreadsheet, the following points should be considered. Note that a number of parameters in the spreadsheet can be adjusted to reflect up to date assumptions:

1. The message size for each protocol is based on empirical experience from previous and ongoing projects at the PNDC (i.e. Bandwidth and security requirements for the smart grid core research project), where the packets are captured by Wireshark for different tests configurations.
2. Some estimated polling rates are also taken from previous PNDC empirical experience as well as from practices from the DNOs.
3. The security overhead is based on 2 levels of security for IEC104 whereas for DNP3 calculations are based only on IPsec level of security which follows industry practice. Other DNP3 security techniques are being developed by vendors. More details can be found in section 6 of this document.
4. 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. Latency associated with larger data transfers (e.g. firmware updates) will be larger than that. This latency will be considered in subsequent technology recommendations and will not be expressed explicitly in the bandwidth calculation spreadsheet.
5. The estimated monthly data usage of each communicating component is also included in the bandwidth calculation tool. The total estimated data requirements for LV Engine installations can be calculated based on the expected number that SPEN will operate.
6. The configuration of each protocol (DNP3 and IEC104) will play a significant role in selecting the minimum number of packets and their required polling, which affects the bandwidth. The estimated message size of the IEC 104 is based on testing carried out at the PNDC. More details about the message size calculations can be found in Appendix 1.

More details about the DNP3 and IEC 60870-5-104 mapping along with their structures can be found in [14-18].

### 4.1 Bandwidth calculations

Based on the requirements of the LV Engine project namely the LV Engine ST technical specifications [1] and communication and data management requirements [2] the calculated bandwidth in the accompanying bandwidth calculation tool is summarised in this section. Table 1 and Table 2 show the estimated bandwidth requirement for the LV Engine based on un-batched reporting (which results in the worst case bandwidth requirements), because un-batching reporting is assumed to be the only available option for IEC101. The bandwidth calculation tool defines the data flow between the LV Engine components and the type of each data flow (i.e. whether it is for monitoring or control). Moreover, how the message sizes have been calculated for different data types is explained in the bandwidth calculation tool and in Appendix 1. It is assumed that an RSC is connected to 18 LSCs when the RSC is located in the primary (in line with typical maximum connectivity possible via UHF/VHF radio communications currently used for secondary substations



as advised by SPEN). 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.

**Table 1 Calculated bandwidth for secure IEC104**

| <b>Secure IEC104 un-batching</b> | <b>Required data rate (bps)</b> | <b>Estimated monthly data with IPsec (Mbyte)</b> |
|----------------------------------|---------------------------------|--|
| NOP (12 analogues + 2 digitals)  | 588                             | 190  |
| LSC (87 analogues + 23 digitals) | 3979                            | 1290   |
| RSC (connected to 18 LSC)        | 71620                           | 23205  |

**Table 2 Calculated bandwidth for DNP3 protocol**

| <b>DNP3 with IP security</b>     | <b>Required data rate bps</b> | <b>Estimated monthly data with IPsec (Mbyte)</b> |
|----------------------------------|-------------------------------|--|
| NOP (12 analogues + 2 digitals)  | 563                           | 183  |
| LSC (87 analogues + 23 digitals) | 3379                          | 1095   |
| RSC (connected to 18 LSC)        | 60806                         | 19701  |

Polling time is considered as 90 seconds after discussion with SPEN (based on the project specifications [1] measurements should be collected each 1 – 5 minutes) and the analogues are sent with time stamps. Empirical results obtained a previous PNDC project (Bandwidth and security requirements for the smart grid) were obtained without timestamps. If timestamps are to be included, each field measurement will require an additional 3 bytes timestamp overhead for each object in the IEC 104 Packet [14]. The accompanying bandwidth calculation tool incorporates the time stamp requirement, and 3 bytes are added to the original packet size obtained from the lab test. For example, where the complete message size of one analogue IEC 104 is 262 Bytes without a time stamp, the new message size with a time stamp will be 265 Bytes. This will not add a significant bandwidth requirement to the calculations. The packet sizes with timestamps and without timestamps are detailed in Appendix 1, Table 5.

**Table 3 Monthly data and required data rates with and without IP security (IP sec)**

| <b>Communication node and protocol</b> | <b>Data rate bps without IP sec</b> | <b>Monthly data without IPsec (MByte)</b> | <b>Data rate bps with IP sec</b> | <b>Monthly data IPsec overhead (MByte)</b> | <b>IP sec overhead in %</b> |
|--|-------------------------------------|---|----------------------------------|--|-----------------------------|
| NOP (DNP3)                             | 433                                 | 140                                       | 563                              | 183  | 23.5%                       |
| LSC (DNP3)                             | 2645                                | 857                                       | 3379                             | 1094                                       | 21.6%                       |
| RSC (DNP3)                             | 47610                               | 15426                                     | 60822                            | 19692                                      | 23%                         |
| NOP(IEC 104)                           | 419                                 | 147                                       | 589                              | 191  | 22.5%                       |
| LSC (IEC 104)                          | 3050                                | 999                                       | 3979                             | 1290                                       | 22.5%                       |
| RSC (IEC 104)                          | 54900                               | 17982                                     | 71622                            | 23220                                      | 22.5%                       |



Table 3 shows the overhead caused by the IP security, where the analysis shows that the overhead caused by the IP sec will vary based on the message size. Smaller message sizes will result in a higher overhead in terms of bandwidth needs. PNDC testing indicates that the message size is a significant factor influencing the security overhead as a percentage of the packet caused by the IP sec through a VPN. The security requirement for LV Engine with un-batch reporting will cost (22 - 28%) of the total required bandwidth as shown in

Table 3.

DNP3 and IEC 104 can support batch reporting which enables the DNP3/IEC104 packets to carry several measurement points in the same message. DNP3 for example can be assigned a class, which could be used for batch reporting [15-18]. In our calculations, the analogues reported spontaneously (i.e. unsolicited) and assigning a class would be unnecessary.

Bandwidth can be saved if the DNP3/IEC104 is configured to support batch reporting. (i.e. in DNP3, the poll request can ask for class1, 2 or 3 data, then all signals assigned to that class can be returned, or all signals within that class that have changed can be returned. Furthermore, a range of DNP3 point addresses can also be requested). During configuration, we could then assign the data into a class, so for example NOP status could be assigned to class 1, voltages, currents, active & reactive measurements of SST into class 2, and everything else into class 3.

## 5 Review of Relevant Standards and Telecommunications Technology Options

A wide range of communications technologies can be used to enable the data exchange between the LV Engine components for monitoring and control purposes. The suitability of wireless technologies such as LPWAN (i.e. NB-IoT, RPMA) and BGAN satellite communication along with G3/G4 and private LTE varies based on their availability (rural/urban) and the main applications (control/monitoring). In this section, the technologies to be considered will be described along with their advantages, disadvantages and relative costs. The communications will only cover the links between NOP and LSC and between LSC and RSC in line with the SPEN enterprise and operation communication architectures. The links are shown in Figure 2.

### 5.1 Low Power Wireless Access Networks (LPWAN)

LPWAN technology supports long-range communication, which allows new types of services. Long Range (LoRa), Sigfox, Random Phase Multiple Access (RPMA) and NB-IoT are the major technologies in the LPWAN space and they have been developed mainly for IoT and Machine to Machine (M2M) applications. Each technology has its own advantages and at the same time suffers from many drawbacks. Based on the ST technical specifications (i.e a maximum latency of 10s for DC, HV, LV AC voltage set point and LV active and reactive power set points), some technologies such as LoRa and Sigfox are not be suitable due to the following reasons:

- Data cannot be transmitted continuously because of spectrum regulations and the duty cycle restrictions (typically 1%).
- The performance (i.e latency) degrades the further away the sensors are from the gateway.
- Bandwidth and data rates limitations (less than 50 kbps).
- Although both technologies can support 2 ways communications, the down link communications from LoRa-Sigfox gateway to the sensors is limited.
- Not suitable for any control application.



