Central Power Research Institute

Vol. 19(1)/75-80, June 2023
ISSN (Print) : 0973-0338
DOI : 10.33686/pwj.v19i1.1117

Power Research

Cyber Security for Power Distribution System

Shailesh Kapoor*, Amit Jain, V. Shivakumar and M. Pradish

Smart Grid Research Laboratory Central Power Research Institute Bangalore – 560080, Karnataka, India; skapoor@cpri.in

Abstract

Electricity distribution utilities in India are facing major challenges such, as higher revenue realization gap and AT&C losses. One of the ways to overcome this challenge is by adoption of smart technologies and automating the network for increased visibility, monitoring and automated control. The adoption of smart technologies merges the conventional power distribution system with modern communicable devices having sensing and control features. The use of such modern communicable devices makes power systems vulnerable to cyber-attack. This paper presents the SCADA system architecture for power distribution systems, NIST guidelines and framework, cyber-security for power systems and standards for security implementation for telecontrol equipment and systems.

Keywords: IEC 60870-5-101, IEC 60870-5-104, IEC 62351, Internet Technology (IT), Operational Technology (OT), Remote Terminal Unit (RTU), Supervisory Control and Data Acquisition (SCADA) And Data Acquisition (SCADA), IEC 60870-5-101, IEC 60870-5-104, IEC 62351

1. Introduction

Electricity is one of the primary needs for a sustainable and progressive economy in a country. In India, distribution utilities have shown remarkable growth in consumer base and sale of energy. In spite of an increase in sales, aggregate losses and AT&C losses for distribution utilities stand at Rs 50,281 Crore and 22.32%, respectively in FY 2020-21[1]. The government of India has launched various reform schemes since 2002 to bring down these losses to acceptable limits and support the distribution utilities by funding them to take up various automation initiatives for better monitoring and control of the distribution network for plugging in the pilferages. Ministry of Power is trying its best to improve the operational and commercial performance of the distribution utilities through various reforms. It is felt that the absence of modern technology and infrastructure in Indian electricity distribution utilities is one of the major factors for the financial burden on distribution utilities. In the present scenario, one of the ways to better distribution management of power utility is to overcome the above challenges and make smarter utilities in terms of efficiency and reliability. Effective distribution management of distribution utilities can be achieved by using smart technologies. Adoption of these smart technologies like Supervisory Control and Data Acquisition (SCADA), Distribution Management System (DMS), Outage Management System (OMS) and Advanced Metering Infrastructure (AMI) require various communicable equipment operated at power distribution utilities. Now, with newer and smart technologies coming into the utility space, the risk of cyber vulnerability increases due to these smart technologies[2]. Cyber-attacks on the power sector are a threat to national security as the dependence on the power sector is very large in numbers, and it is one of the critical infrastructures which play a vital role in the country's economic growth and progress. Remote Terminal Unit (RTU) is one of the main and commonly used devices in the distribution network, which communicates the field data to the utility and is also used to monitor and control the distribution network points from the utility control centre.

This paper is divided into five sections, Section 1 is an introduction, Section 2 provides an explanation of the SCADA system used in power distribution and Section 3 describes the NIST framework for power system cyber security. Section 4 discusses the importance of cyber security in power distribution systems. Finally, Section 5 provides a summary of the paper.

*Author for correspondence

2. Scada System for Power Distribution System

Supervisory Control and Data Acquisition (SCADA) is a control system used by various utilities and industries to monitor and control processes and operations. SCADA systems consist of sensors, Human-Machine Interfaces (HMIs) and controllers, which communicate with each other to collect real-time data for monitoring and control. SCADA system is used by power distribution utilities to get real-time data from distribution substations and various field devices to monitor and control, including from equipment in the distribution substations, like circuit breakers, numerical relays, battery chargers, and distribution transformers etc[3,4].

