Indonesian Journal of Electrical Engineering and Computer Science
Vol. 9, No. 3, March 2018, pp. 616~618
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i3.pp616-618

Protection of Sequence and Communication Technology Equipment Using Smart Grid Application

Archenaa J[1], E.A. Mary Anitha[2]
[1]Department of Information Technology, AMET University, Chennai
[2]Department of Information Technology, S.A. Engineering College, Chennai

Article Info

Article history:

Received Nov 29, 2017
Revised Feb 8, 2018
Accepted Feb 23, 2018

Keywords:

Smart grid
Protection sequence

ABSTRACT

This paper investigates the merger of energy utility circuits with that of the data and correspondence innovation (ICT) gear under the keen matrix and the security suggestions that this postures, and figures out what is the most extreme voltage that ICT hardware, composed as per IEC 62368-1 can specifically get to control framework circuits. The coming of the keen lattice, the modernization of the power framework utilizing current data and correspondence innovation methods, alongside the expansion of electric vehicle frameworks to the matrix, guarantees to change the business in uncommon manners. In this paper will be utilized as a part of this paper for deciding the level of security of ICT gear must be built to keeping in mind the end goal to be conveyed in higher-voltage application.

Corresponding Author:

Archenaa J,
Department of Information Technology,
AMET University, Chennai,
India.

1. INTRODUCTION

The brilliant matrix, now considered piece of the Internet of Things (IoT) can be seen as the merger of the once in the past isolated power, media transmission, data innovation, and car businesses. These previously isolated ventures each had its own measures and strategies for chipping away at and working hardware in a protected way [1], and, generally, there was no section into each other's workspace.

2. BACKGROUND

In any case, now with the coming of brilliant framework innovation, we ought to expect more section of correspondence and data innovation hardware into the workspace of the power utilities [2]. We ought to likewise observe more associated car innovation with module electric vehicles (PHEV) and vehicle-to-network (V2G) fueling. Additionally, the expansion in sustainable power innovation, for example, photovoltaic (PV), wind, and battery stockpiling depend emphatically on data innovation and need wideband [3], fast correspondence for social occasion and transmission of information. Also, the approach of electric vehicles has brought on "candy machine controlling" stations situated at work environments and business focuses, where clients interface with a metered vehicle charging station and pay for power to control their vehicle. This exhibits a merger of the power [4], interchanges, data innovation and car businesses into other mechanical outskirts.

3. THE PROBLEM

This paper investigates how previously free enterprises, for example, control, interchanges, data innovation, and car innovation have combined as the "savvy network," audits existing item security benchmarks for ICT to decide the most noteworthy voltages the hardware can be intended to get to [5]-[6], and investigates what other wellbeing marvels ought to be considered for wellbeing of shrewd matrix ICT gear.

4. PROPOSED SOLUTION

Voltages utilized as a part of the era, transmission, and dispersion of electric power are ordinarily delegated low voltage (LV), medium voltage (MV), high voltage (HV), extrahigh voltage (EHV), and ultra-high voltage (UHV). HV frameworks are ordinarily utilized for transmission frameworks. MV frameworks are commonly utilized as a part of conveyance frameworks. LV frameworks are ordinarily utilized for associating with homes and independent venture foundations. EHV frameworks are utilized for long-remove transmissions [7], and UHV frameworks, the most present day transmission frameworks are utilized for long-separate, appeal utilizes, for example, where the era assets are in one area, and the mechanical request is in another district of vast nations

Assume expenses and assets were of no issue, and we wished to evacuate homeless people on a power transmission or dissemination line utilizing commotion dropping strategies. With this, we should have the capacity to play out the accompanying:

Utilize quick acting sensors to test the transmission waveform, sufficiently quick to catch the mark of the transient or commotion forced on the power transmission line. Change the tested waveforms from high voltage down to levels that would be satisfactory for use by the interchanges and data innovation frameworks. Neither correspondences systems nor data innovation frameworks can handle high voltages, however hope to see additional low voltage signals. Information the changed low-voltage motions on a correspondence system to be prepared by information handling gear [8]-[10].

At information preparing, move the waveform 180 degrees from that tested and gathered. 5. Restore the 180 degrees out-of-stage flag to the correspondence organize. Change the 180 degrees out-of-stage motion go down to high voltage, and add to the power transmission flag [11]. The outcomes ought to be that the clamor and transient voltages on the power transmission line are crossed out by the expansion of the flag that was moved 180 degrees.

5. CONCLUSION

All power-network voltages at MV or HV or LV over 30 V rms or 60 V dc are in this manner considered ES3 sources. If we somehow managed to "commotion cross out" a power-matrix, per our definite case with coordinate access with ICT hardware, the most extreme voltage would be around 63 kVAC (89 kVDC), just underneath voltages utilized for transmission, yet well inside medium voltages utilized as a part of substations and in appropriation lines to low-voltage transformers. As it won't not be doable to develop ICT hardware in light of direct access to control matrix voltages, it might be more pragmatic to anticipate that voltages and streams will be changed utilizing PTs and CTs, in like manner.

REFERENCES

[1] Parikh PP, Kanabar MG, & Sidhu TS. *Opportunities and challenges of wireless communication technologies for smart grid applications*. In Power and Energy Society General Meeting. July 2010; 1-7.
[2] Amin SM, & Wollenberg B. Toward a smart grid: power delivery for the 21st century. *IEEE power and energy magazine*. 2005; *3*(5), 34-41.
[3] Gungor VC, Lu B, & Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE transactions on industrial electronics*. 2010; 57(10), 3557-3564.
[4] Hadley M, Lu N, et al. Smart-grid security issues. *IEEE Security & Privacy*. 2010; 8(1).
[5] Usman A, & Shami SH. Evolution of communication technologies for smart grid applications. *Renewable and Sustainable Energy Reviews*. 2013; 19, 191-199.
[6] Yan Y, Qian Y, Sharif H, & Tipper D. A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials.*2012.
[7] Karthik S. Underwater vehicle for surveillance with navigation and swarm network communication. *Indian Journal of Science and Technology*. 2014; 7, 22.
[8] Raja M C and Rabbani, M M A. *Combined analysis of support vector machine and principle component analysis for IDS*. In Communication and Electronics Systems (ICCES), International Conference on October 2016; 1-5.
[9] R. Geetha, R. Bavya. Design of FIR Filter Using Different Multiplier Architecture for High Speed and Low Power Applications, *IJMSR*, 2017; 9(1): 1-9.

[10] Vu, T. A, Fujishima, M. A 300 GHz CMOS Transmitter Front-End for Ultrahigh-Speed Wireless Communications. *International Journal of Electrical and Computer Engineering (IJECE)*, 2017; 7(4): 2278-2286.
[11] Alasafi, L, Göksu, T, Albayati, A. Copyright Protection by Robust Digital Image Watermarking in Unsecured Communication Channels. *Indonesian Journal of Electrical Engineering and Computer Science*, 2017; 7(1): 234-249.