- The maximum latency of 10s for some LV Engine messages cannot be achieved.
- The penetration of the signal can prevent the signal from reaching many distributed assets for the LV Engine (i.e. the ability of the signal to penetrate the link boxes and underground assets should be tested).

Real time monitoring for industrial automation, critical infrastructure monitoring and LV control application requires a degree of real time operation (maximum of 10s latency for LV Engine). Where real time operation requires low latency, both LoRaWAN and Sigfox technologies cannot be considered an optimal solution for the LV Engine automation.

A licensed option of the LPWAN technology is NB-IoT, which was developed based on the 3GPP Release 13 specifications using a subset of LTE standard with a much narrower bandwidth (180 kHz). The technology can be operated over the existing 2G/3G/4G spectrums, which can offer good coverage in most residential areas. The penetration of the NB-IoT can be better than the other LPWAN technologies as some mobile operators run the technology in the 700MHz frequency band. The limited bandwidth of NB-IoT (200 kbps) and the extra delay caused by the signal quality (where the coverage is poor) are the main disadvantages of the technology. If TCP will be used to transmit and exchange the messages, NB-IoT latency may not meet the packet retransmission time outs (since NB-IoT is a best effort delivery mechanism). This may make it difficult for the DNOs to select this option for control applications especially if they use IEC104 which requires a reliable TCP/IP connection. Moreover, over the air firmware updates can be challenging over NB-IoT if the files sizes are large [13].

Another LPWAN technology is RPMA which is an unlicensed technology that operates in the 2.4 GHz band and provides bandwidth of around 38kb/s per access point. It does not have a duty cycle restriction. This means that the throughput could be divided across any number of distributed devices. Such flexibility could be acceptable for LV Engine applications. However, the penetration of the signal without an external antenna is worse than NB-IoT. Moreover, the limited available shared bandwidth may not be sufficient for all future applications and the technology is not yet deployed in the UK market. Although, the available bandwidth of NB-IoT and RPMA could meet the requirements for the NOP with the LSC, the penetration of the signal to the link box without extended antenna is an issue. Findings from ongoing trials of NB-IoT will be reported in due course.

## 5.2 Mobile networks

Mobile network operators such as Vodafone, O2 and EE run different technologies such as GPRS/3G/4G and they are in the process of deploying 5G technology. Such technologies are almost available everywhere in urban areas and do not have bandwidth limitations (compared to the LPWAN technologies) and the other restrictions that LPWAN suffer from. As such, this is a viable option for communications. Regarding the link box penetration, mobile networks which operate in different frequency bands will have different penetration capabilities. For a spectrum with a frequency band of more than 900 MHz (i.e 1800 MHz and 2100 MHz bands), the penetration may not be sufficient for some hard to reach areas and link boxes. For mobile base stations which operate with lower bands (i.e 800 and 700 MHz), the penetration can be similar to that of NB-IoT. The signal penetration for the available technologies should be tested and the requirement to have an extended antenna should be evaluated.

Private wireless communications such as Private LTE can be an alternative choice as the bandwidth requirements could be easily met provided that the DNOs obtain sufficient spectrum to accommodate LV Engine traffic as well as other secondary substation communication traffic. Determining the spectrum required for secondary substation communication is part of ongoing testing and future activities at the PNDC. Initial results indicate that the minimum spectrum needed for secondary substation monitoring (with two level of security in place) is 5 MHz.





Connecting distributed devices often require communications equipment that can be easily installed and integrated with SCADA. LTE technology can be operated by a commercial mobile network or deployed as a private LTE network to deliver scalable and suitable data rates for utility applications. Using LTE technology can offer flexibility advantages to DNOs including:

- LTE gateways can be integrated into an existing setup in the power networks;
- LTE gateways are backward compatible and designed to work with existing mobile technologies such as 2G and 3G;
- LTE gateways can support RS-232 for serial connectivity, IoT connectivity as well as Gigabit Ethernet for local communications;
- Most industrial automation vendors use LTE as a radio interface in their products;
- Private LTE gateways can be integrated and interworked with commercial 4G/5G infrastructure operated by a Mobile Network Operator (MNO).

### 5.3 Wireless mesh networks

Wireless mesh networks consist of several distributed radio mesh nodes that are designed to be integrated with many distributed assets and applications. They can support automation, monitoring and security for connected to the field devices. Also they can cover hard to reach areas, and operate wireless links of a range of up to 2km in an optimal environment. They can be operated in different unlicensed spectrum bands such as 2.4 GHz, 5 GHz and 870-873 MHz RF bands and can deliver 300kbps with a Round Trip Time (RTT) less than 1.5s. The operation of the 870-873 MHz RF bands could extend the penetration of the signal, however, the possibility of communicating with link boxes has not been verified.

Although a mesh network offers a number of technical advantages, it suffers from some limitations when applied to the DNO applications. For example, each connected device to a mesh network requires the following:

- A data connection; either Serial or Ethernet.
- Either a 230V AC power supply or a DC power supply (between 10V and 60V) due to the power consumption requirements.
- Ability to install weatherproof housing or provide space in existing cabinets for the mesh network bridge/switch. This may not be achievable in space constrained link boxes.
- An extended antenna may be required to guarantee communication to a link box.
- Mesh devices (bridge/gateway) are relatively expensive with (a few hundred pounds each).

### 5.4 Power-line communication

Power-Line Communication (PLC) can be a very cost effective solution for the communication between the NOP and secondary substation (i.e. LSC). The reliability of the connection, however, should be assessed to ensure that the Quality of Service (QoS) could meet the requirements of the LV Engine SCS.

There are two PLC technologies, namely Broadband over Power Line (BPL) and low-frequency narrowband PLC. Broadband PLC allows a data rate for several Mbps, which operates in the 2-30 MHz band to support applications with high data rates. While a low-frequency narrowband PLC has an ability to support applications with data rate of up to 128 kbps.



The main advantages of the PLC technology to transmit the measurements from the NOP to the LSC are:

- No new communication link infrastructure (i.e. cables/antennas) are required, since PLC uses the existing power cable to communicate between the NOP to the LSC.
- The technology does not rely on any radio penetration restrictions (it can reach 1.7km in LV networks [21])
- PLC is independent of third party providers (i.e. no monthly fees).
- Some field tests on the low voltage system have measured ranges of up to 1 mile.

The main disadvantages of the PLC technology are:

- PLC is subject to the noise imposed on power lines and is subject to signal corruption by signal-distorting transformers.
- The bandwidth offered by the PLC is dependent on the signal to noise ratio, so the noisy environment of the power lines could affect the quality of the connection.

PLC is however still an appropriate technology for a number of applications and is used by DNOs. Some successful use cases for Broadband Power line (BPL) provided connection to transfer data from field devices (i.e. smart meters) to the substation. It is used by the power utilities in Germany as an option for devices which are located in a basement and are unreachable by wireless communication technologies [23-25]. Many projects for BPL for smart grid applications were delivered [23]. These projects enabled metering services and network management (including 11kV networks) via BPL.