Data from distribution substations and field devices are collected using sensors, hard wire connections and Intelligent Electronic Devices (IEDs) etc. There are two types of data which are collected from distribution substations, i.e., analog data and digital data. Analog data like the voltage, current, frequency, active power, reactive power, and power factor, of a particular feeder are collected using communicable digital meters or transducers. Digital data like the status of circuit breakers, isolators, battery chargers and type of faults etc., are collected either using a numerical relay or hard wire connections with the control and relay panels. To transmit these data to SCADA, distribution substations are equipped with Remote Terminal Units (RTUs) through various communication technologies and media and as per standards.

RTU is a microcontroller-based device, which mainly consists of electronic cards like analog input and analog output cards, digital input and digital output cards, CPU etc., used for monitoring and controlling purposes. The communication between distribution substation devices and RTUs are typically established over a communication protocol, such as IEC 61850, MODBUS, DNP 3.0, TCP/IP etc. Once the data is collected from distribution substation devices, it is transmitted to the SCADA system over communication protocols such as IEC 60870-5-104 and IEC 60870-5-101 etc., using the communication infrastructure of the utilities[3,4], usually or over a third-party communication network.

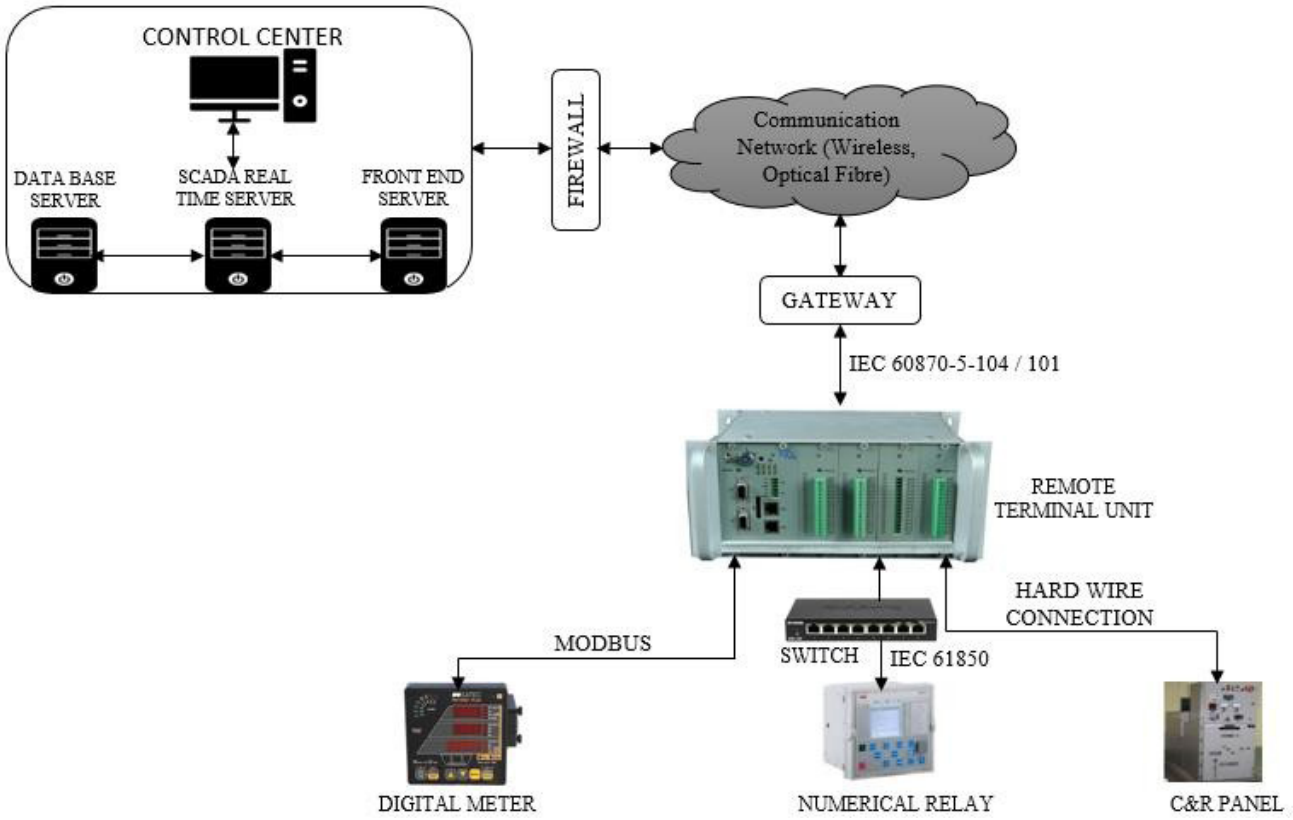

Figure 1. SCADA system architecture for power distribution system.

Figure 1 represents the basic architecture of the SCADA system for the power distribution network.

As shown in Figure 1, a typical SCADA system comprises at least three servers: the front-end server, the SCADA real-time server, and the database server, all configured as separate physical servers or as virtual servers depending upon the size of the system. The front-end server acts as the intermediary between the RTUs and the SCADA real-time server, responsible for collecting and communicating data between RTUs and the SCADA real-time server for processing and analysis. The SCADA real-time server can be configured to display required data for utility control centres and to store in the database server based on the utility requirements both as raw format and as processed data.

