Vulnerability considerations for power line communication's supervisory control and data acquisition

Ali Hosseinpournajarkolaei*

School of Architecture, Computing and Engineering,
University of East London,
Docklands Campus,
4-6 University Way, E16 2RD, London, UK
E-mail: Najarkolaei@ieee.org
*Corresponding author

Hamid Jahankhani and Amin Hosseinian-Far

Williams College, Duncan House,
High Street Stratford,
E15 2JB, London, UK
E-mail: Hamid@williamscollege.co.uk
E-mail: Ahosseinianfar@glos.ac.uk

Abstract: Due to the increasing importance of communication networking, the power line (PL) channel has been considered as a good candidate for the communication medium. Power line communications (PLC) term stands for the technologies for the data communication over the electrical power supply network. The PL channels were not designed to transmit high speed data; therefore, they exhibit hostile medium for communication signal transmission. There are many factors such as noises, attenuation, distance, etc. affecting the quality of the transmission over PL channels. This paper presents PL model in the first sections of the work. Then it covers the security assessment of the PL system in the supervisory control and data acquisition (SCADA) context.

Keywords: power line communications; PLC; SCADA security; smart metering; system of systems; SoS; narrowband technology.

Reference to this paper should be made as follows: Hosseinpournajarkolaei, A., Jahankhani, H. and Hosseinian-Far, A. (2014) 'Vulnerability considerations for power line communication's supervisory control and data acquisition', *Int. J. Electronic Security and Digital Forensics*, Vol. 6, No. 2, pp.104–114.

Biographical notes: Ali Hosseinpournajarkolaei is a final year doctoral student at University of East London. He gained his MSc in Electrical and Electronic Engineering subject area from City University London following his Bachelor's degree in the same subject from UEL. As part of his research, he is investigating the power line communications and the technologies for data communication over the electrical power supply. He has been the author and co-author of a number of publications in his field and holds associate fellowship of higher education academy. He has also worked for Docklands Light Railway as Engineering Technician and for University of East London as a Visiting Lecturer.

Hamid Jahankhani recently joined Williams College as the Director of Research and Consultancy Development. He gained his PhD from the Queen Mary College, University of London. In 2000, he moved to the University of East London to become the first Professor of Information Security and Cyber Criminology at the university in 2010. Over the last decade he has been developing and leading portfolio development at both University of East London (UEL) and Middlesex. His principal research area for a number of years has been in the field of information security and digital forensics. He is the Editor-in-Chief of the *International Journal of Electronic Security and Digital Forensics* published by Inderscience, http://www.inderscience.com/ijesdf and General Chair of the annual International Conference on Global Security, Safety and Sustainability (ICGS3). He has edited and contributed to over ten books and has over 100 conference and journal publications.

Amin Hosseinian-Far is currently the Assistant Director of Studies of School of Business and IT at Williams College in London. He gained his PhD from University of East London after researching a multidisciplinary domain of sustainability. Prior to his PhD, he obtained an MSc in Satellite Communication and Space Systems from University of Sussex. As a multidisciplinary researcher, he has published widely in areas including, but not limited to, probabilistic inference and influence diagrams, KMS, systems' sustainability and SD, environmental financial modelling & climate change, and smart grids.

This paper is a revised and expanded version of a paper entitled 'Vulnerability considerations for power line communication's (PLC) supervisory control and data acquisition' presented at 9th International Conference on Global Security, Safety and Sustainability, Williams College London, 4–6 December 2013.

1 Introduction

Recently, there has been a big interest in utilising the PL channel for communication due to its potential to telecommunication users (Anatory et al., 2008). Power line communications (PLC) is using an existing power line (PL) system, i.e., this is great saving in cost and time. The general idea of PLC system is to modulate a radio signal with data and transmit it through PL channels in a different band of frequencies which are not used for supplying electricity. PLC technology can be divided into two categories; the narrowband and broadband communication. The frequency range of up to 150 kHz is for narrowband with the theoretical bit rate of kilobits (up to 2 Mbit/s). The frequency range for broadband technology is between 1.61–30 MHz with theoretical bit rate up to 200 Mbit/s (Agrawal et al., 2011). The used frequencies and the modulation scheme are two main factors which have a significant influence on the efficiency of the system and also the speed of the PLC service. The best suitable modulation technique for PLC system is an orthogonal frequency division multiplexing (OFDM) (Agrawal et al., 2011). OFDM is a multi-carrier modulation scheme in which a single high rate data-stream is divided into multiple low rate data-streams. It is also modulated by using sub-carriers which are orthogonal to each other. The main advantages of OFDM are its efficient spectral usage by allowing overlapping in the frequency domain (reducing the bandwidth