BPL can use various techniques to eliminate the noise such as Orthogonal Frequency Division Multiplexing (OFDM) and Smart Notching. Another ongoing research on PLC technology suggests that the filtering system can be utilised to reduce the interference in the 120 – 150 kHz band that is introduced into the network by receivers [21, 22].

BPL could work for up to 4 KM. So 500 – 800 metres which is the upper limit between devices in a typical distance between substations and link boxes indicates that BPL is expected to function adequately. Other considerations such as the topography and nature of the area to be connected (rural or urban), age and type of power cables, availability of installers (own or contracted) and access to the grid will affect the cost of the installation.

Although, BPL seems to be a promising communication technology to connect the NOP to the LSC, further empirical and field trial evidence of the reliability of the connection needs to be established.

## 5.5 M2M/IoT satellite communication:

Due to its wide geographic coverage, satellite communication can be a suitable alternative for power system automation for reaching remote substations. Satellite IoT and SCADA solutions such as Broadband Global Area Networks (BGAN) M2M technology could offer an option for IP-based connectivity services and could be suitable for managing remote assets such as LV pillar switchgear. BGAN has a global coverage and data rates of up to 448 kbps with a latency around (800 ms). It suffers from some drawbacks such as the impact of weather conditions, high latency and high cost which limit their use. In the absence of other technologies, BGAN could be used for LV Engine to connect the LSC to field online.

Satellite IoT can provide the required connectivity to LPWAN Technologies such as LoRa, RPMA and NB-IoT in hard to reach areas (i.e. satellite signal are available everywhere). This allows the gateway to serve hundreds of distributed sensors. The hybrid satellite-LPWAN approach can be





used for several remote monitoring applications. Satellite IoT technology can offer the required backhaul of any LPWA networks; however, it will not add to the end technology data rate. If Satellite IoT technology is connected to an evolved NodeB (4G radio base station) with sufficient spectrum, this will add significant improvements to the services in hard to reach areas and will enable LV Engine communication. Currently, the cost of using Satellite to carry the data is expensive, where the cost of carrying 1 Byte can be several folds higher than any alternative technology.

A comparison of different available wireless technologies for LV monitoring are summarised in Table 4.

**Table 4 comparison between different available communication technologies**

|  | LoRa Sigfox             | NB-IoT                   | RPMA                         | Wireless mesh <sup>4</sup> | LTE Private LTE  | UHF   | PLC                | Satellite M2M/IoT          |
|--|-------------------------|--------------------------|------------------------------|----------------------------|--|---|--------------------|----------------------------|
| <b>Peak data rate per base station</b>   | 50 Kbps                 | 250 kbps                 | 31 kbps                      | 50kbps - 2.4 Mbps          | More than 3 Mbps (based on the bandwidth h) <sup>5</sup> | Up to 1 Mbps for 200 KHz (based on 256 QAM) | 128 kbps           | 448 kps                    |
| <b>Latency</b>   | More than 10s           | 1-10s based on coverage  | 5 - 40s based on coverage    | less than 2 seconds        | Less than 100ms  | Less than 2 seconds                         | less than 1 second | 800 ms                     |
| <b>Link box penetration without extended antenna</b>                                       | Needs to be tested      | Needs to be tested       | No                           | No                         | No   | Needs to be tested                          | Yes                | Needs to be tested for IoT |
| <b>Relative Cost</b>   | Very Low                | Very Low                 | Very Low                     | High                       | Medium   | Medium to High                              | Low to medium      | High                       |
| <b>Factors influencing availability</b>  | Location of the gateway | Mobile operator coverage | Location of the base station | Mesh node location         | Mobile operator coverage                                 | Location of the master station              | Local installation | Available                  |
| <b>Support future deployment (adaptive demand response, EV storage and DER management)</b> | Very Limited            | Limited                  | Limited                      | Good                       | Good   | Very Limited                                | Limited            | Good                       |

## 6 SCS Architecture

With reference to Figure 2, the NOP requires a communication gateway to enable data exchange with the LSC in the secondary substation cabinet. The gateway should have at least an Ethernet and radio interface.

<sup>4</sup> It is based on neighbourhood Mesh Area Networks rather than WAN Mesh, where data rates can go up to 270 Mbps

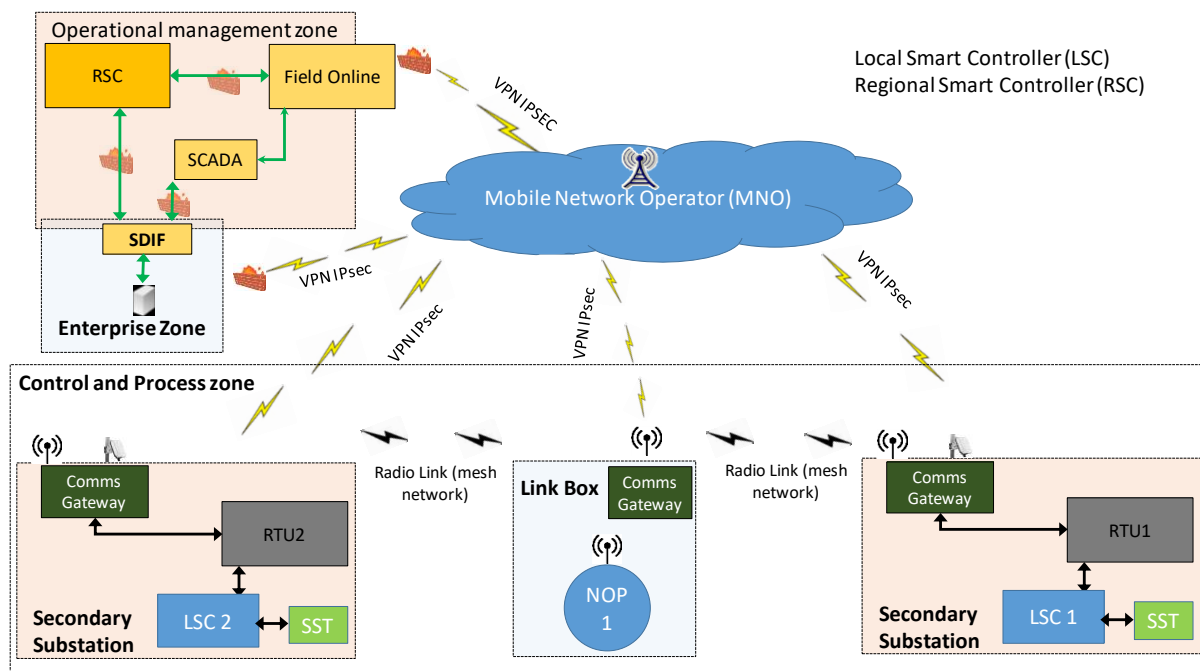
<sup>5</sup> LTE supports bandwidths of {1.4, 3, 5, 10, 15, 20} MHz, with 3MHz, 5 Mbps could be achieved (subject to operation mode and received signal condition)



The secondary substation gateway will collect data and measurements from the NOP and LSC and communicates to the SPEN field online which in turn forwards the messages to be processed, analysed or archiving centrally.

The secondary substation gateway communicates to field online 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 SPEN such as private LTE. The gateway should be configured to send/receive data to/from three locations (field online and the LSC and NOP). The NOP gateway should be equipped with a radio with at least two SIMs and an Ethernet interface.

The transmitted data from the NOP 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, which provides authentication, integrity, and confidentiality of network packets data/payload.