Based on the configuration, the SCADA real-time server transmits the required data to the database server for storage, which may be used for various applications such as reports generations, analysis of load trends and identification of issues in the system. Basically, the database server acts as a centralized storage for all the data transmitted. So, all three servers act together to provide real-time monitoring and control of the distribution system devices while also storing the relevant data for future analysis.

3. Nist Guidelines for Power System Cyber Security

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce which develops and promotes standards and guidelines to improve the cyber security of information systems. NIST guidelines for smart grid cyber security explaining about smart grid logical reference model. This model identifies seven domains within the smart grid: transmission, distribution, operations, generations, markets, customers, and service providers. NIST explains that the participants i.e., devices, systems, or programs of these domains, have similar objectives or participate in similar types of applications. The participants of a particular domain often interact with participants of the other domains, as shown in Figure 2. These participants transmit, store, process and edit the information required within the smart grid[4,5].

NIST also explains the high-level view of the participants of each domain of the smart grid. For the distribution domain, RTUs, IEDs, Geographical Information Systems (GIS), distribution sensors etc. are the participants, which interact with transmission, operations, markets, and customer domains. Secure communication between the participants of each domain is very much essential to protect smart gird from cyber-attacks[5].

Based on the high-level security requirements, cyber security objectives for power system operations are as below:

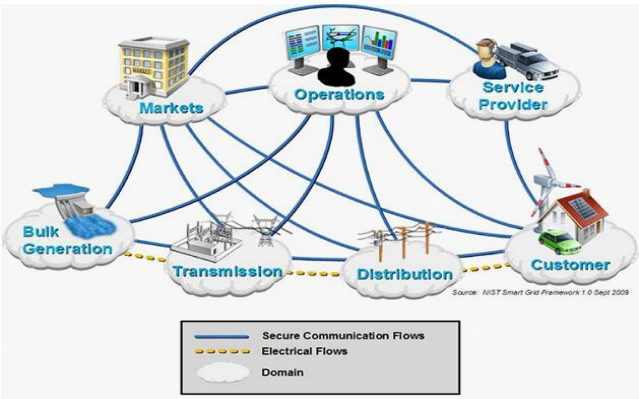

Figure 2. Interaction of participants in different Smart Grid domains through secure communication flows[5].

3.1 Confidentiality

It refers to maintaining authorized limitations on accessing and sharing information, including safeguarding personal privacy and proprietary information[5]. Confidentiality in the context of a power distribution system is the protection of sensitive information, such as access to control commands, customer information, power usage, internal strategic planning etc., from unauthorized individuals. It ensures that only those with proper authorization are granted access to confidential information, which minimizes the risk of cyber-attacks[4,5].