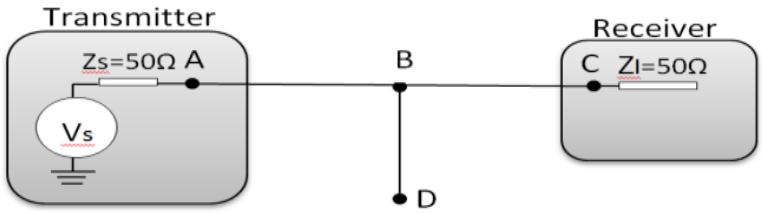
by squeezing subcarriers until they overlap with each other) and multi-path delay spread tolerance (Agrawal et al., 2011).

In this paper, in Section 2, the PL channel will be briefly introduced. Moreover, simulations on the PLC model are represented. In Section 3, PLC noise is outlined. And Section 4 would present the security assessment of the PL system in the supervisory control and data acquisition (SCADA) context.

2 PL channels

The PL networks usually classified as high-voltage (100 kV), medium-voltage (1–100 kV) and low-voltage (110–380 V). High voltages are not suitable for data transmission, therefore conventional fibre optics or wireless radio-link is used for transmission of this data over the existing PLs with repeaters used in MV networks to mitigate the effects of noise interference. Couplers then can be used to by-pass transformers when the power is lowered from MV to LV (Industry of Canada, 2012). Power grid consists of cascaded cables of diverse line lengths with a various number of branches of different line lengths and terminal loads. Switching on/off electrical equipment's change the terminal load, i.e., it results changing the frequency response of the network. The effect of changes in the power distribution system topologies over the PL channels are investigated in Hosseinpournajarkolaei and Hosseinian-Far (2012). A simple topology for such a power distribution system was used to investigate the effect of variation in direct length, branch load, branch lengths and different number of paths.

Figure 1 A simple LV PL network configuration



Source: Hosseinpournajarkolaei et al. (2012a)

The multipath model is a widely used model for investigating the data transmission over PL networks and is given below:

$$H(f) = \sum_{i=1}^{N} g_i . e^{-(a0+a1f^k)di} . e^{-j2\pi f d_i / V_p} \tag{1}$$

where $H(f)$ is the frequency response of the channel, g_i the weighting factor, d_i the length of the data transmission path for various path numbers and N is the total number of paths.

As it can be observed from the results in Hosseinpournajarkolaei and Hosseinian-Far (2012), variation in the direct line length from the transmitter results no multi-path fading as the channel response is a linear function of the frequency. The receiver can therefore recover the data transmitted using a single-carrier modulation transmission.

However, the multi-path behaviour in Hosseinpournajarkolaei et al. (2012b) indicates that multi-carrier transmission would be suitable for data transmission over the PL channel in case of varying the length AC with one branch. The increase in the direct line length AC reduces the channel bandwidth and its effect on frequency response is similar to the no-branch case, the difference being that the frequency notches are superimposed on the frequency response.

From the simulation results in Hosseinpournajarkolaei et al. (2012b), it is observed that increasing the branch length BD increases the PL attenuation which is especially noticeable in higher frequencies.

In case of multipath with different numbers of paths, from the simulation results for number of path 4 and 10 shown in Figures 2 and 3, it can be observed that the position of notches do not change. But as the number of paths increases from 4 to 10, the attenuations of notched points and signal distortion tend to increase.