**Figure 2 High-level communication architecture for LV Engine**



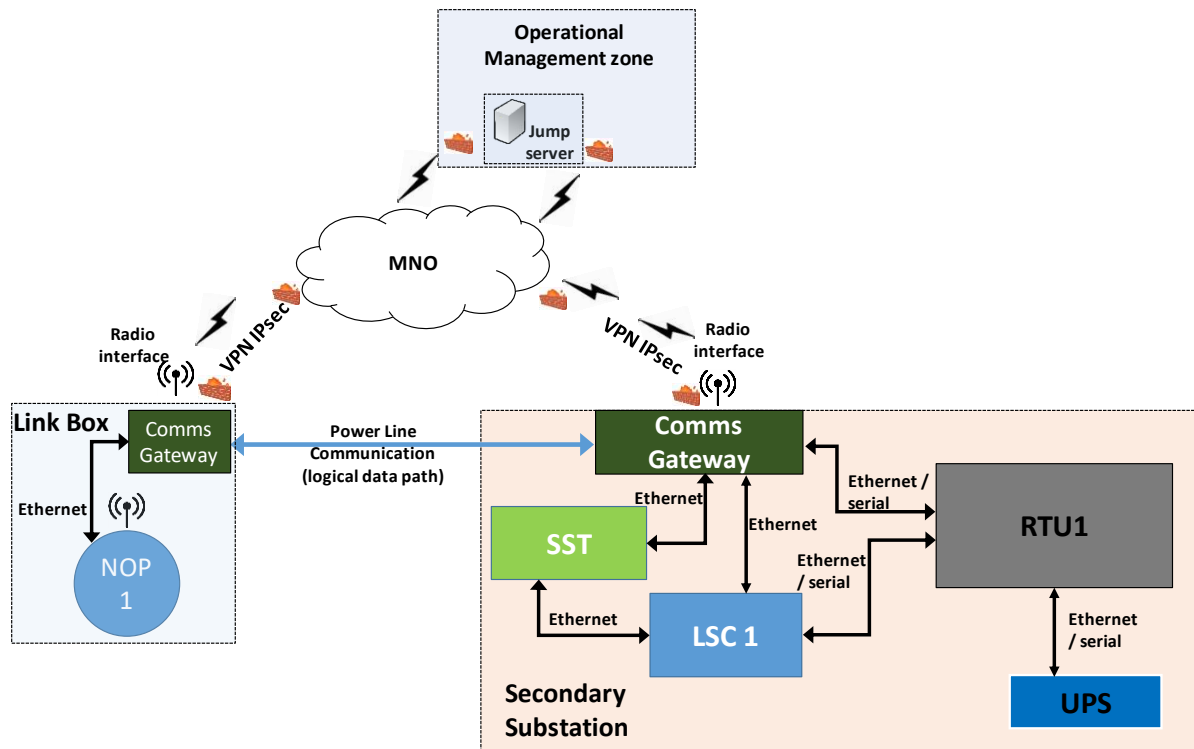
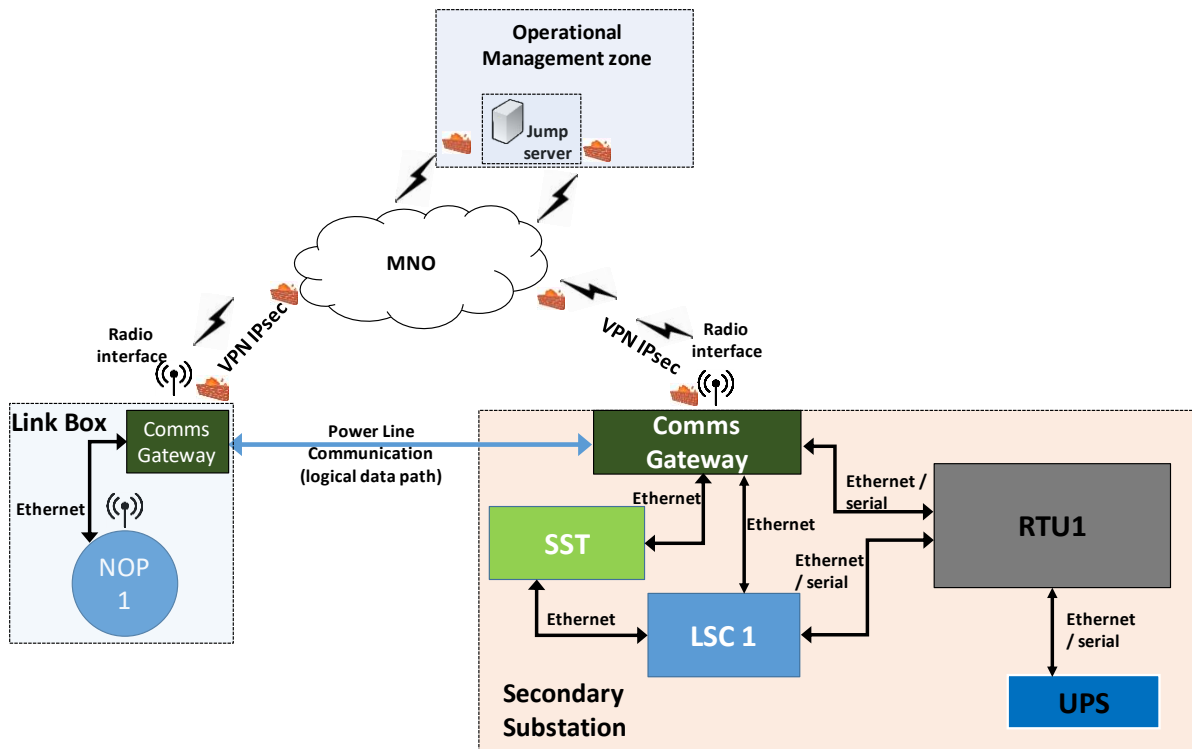


Figure 3, illustrates the main communication interfaces needed to connect the LSC to the RTU. The main interfaces are:

- Ethernet between the LSC and SST, between LSC and RTU also between RTU and secondary substation gateway.
- LSC should have at least two communication interfaces (Ethernet and radio), the Ethernet is to connect the LSC to the SST and the radio to communicate with the NOP a outline in the communication technology review above.
- To ensure support for legacy RTUs, the LSC should also have a serial interface (e.g. RS485).
- To meet the DNO requirements for backup power in a black start scenario, battery back up power should support at least 24 hours of operation for each secondary substation. This is typically supported via an uninterruptable power supply (UPS) composed of a pair of 12V, 12-15 Ah rechargeable batteries typically specified by SPEN.





**Figure 3 Main communication interfaces for the LV Engine components**

Any SCADA message from master should come through the field online, where the master SCADA connects to the slave gateway through a proper communication technology. The analogue and digital measurements along with any alarms for the LSC should be sent to the RSC through the field online. The gateway should also be able to generate events based on the main requirements for the LV Engine. The gateway also should be configured for a proper time synchronization through an NTP server.

Any remote access and third party remote connection for configuration, maintenance or firmware update should be done through a secured VPN connection where, Enterprise zone security arrangements should issue, monitor and enable any access to any field device with a tracked secure access through DMZ and firewalls.

## 7 Cyber Security Considerations

The bandwidth calculations included the overhead of security requirements applicable to power utilities. Based on SPEN policy, IEC 62351 should be complied with. Based on the IEC 62351 security standard, DNP3 and IEC 60870-05-104 should be secured with at least two levels of security. Security through authentication and encryption are required.

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 IP sec through a VPN between the routers.

The main security techniques that can be used in the utility for authentication, management, encryption and certificate updates are listed below:

- The Internet Protocol Security (IPsec) authentication and encapsulation standard is widely used to establish secure VPN communications. This protocol is considered in the bandwidth calculations as a level of security when using Wide Area Network (WAN).