Figure 2 Multipath channel model with number of path = 4 (see online version for colours)

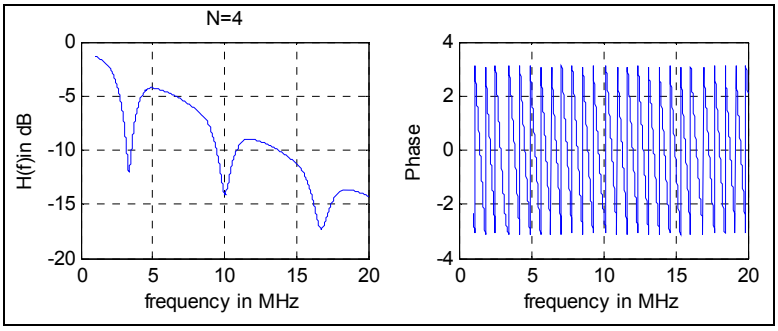
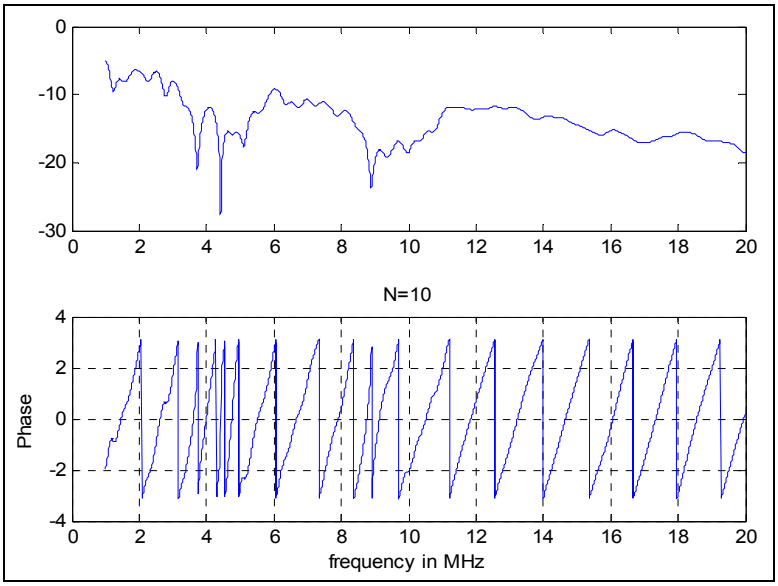


Figure 3 Multipath channel model with number of path = 10 (see online version for colours)



2.1 Narrowband technology

The narrowband PLC are normally used in automation systems. The automation systems based on PLC technology are implemented with no any additional insulation of communication networks which results substantially reduction in costs for the installation and realisation of the new network within the existing buildings. The automation system in this system can be used in:

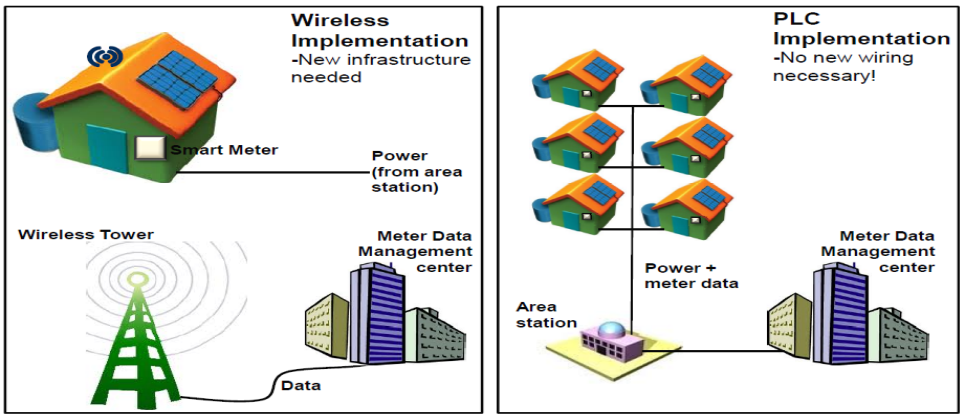
1 central control of various home system such as controlling doors/windows

2 controlling connected devices to the internal wiring such as lighting, air conditions

3 the security function, sensor control (Hosseinpournajarkolaei et al., 2012b).

Another application for narrowband technology is called smart metering. The smart metre system includes metres at the consumer site, communication medium between a service provider and consumer, such as a gas, an electric, or water, and data management systems in service provider site that make the information available. The smart metre transmits the collected data through PLC to a metre data management system for data analysis and billing (Consumer Focus UK GOV, 2013).

Figure 4 The basic smart metering system (see online version for colours)



Source: Fernandes and Dave (2011)

If you get a smart metre in your house/building you should get the following benefits:

- Accurate bills: the smart metre sends information to your energy provider on how much energy you have exactly used, so no more estimated bills.
- Could help to save money: by knowing what you are using, and having an idea of which appliances use the most energy, you may be able to reduce your energy usage and save money.
- A standard in-home energy display: has a small screen which shows your energy usage at any one time with no any additional cost.

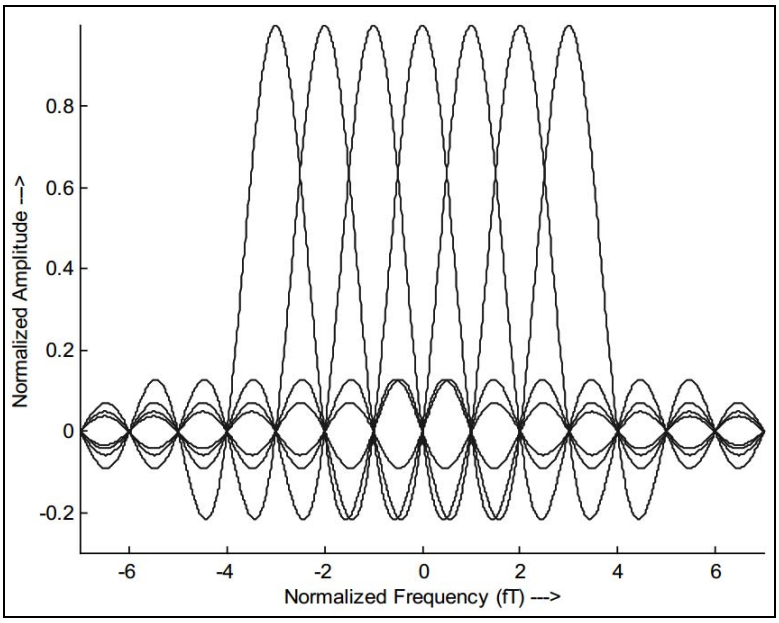
- Reduced theft of energy: the energy theft detection is more easily therefore it can be easily prevented, meaning you will not have to pay for stolen energy (Consumer Focus UK GOV, 2013).

2.2 Orthogonal frequency division multiplexing

Nowadays, in order to achieve higher data rates in communication system OFDM which is a multi-carrier modulation technique is being used. In OFDM scheme, data will be transmitted by dividing a single wideband stream into several smaller/narrowband parallel bit streams. Thus the modulated sub-carrier narrowband streams are summed to form an OFDM signal.

The narrowband channels are orthogonal vis-à-vis each other, and are transmitted simultaneously which results an increase in the symbol duration proportionately, and reduction on the effects of inter-symbol interference (ISI) which are induced by multipath Rayleigh-faded environments (Agrawal et al., 2011).

Figure 5 Basic OFDM system architecture



The study on the effect of number of branches in PL networks indicated the possibility of degradation of the channel performance. Therefore, in order to enhance the network stability and performance, the multi-carrier modulation techniques such as OFDM can be considered (Hosseinpournajarkolaei et al., 2012b).

3 Different types of noise on PLC

In order to design high speed data transmission over PL networks details knowledge of channel properties noise are required. Due to the signal distortion, cable losses and multipath propagation the noise is known as the most crucial factor effecting data communication over PL systems.

Normally, in LV PL networks, the source of the noise can be internal (inside the network) or external (outside the network). Overall, in BPL channels, the additive noise normally classified into five different classes;

1 Coloured background noise: has very low power spectral density (PSD) which also varies with the variation in frequency and resulted by summation of number of different noise sources with very low power.

2 Narrow band noise: normally has sinusoidal signals with modulated amplitudes and caused by ingress of broadcast station in short wave broadcast bands and the medium.

3 Periodic impulsive noise asynchronous to the mains frequency: have a repetition rate between 50 kHz to 200 KHz in most cases and normally resulted by switching power supplies.

4 Periodic impulsive noise synchronous to the mains frequency: with the repetition rate of 50 Hz or 100 Hz and are synchronous to the mains cycle and normally created by the power supplies operating synchronously with the mains cycle.