- Simple Network Management Protocol (SNMP) is used for monitoring the health of network devices, and it can provide data security and authentication.
- File Transfer Protocol Secure (FTPS) is used securely transfer files between a client and a server on a network.
- Syslog is used by the field devices to send event messages to a logging server.
- LDAP (Lightweight Directory Access Protocol) is used to allow access to an application via its ability to store credentials in a network security system and retrieve it with the right password and decrypted key.
- TACACS (Terminal Access Controller Access Control System) is an authentication protocol that enables a remote access server to forward the login password to the authentication server to give an access permission.
- Hypertext Transfer Protocol Secure (HTTPS) is used for securing the connection between the server and the web, ensuring the protection and the privacy of the data.
- Transport Layer Security (TLS) is a security protocol that can provide an end-to-end communications security when transferring data through a network.
- SMTPS (Simple Mail Transfer Protocol Secure) is a technique to secure the exchanged emails. It provides authentication and data confidentiality.

The above security protocols will be applied based on the application, as some applications may not require all the above listed protocols. The accompanying bandwidth calculation tool considers the main security protocols that are needed for LV Engine covering authorisation of the connected devices and authorisation of user management along with security certificate updates and security logging.



## 8 Recommendations, Observations and Lessons Learnt

The outcome of this reported activity identifies the main requirements for utilising the optimal communication technology (in terms of bandwidth, availability and cost) to fulfil the requirements of the LV Engine SCS functions. In addition, some observations were made to meet with the ongoing deployments, scalability and availability.

### 8.1 Bandwidth

- It is recommended to incorporate the bandwidth requirements specific to LV Engine as an integral part of the secondary substation bandwidth requirements being developed by SPEN rather than separately. This should also take into account the recommendation of using a single RTU to support LV Engine as well as existing and future secondary substation communications.
- Since the LV Engine data exchange involves tens of analogue measurements and digital data (up to 87 analogues and 22 digitals) in a frequent polling time between (1-5) minutes, this will consume more bandwidth than currently used in secondary substation (taking into consideration the security overhead). This additional bandwidth requirement exceeds that offered by UHF/VHF radio technology currently in used by DNOs.
- The bandwidth requirements will be affected by:
  - The configuration of DNP3 and IEC 104;
  - The number of analogue and digital measurements and their polling rates (frequency of polling);
  - Level of implemented security in place (i.e. IEC 104 secure, IP sec and the security overhead for authentication and encryption);
  - Remote access for reconfiguration and maintenance.
- It is recommended for the sake of saving bandwidth to use batching polling messages (for IEC 104) and class reporting (for DNP3). However, some legacy RTUs, which use IEC 101, may not support batch reporting. It is also recommended to optimise the frequency of the analogue polling and to consider whether all the analogues should be sent to field online.
- In case of any bandwidth limitations imposed by the communication solution, the optimal configuration can be a tool to accommodate the minimum required data exchange within the available bandwidth headroom.
- Implementation of two levels of security could increase the bandwidth by 2 to 3 folds. Whether two level of security for every function and application in the LV Engine is required or not needs to be confirmed and implications of which must be understood.

### 8.2 Communication technology

The availability of the communication technology along with its cost, peak data rate and ability to accommodate any future developments in distribution network operational requirements will determine the most suitable communication technology for the LV Engine. Consequently, the following should be taken into account:

- Site survey analysis, LV Engine asset mapping and heat-map for the available communications are needed to help select the available communication technology.



- The communication technology for LV Engine should not be considered as a standalone service. SPEN should consider, in detail, the required wireless technology that can meet the requirements of LV Engine in addition to secondary substation functions such as monitoring, HV control, etc. Consequently, the choice of technologies should be limited to a small manageable number. This will avoid a piecemeal approach to the communications, which simplifies the integration of field communications with the enterprise network and should offer lifetime cost savings (e.g. maintenance of a smaller number of communications technologies).
- Third party networks such as mobile networks can be a suitable solution to connect the LSC to field online, where the reliability of the connection (mainly in rural areas) is subject to the coverage and the penetration of the signal.
- Broadband over power line communication could be a cost effective option for communicating between the NOP and the LSC. It is therefore recommended to consider this solution provided that the performance of BPL can be verified prior to any field deployment. There are potential issues with noise and network characteristics that may impact the performance of BPL, but field experience suggests that it is technically feasible to overcome these issues. Furthermore, the secure integration of BPL into the substation communication gateway needs to be designed since it uses the power cables as the communications medium.
- If a wireless communication technology is selected to connect the NOP to the LSC, it needs to be applicable for use in all link boxes. The penetration of any recommended technology needs to be tested prior to any field deployment.
- A private LTE operated by the DNOs (with sufficient spectrum bandwidth) is a highly recommended and suitable option to meet current and future needs for both LV Engine and other secondary substation functions. Private LTE with a frequency band of 410 MHz will have a much better penetration capability compared to public LTE wireless technology. However, any field deployments in the link box may recommend using an extended antenna to achieve the required QoS of the received signal strength.
- Based on the bandwidth, latency and security requirements, LPWAN is not considered an appropriate option for the LV Engine SCS functions overall. The security overhead for authentication and encryption will make it challenging for LPWAN (LoRa, NB-IoT sigfox and RPMA) to meet the bandwidth and latency requirements for the LV Engine.
- Any chosen technology should be able to meet the maximum latency requirements for LV Engine which is around 30-60s. Therefore, Sigfox and LoRA will not be adequate for LV Engine SCS functionality. NB-IoT can meet the latency requirement for the LV engine as the time delay will not exceed 30s.
- For internal communications in the secondary substation, the interfaces of any new physical devices (i.e LSC and NOP) should support Ethernet and serial connections (i.e RS 485) to accommodate any legacy equipment connections in the substation such as existing RTUs.





## 9 References

- [1] SP Energy Networks - Smart Transformer Technical Specifications, LV ENGINE, 2018.
- [2] SP Energy Networks -Communications and data management requirements, LV Engine, 2018.  
[https://www.spenergynetworks.co.uk/pages/lv\\_engine.aspx](https://www.spenergynetworks.co.uk/pages/lv_engine.aspx)
- [3] Western Power Distribution, Open LV, Detailed design of the overall open LV solution,  
<https://www.westernpower.co.uk/downloads/2171> [Accessed: 13-Sep-2019].
- [4] <https://www.westernpower.co.uk/downloads/25762> (Learning from the deployment of the OpenLV Solution) [Accessed: 13-Sep-2019].
- [5] Electricity North West Low Voltage Protection and Communications (LVPaC),  
<https://www.enwl.co.uk/lvpac> [Accessed: 13-Sep-2019].
- [6] Electricity North West, "Low Voltage Protection and Communications" A First Tier Low Carbon Networks, Fund Project Closedown Report, June 2015, <https://www.ofgem.gov.uk/ofgem-publications/96166/lvpacclosedownreportfinal-pdf> [Accessed: 13-Sep-2019].
- [7] LCNF Tier 1 Close-Down Report, Demonstrating the Benefits of Monitoring LV Networks with embedded PV Panels and EV Charging Point, SSEN, 2013, <https://www.ofgem.gov.uk/ofgem-publications/45826/sset1002-lv-monitoring-lcnf-t1-close-down-report-130228pdf> [Accessed: 13-Sep-2019].
- [8] Net2DG Project Net2DG - Leveraging Networked Data for the Digital Electricity Grid,  
<http://www.in4com.de/2-in4com/80-net2dg-project> [Accessed: 13-Sep-2019].
- [9] High-Level Design Specification of Advanced Automation Solution Active Response – Project Deliverable 1, UKPN, 2017, <https://innovation.ukpowernetworks.co.uk/wp-content/uploads/2019/05/Active-Response-Project-Deliverable-1-Report.pdf> [Accessed: 13-Sep-2019].
- [10] SP Energy Networks, 400kV Dynamic Cable Rating Retrofit Project utilising RPMA Communications Technology, Jul 2019,  
<https://www.smarternetworks.org/project/niaspen0044/documents> [Accessed: 13-Sep-2019].
- [11] SP Energy Networks, Enabling Monitoring and Control of Underground Assets, Jun 2019  
<https://www.smarternetworks.org/project/niaspen0043> [Accessed: 13-Sep-2019].
- [12] Light reading, Vodafone Brings NB-IoT to UK, Starts Trial With Scottish Power,  
<https://www.lightreading.com/iot/nb-iot/vodafone-brings-nb-iot-to-uk-starts-trial-with-scottish-power/d/d-id/746377> [Accessed: 13-Sep-2019].
- [13] LinkLabs, NB-IoT vs. LoRa vs. Sigfox, June 2018, <https://www.link-labs.com/blog/nb-iot-vs-lora-vs-sigfox> [Accessed: 13-Sep-2019].
- [14] Description and analysis of IEC 104 Protocol, technical report, P. Matousek, Faculty of Information Technology, Brno University of Technology ,Brno, Czech Republic , Dec 2017,  
<https://www.fit.vutbr.cz/research/pubs/tr.en?file=%2Fpub%2F11570%2FTR-IEC104.pdf&id=11570>
- [15] MicroSCADA Pro SYS600 9.4 IEC 60870-5-104 Master Protocol, ABB, 2016,.  
[https://library.e.abb.com/public/f68df90dfec441f38dcad54442eacacf/SYS600\\_IEC%2060870-5-104%20Master%20Protocol\\_758109\\_ENc.pdf](https://library.e.abb.com/public/f68df90dfec441f38dcad54442eacacf/SYS600_IEC%2060870-5-104%20Master%20Protocol_758109_ENc.pdf) [Accessed: 13-Sep-2019].
- [16] DNP3 Configuration/Interoperability Guide for RTU32 DNP3 Slave, Brodersen, August 2014,  
<http://brodersen.com/wordpress/wp-content/uploads/RTU32-DNP3-Slave-Device-Profile.pdf>
- [17] 650 series DNP3 Communication Protocol Manual, ABB, 2011, [Accessed: 13-Sep-2019].  
[https://library.e.abb.com/public/5b0552a1511e3d9ac125783a004549d7/1MRK511241-UEN\\_-\\_en\\_Communication\\_protocol\\_manual\\_\\_DNP\\_\\_650\\_series\\_\\_IEC.pdf](https://library.e.abb.com/public/5b0552a1511e3d9ac125783a004549d7/1MRK511241-UEN_-_en_Communication_protocol_manual__DNP__650_series__IEC.pdf) [Accessed: 23-Sep-2019].



- [18] 650 series ANSI DNP3 Communication Protocol Manual, ABB, 2012, [https://library.e.abb.com/public/2ef28ecbeaf69cd0c1257a690042c786/1MRK511257-UUS\\_A\\_en\\_Communication\\_protocol\\_manual\\_\\_DNP\\_\\_650\\_series\\_1.2\\_\\_ANSI.pdf](https://library.e.abb.com/public/2ef28ecbeaf69cd0c1257a690042c786/1MRK511257-UUS_A_en_Communication_protocol_manual__DNP__650_series_1.2__ANSI.pdf) [Accessed: 23-Sep-2019].
- [19] CIMCON Lighting, Power Line Communications vs. Radio Frequency Communications, Sep 2018, <https://www.cimconlighting.com/blog/power-line-communications-vs.-radio-frequency-communications> [Accessed: 23-Sep-2019].
- [20] Devolo, technology for powerline communication, <https://www.devolo.com/smart-grid/plc-technology> [Accessed: 23-Sep-2019].
- [21] Bernacki, K., Wybrańczyk, D., Zygmanski, M., Latko, A., Michalak, J. and Rymarski, Z., 2019. Disturbance and Signal Filter for Power Line Communication. Electronics, 8(4), p.378.
- [22] Zhu, Y.; Wu, J.; Wang, R.; Lin, Z.; He, X. Embedding Power Line Communication in Photovoltaic Optimizer by Modulating Data in Power Control Loop. IEEE Trans. Ind. Electron. 2019, 66, 3948–3958.
- [23] PPC, Smart Grid Projects, <https://www.ppc-ag.com/projects/smart-grid-projects/> [Accessed: 23-Sep-2019].
- [24] Engerati network, Power line communication is ready for the smart grid today, June 2016 <https://www.engerati.com/article/power-line-communication-ready-smart-grid-today> [Accessed: 23-Sep-2019].
- [25] J. Haas, D. Lauk, T. Schaub, and A. Wirtz, “White paper: Introducing the power of PLC.”
- [26] ENA Engineering Recommendation G91 Issue 1 (2012) - Substation Black Start Resilience.
- [27] ENA Energy Delivery Systems – Cyber Security Procurement Guidance, 2016 <http://www.energynetworks.org/assets/files/BEIS%20ENA%20Cyber%20Security%20Procurement%20Language%20Guidance.pdf> [Accessed: 28-Sep-2019].



## 10 Glossary of Terms

| Abbreviation  | Definition                                       |
|---------------|--|
| <b>APN</b>    | Access Point Name                                |
| <b>BGAN</b>   | Broadband Global Area Networks                   |
| <b>BPL</b>    | Broadband over Power line                        |
| <b>ESP</b>    | Encapsulating Security Payload                   |
| <b>FTSP</b>   | File Transfer Protocol Secure                    |
| <b>GPRS</b>   | General Packet Radio Services                    |
| <b>HTTPS</b>  | Hypertext Transfer Protocol Secure               |
| <b>ICMP</b>   | Internet Control Message Protocol                |
| <b>IPsec</b>  | Internet protocol Security                       |
| <b>LPWAN</b>  | Low Power Wireless Access Networks               |
| <b>LTE</b>    | Long Term Evolution                              |
| <b>NB-IoT</b> | Narrow Band Internet of Things                   |
| <b>OFDMA</b>  | Orthogonal Frequency Division Multiplexing       |
| <b>PLC</b>    | Power Line Communication                         |
| <b>RPMA</b>   | Random Phase Multiple Access                     |
| <b>SCADA</b>  | Supervisory Control and Data Acquisition         |
| <b>SMTPS</b>  | Simple Mail Transfer Protocol Secure             |
| <b>SNMP</b>   | Simple Network Management Protocol               |
| <b>TACACS</b> | Terminal Access Controller Access Control System |
| <b>TCP</b>    | Transmission Control protocol                    |
| <b>TLS</b>    | Transport Layer Protocol                         |
| <b>VPN</b>    | Virtual Private Network                          |
| <b>VPN</b>    | Virtual Private Network                          |
| <b>WAN</b>    | Wide Area Networks                               |



## 11 Appendix: IEC 104 and DNP3 Message Size

The results obtained from the PNDC testing shows that the message size of the IEC 104 vary based on the configuration of the IEC 104 protocol. Figure 4 shows the exchange messages between the client RTU and the server to carry 2 analogue measurements from the field device via a 104 IEC message with 286 bytes of size.

| Source       | Destination  | Protocol | Length | Info  |
|--------------|--------------|----------|--------|---|
| 10.10.40.151 | 10.12.40.50  | 104apci  | 64     | <- S (53)   |
| 10.12.40.50  | 10.10.40.151 | TCP      | 60     | 2404 → 59831 [ACK] Seq=1 Ack=7 Win=8186 Len=0     |
| 10.12.40.50  | 10.10.40.151 | 104asdu  | 98     | -> I (53,1) ASDU=3 M_ME_NC_1 Spont IOA[4]=304,... |
| 10.10.40.151 | 10.12.40.50  | TCP      | 64     | 59831 → 2404 [ACK] Seq=7 Ack=45 Win=8148 Len=0    |

**Figure 4 IEC 60870-5-104 packets exchange captured by Wireshark for 2 analogues**

In the calculations, it is assumed that the analogue messages are sent one at a time (i.e. separate packets with no batching of data, which reflects a worst case scenario). The following table shows a list of the IEC 104 message size based on the analogues measurements included.