5 Asynchronous impulsive noise: which sometimes has a very high PSD value of more than 50 dB above the background noise and is normally caused by switching transients in the network (Chariag et al., 2011).

3.1 MATLAB Simulink model of different types of noise on PLC system

- Asynchronous impulsive noise: to simulate the noise produced by turning on/off the electrical devices the scheme in Figure 6 was used. The maximal delayed used at delay block is 100 the M-ary of random integer generator was set to 100 with sample time 1/1,000.
- Periodic impulsive noise: to simulate noise like that produced by switched power supplies, the scheme showed by Figure 7 was used.
- Synchronous impulsive noise: as it can be seen in Figure 8, by adding a spectral colouring to the white noise together with a periodical rectangular signals synchronous impulsive noise can be modelled. This type of noise is caused by thermistors in light dimmers and copiers.

The final model of applying different types of noises on PLC has been created with PL channel together with white Gaussian noise (Figure 9).

Figure 6 Asynchronous impulsive noise

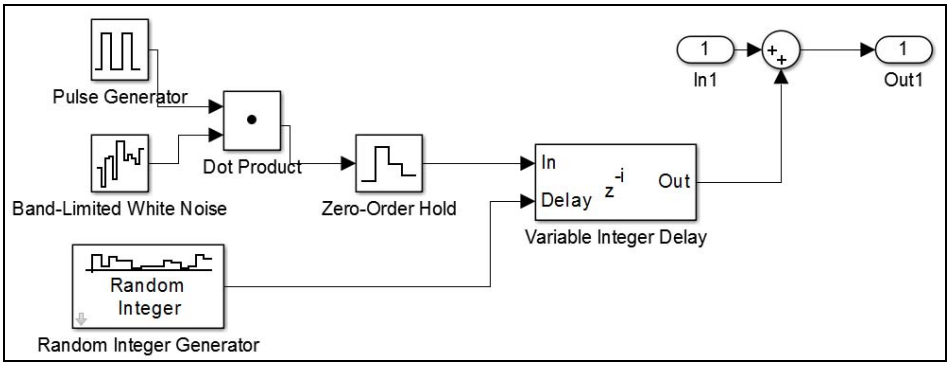


Figure 7 Periodic impulsive noise (see online version for colours)