**Table 5 Secure IEC message size per number of analogues**

| Number of analogues | Secure IEC 104 Message size in bytes (without timestamp) | Secure IEC 104 Message size in bytes (with timestamp) |
|---------------------|--|---|
| 1                   | 262  | 265   |
| 2                   | 286  | 289   |
| 3                   | 304  | 307   |
| 4                   | 326  | 329   |

The complete message size of the IEC 104 (i.e. including security) for one digital point is 228 Bytes without timestamp and 231 bytes with timestamp, further details could be found in [14].

For the DNP 3, the calculated message size has been taken from previous PNDC testing. Unsolicited Digital message exchange 214 Bytes. The message size for one analogue measurement is 268 Byte (assuming unbatched reporting).

If batching is adopted, the message size will be reduce, for example:

- Analogue (25 points x 16bit) = 324 bytes,
- Class 1 poll of (6 analogues , 2 digitals) = 288 bytes

### IP sec packet overhead

Figure 5 shows how the IP security packets appears inside the VPN (i.e encapsulating in ESP format). The screenshots have been taken from a PNDC testing project of a full-secured IP RTU (i.e. ABB 500 RTU supports secure authentications and it is compliant with the IEC 62351). It can be seen that there is an overhead of 58-66 bytes for each packet entering the VPN (the packet will appear in ESP format).



| Protocol | Length | Protocol | Length | Info     |
|----------|--------|----------|--------|----------|
| TCP      | 60     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| 104apci  | 1404   | ESP      |        | 118 ESP  |
| 104apci  | 1156   | ESP      |        | 150 ESP  |
| TCP      | 60     | ESP      |        | 1478 ESP |
| TCP      | 60     | ESP      |        | 1222 ESP |
| TCP      | 60     | ESP      |        | 118 ESP  |
| 104apci  | 1192   | ESP      |        | 118 ESP  |
| TLSv1.2  | 85     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| TLSv1.2  | 139    | ESP      |        | 1254 ESP |
| TCP      | 60     | ESP      |        | 150 ESP  |
| 104apci  | 89     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 214 ESP  |
| 104apci  | 99     | ESP      |        | 118 ESP  |
| 104apci  | 189    | ESP      |        | 166 ESP  |
| 104apci  | 239    | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 166 ESP  |
| TCP      | 99     | ESP      |        | 262 ESP  |
| TCP      | 60     | ESP      |        | 310 ESP  |
| 104asdu  | 188    | ESP      |        | 118 ESP  |
| 104apci  | 99     | ESP      |        | 166 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 262 ESP  |
| TLSv1.2  | 85     | ESP      |        | 166 ESP  |
| TLSv1.2  | 108    | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 150 ESP  |
| TLSv1.2  | 85     | ESP      |        | 150 ESP  |
| TLSv1.2  | 108    | ESP      |        | 182 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| TCP      | 60     | ESP      |        | 118 ESP  |
| TLSv1.2  | 85     | ESP      |        | 150 ESP  |
| TLSv1.2  | 139    | ESP      |        | 150 ESP  |
| TCP      | 60     | ESP      |        | 150 ESP  |
| TLSv1.2  | 85     | ESP      |        | 150 ESP  |
| TLSv1.2  | 108    | ESP      |        | 182 ESP  |
| TLSv1.2  | 85     | ESP      |        | 118 ESP  |
| TLSv1.2  | 108    | ESP      |        |          |

Figure 5 IP sec packets inside the VPN

Remote access can be a bandwidth-hungry application, but this is for a short time and only for the duration of any required reconfigurations and maintenance of SCS field components (e.g. LCS). Figure 6 and **Error! Reference source not found.** illustrates the intensive bandwidth consumed by remote access.