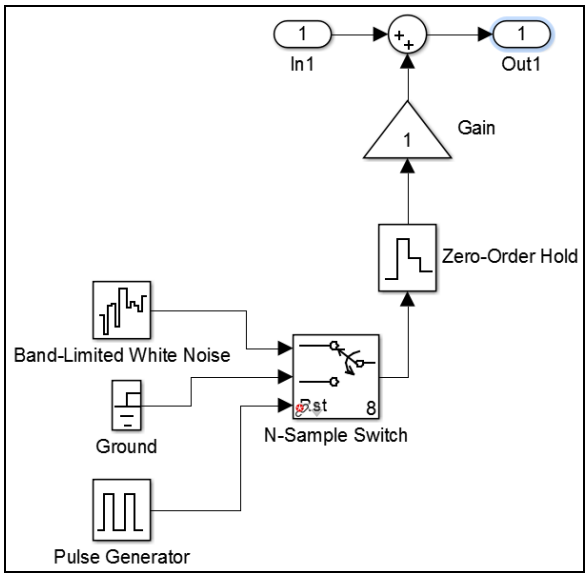


Figure 8 Periodic rectangular signal

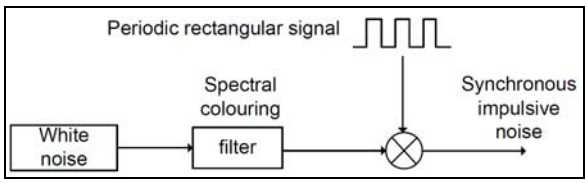
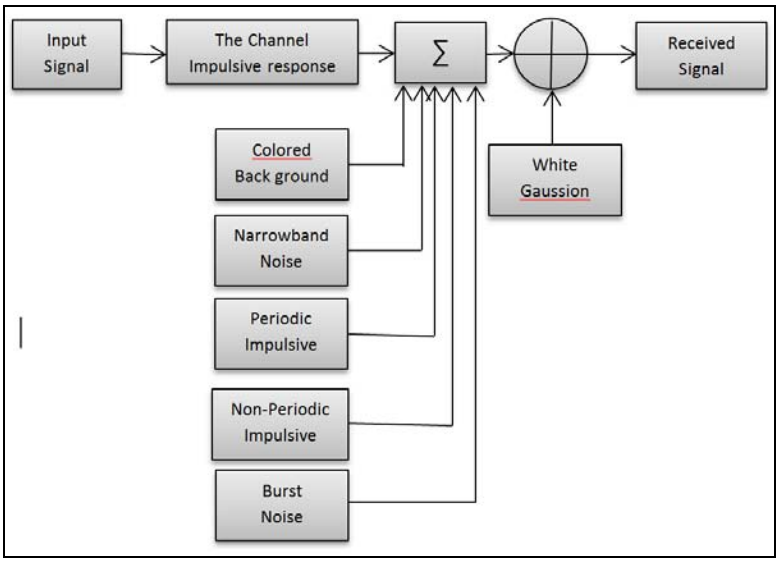


Figure 9 PLC noise together with Gaussian noise



The PL channel model is modelled as a digital filter together with the source of interferences/noises. The PLC 16 QAM model with OFDM modulation which enables to simulate better data communication over PLs.

4 Vulnerability considerations for the PLC SCADA

SCADA is a combination of telemetry and data retrieval system and has existed long time before control engineering (Robles et al., 2008). Smart grids where the narrow band PLC is implemented are also vulnerable to threats associated with similar infrastructural systems. Ericsson (2010) points out that the threat SCADA arises in the access points (Figure 10) available in them. Moreover, the complexity the SCADA makes it difficult to consider the system of systems' (SoS) frameworks for the security assessment. Knowing that the PLC model introduced above would be also exposed to security threats and vulnerabilities when it comes to application.

Using Ericsson's (2010) domain categorisation of SCADA, the following domain's securities are considered for the above mentioned PLC model:

a Public, supplier, maintainer domain

One of the main security considerations in this domain would be provision of appropriate encryption/decryption technique in order to avoid public access to the data transferred via PLC. Furthermore, the maintainer domain should be contracted in a way which avoids future potential eavesdropping scenarios by third parties.

b Power plant domain

Injection from the power plant can be performed in various ways and the vulnerabilities and risks would depend on the system involved as the medium. Therefore, security consideration should be presented for each individual SCADA.

c Substation domain

Distance between branches and securities involved in losing data due to lack of repeater on the way should be considered in domain. A longitudinal analysis of potential extensions to the PLC, to the distance between branches and any probable amendments should be considered before implementation of the smart grid.

d Telecommunication domain

Securing gateways in the smart grid is an area to be considered for implementation. Use of repeaters, electrical physical structures and the bridges used may also lead to physical security threat. Data does not pass into transformer and therefore the bridges are used. The physical bridge outside the transformed is subject to the main access point for eavesdropping.