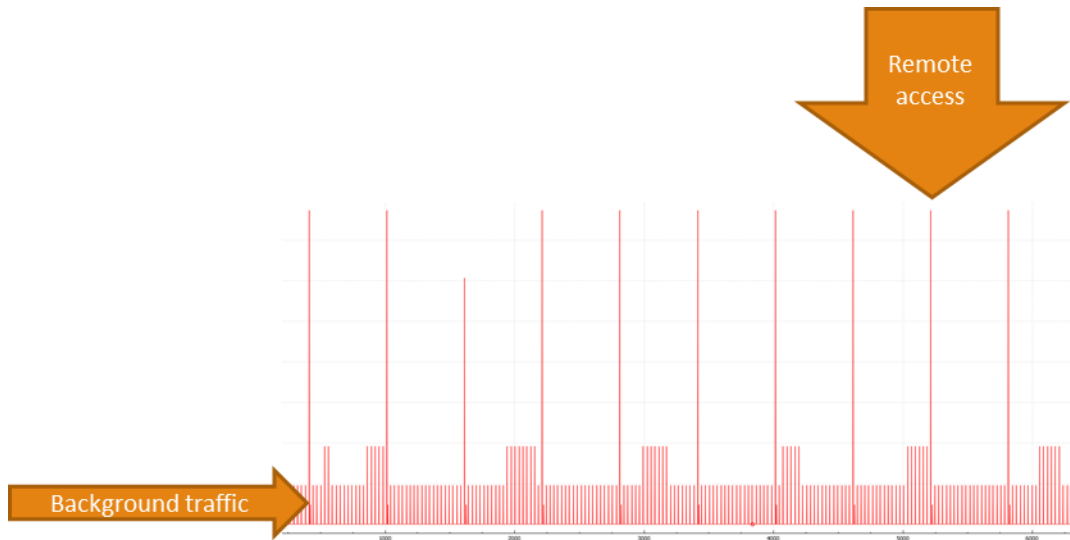


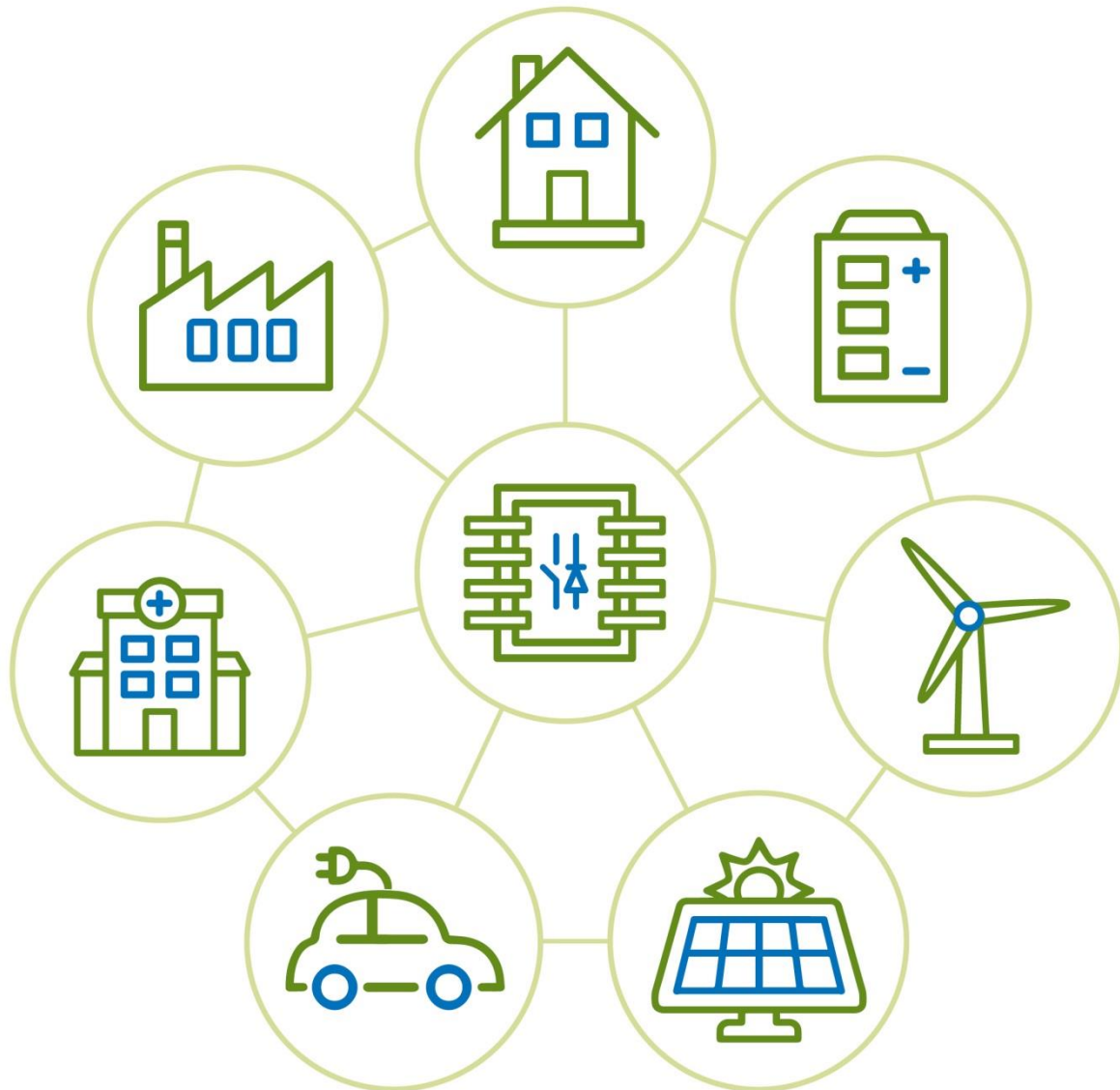
Figure 6 The effect of Remote access on bandwidth

|            |              |              |         |  |
|------------|--------------|--------------|---------|--|
| 249.047384 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56326 → 443 [FIN, ACK] Seq=1146 Ack=751 Win=65400 Len=0   |
| 249.048020 | 10.12.40.50  | 10.10.40.152 | TCP     | 60 443 → 56326 [ACK] Seq=751 Ack=1147 Win=8192 Len=0   |
| 249.413210 | 10.12.40.50  | 10.10.40.105 | SNMP    | 99 get-request 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.3.0   |
| 249.414929 | 10.10.40.105 | 10.12.40.50  | ICMP    | 127 Destination unreachable (Port unreachable)   |
| 250.408810 | 10.10.40.151 | 10.12.40.50  | 104apci | 64 <- 5 (168)  |
| 250.409422 | 10.12.40.50  | 10.10.40.151 | TCP     | 60 2404 → 61723 [ACK] Seq=1057 Ack=151 Win=8186 Len=0  |
| 250.412241 | 10.12.40.50  | 10.10.40.151 | 104asdu | 98 -> I (168,1) ASDU=3 M_ME_NC_1 Spont IOA[4]=304,...  |
| 250.413877 | 10.10.40.151 | 10.12.40.50  | TCP     | 64 61723 → 2404 [ACK] Seq=151 Ack=1101 Win=8148 Len=0  |
| 251.496021 | 10.10.40.152 | 10.12.40.50  | TCP     | 66 56327 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1  |
| 251.497645 | 10.12.40.50  | 10.10.40.152 | TCP     | 62 443 → 56327 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1350 WS=1   |
| 251.499188 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1 Ack=1 Win=66148 Len=0   |
| 251.500347 | 10.10.40.152 | 10.12.40.50  | TLSv1.2 | 571 Client Hello   |
| 251.500986 | 10.12.40.50  | 10.10.40.152 | TCP     | 60 443 → 56327 [ACK] Seq=1 Ack=518 Win=7675 Len=0  |
| 251.512126 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 191 Server Hello, Change Cipher Spec, Encrypted Handshake Message  |
| 251.514113 | 10.10.40.152 | 10.12.40.50  | TLSv1.2 | 105 Change Cipher Spec, Encrypted Handshake Message  |
| 251.514741 | 10.12.40.50  | 10.10.40.152 | TCP     | 60 443 → 56327 [ACK] Seq=138 Ack=569 Win=8141 Len=0  |
| 251.515140 | 10.10.40.152 | 10.12.40.50  | TLSv1.2 | 764 Application Data   |
| 251.516005 | 10.12.40.50  | 10.10.40.152 | TCP     | 60 443 → 56327 [ACK] Seq=138 Ack=1279 Win=7431 Len=0   |
| 251.533433 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 100 Application Data   |
| 251.540068 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 1404 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, |
| 251.542178 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=1534 Win=66148 Len=0   |
| 251.542739 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 511 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data,  |
| 251.549804 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 1404 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, |
| 251.551684 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=3341 Win=66148 Len=0   |
| 251.552257 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 269 Application Data, Application Data, Application Data, Application Data                                       |
| 251.561288 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 1404 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, |
| 251.563231 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=4906 Win=66148 Len=0   |
| 251.563783 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 308 Application Data, Application Data, Application Data, Application Data, Application Data                     |
| 251.572185 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 1404 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, |
| 251.574231 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=6510 Win=66148 Len=0   |
| 251.574791 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 376 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data,  |
| 251.582469 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 1404 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, |
| 251.584407 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=8182 Win=66148 Len=0   |
| 251.584941 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 328 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data,  |
| 251.588499 | 10.12.40.50  | 10.10.40.152 | TLSv1.2 | 621 Application Data, Application Data, Application Data, Application Data, Application Data, Application Data,  |
| 251.590099 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [ACK] Seq=1279 Ack=9024 Win=65308 Len=0   |
| 251.591084 | 10.10.40.152 | 10.12.40.50  | TCP     | 64 56327 → 443 [FIN, ACK] Seq=1279 Ack=9024 Win=65308 Len=0  |
| 251.591743 | 10.12.40.50  | 10.10.40.152 | TCP     | 60 443 → 56327 [ACK] Seq=9024 Ack=1280 Win=8192 Len=0  |

Figure 7 Captured data from Wireshark during remote access activation















-  [www.spenergynetworks.co.uk/](http://www.spenergynetworks.co.uk/)
-  [facebook.com/SPEnergyNetworks/](https://facebook.com/SPEnergyNetworks/)
-  [twitter.com/SPEnergyNetwork](https://twitter.com/SPEnergyNetwork)
-  [<Insert Email>](#)