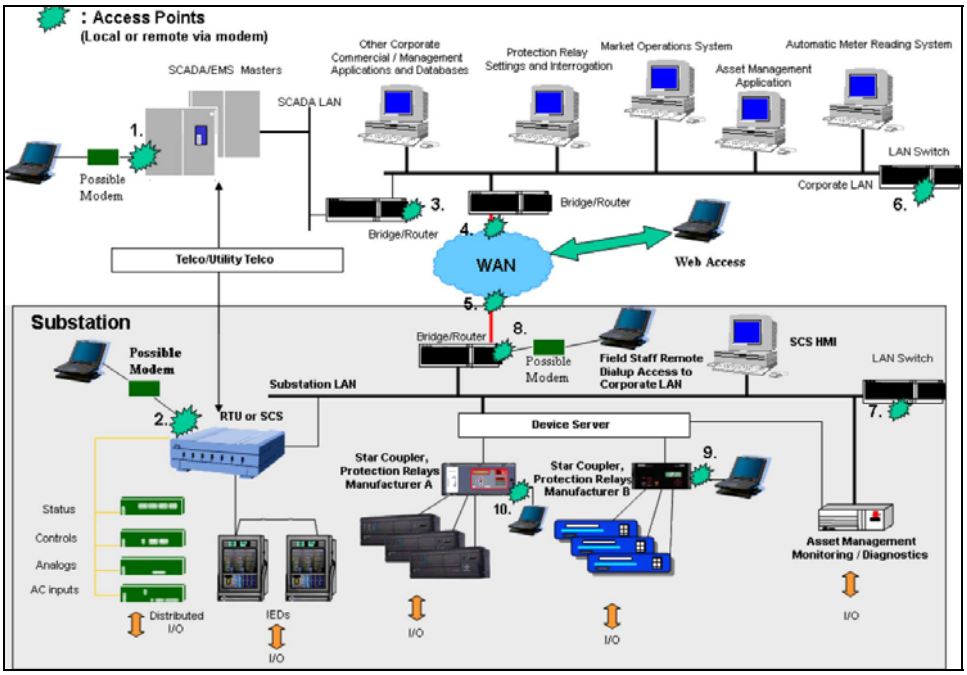
e Real-time operation domain

Noise as a result of increased attenuation which then leads to poor data is a major threat in the real-time operation domain. However, the physical unintentional threats such as systems' failure should also be considered.

f Corporate IT domain

Failure in the software used for the control system of the smart grid is susceptible to damage. Similar to any other information system, software is likely to be influenced by poor algorithm or external viruses.

Figure 10 Access points to SCADA system (see online version for colours)



Source: Ericsson (2010)

5 Conclusions

To conclude, this major project gives the detail knowledge of a current key issue in the field of PLC. Various effects on PLC (such a different number of paths) have been investigated. Different types of noise on PLC were modelled and simulated theoretically; and the threats and risks associated with the practical implementation of smart grid using the PLC is analysed. Domain classification is used for breaking down different facets for consideration. This would simplify the complexities and integrations involved in smart grid.

References

Agrawal, D.G., Paliwal, R.K. and Subramanium, P. (2011) 'Effect of turbo coding on OFDM transmission to improve BER', *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, Vol. 2, No. 1, pp.94–102.

Anatory, J., Theethayi, N., Kissaka, M.M. and Mvungi, N. (2008) 'Broadband powerline communications: performance analysis', *World Academy of Science, Engineering and Technology*.

Chariag, D., Guezgouz, Y., Raingeaud, J. and Lebunetel, C. (2011) 'Channel modeling and periodic impulsive noise analysis in indoor power line', in *IEEE International Symposium on Power Line Communications and its Applications*.

Consumer Focus UK GOV (2013) 'Smart meters – what are they and how can I find out more?', *Consumer Focus* [online] http://www.consumerfocus.org.uk/get-advice/energy/smart-meters-what-are-they-and-how-can-i-find-out-more/benefits-and-disadvantages-of-smart-meters (accessed 29 August 2013).

Ericsson, G.N. (2010) 'Cyber security and power system communication – essential parts of a smart grid infrastructure', *IEEE Transactions on Power Delivery*, Vol. 25, No. 3, pp.1501–1507.

Fernandes, A.D.L. and Dave, P. (2011) 'Power line communication in energy markets', *CYPRESS*, San Jose, USA.

Hosseinpournajarkolaei, A. and Hosseinian-Far, A. (2012) 'Channel characterization for broadband power line communication system', in *6th Sastech Intl. Conference*, KL Malaysia.

Hosseinpournajarkolaei, A., Lota, J. and Hosney, W. (2012a) *Challenges Facing the Design of Broadband Power Line Communication (BPLC) Systems*, in UPEC-Brunel University of London, London.

Hosseinpournajarkolaei, A., Lota, J. and Hosney, W. (2012b) *Design of Broadband Power Line Communication System for UK Power Line System*, in University of East London, London.

Industry of Canada (2012) *Spectrum Management and Telecommunications* [online] https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08434.html (accessed 2013).

Robles, R.J., Choi, M-K., Cho, E-S., Kim, S-S., Park, G-C. and Yeo, S-S. (2008) 'Vulnerabilities in SCADA and critical infrastructure systems', *International Journal of Future Generation Communication and Networking*, Vol. 1, No. 1, pp.99–105.