3.2 Integrity

It refers to preventing unauthorized alteration or destruction of information, which includes verifying information non- repudiation and authenticity[5]. Integrity in the context of a power distribution system is the protection of the data from unauthorized modification and tampering. It also ensures that the source and quality of data are authenticated. The adoption of smart technologies is increasing the use of various communicable equipment in power distribution systems. The integrity of the information shared by this equipment is very important as modification of data may disrupt the operation of the power distribution systems[4,5].

3.3 Availability

It refers to guaranteeing timely and reliable access to and use of information[5]. Availability in the context of a power distribution system is the time latency of various information such as availability of real-time data on SCADA, monitoring of equipment and power price information etc. For example, denial of service attacks on power distribution systems may delay sensitive information, which may cause malfunction of critical equipment[4,5].

NIST also provides the framework for improving critical infrastructure cybersecurity, which defines how organizations can manage cybersecurity risk based on a risk-based approach. This framework is divided into three parts: the framework core, the framework implementation tiers, and the framework profiles[6].

The framework core is a set of activities, outcomes, and references that are relevant to critical infrastructure sectors. The framework core consists of five functions: Identity, Protect, Detect, Respond and Recover. These functions provide a strategic view cybersecurity risk management lifecycle for an organization[6]. These functions cover the entire process, from identifying cybersecurity risks to responding and recovering from cybersecurity attacks. It presents the key cybersecurity outcomes to manage the cybersecurity risk. The framework core structure consists of functions, categories, subcategories, and informative references, which is shown in Figure 3[6].

4. Cyber Security for Power Distribution System

Distribution substation automation uses various communicable devices to monitor and control the substation's equipment. As explained in Section 2 of this paper, the transmission of the data between RTUs and SCADA systems uses the communication infrastructure, which makes the power distribution system vulnerable to cyber-attacks.

Cyber-attacks on a distribution system can have serious outcomes[4]. It can target communication networks, control centres and physical devices etc. For example, it can cause the relay to maloperate, which can disrupt the efficient delivery of electricity to consumers. Some of the common types of cyber-attacks on power systems are discussed in this Section[7].

4.1 Malware Attacks

Malware, such as viruses or trojans, can be used to attack the RTU or SCADA system. It can manipulate the data being transmitted from RTU to SCADA and vice versa, causing malfunction of the system.

4.2 Phishing Attacks

These attacks use fraudulent emails or website for the users to trick them into providing sensitive information. Using

Figure 3. The framework core structure[6].

this, attackers can gain access to the control systems of the distribution systems.

4.3 Denial of Service (DoS) Attacks

It involves flooding of unusual packets into the communication network to increase traffic, causing the delay or loss of data between RTU and SCADA system. A DoS attack can disrupt the functioning of the system.

4.4 Man-in-the-Middle Attacks

In this attack, an attacker intercepts the communication between RTU and SCADA system. An attacker can alter the data, which may lead to incorrect measurement and control commands to the substation devices.

5. Standards for Security Implementation for Telecontrol Equipment and Systems

Power distribution utilities are adopting smart technologies such as SCADA, DMS, OMS, and AMI. The deployment of these technologies requires the installation of various communicable equipment within the system. In distribution substation automation, system engineers recognize RTUs / FRTUs as the central component of the SCADA system, serving as the core of automation and control of field equipment. Therefore, ensuring the security and preserving the normal system operation of such telecontrol equipment is of utmost importance. Implementation of security measures like encryption, authentication, intrusion detection and routine security audits of substations is very important to prevent systems from any possible cyber-attacks. This section provides a few of the standards for communication protocol conformance and security implementation for telecontrol equipment and systems.

5.1 IEC 60870-5-101

This is an international standard for the exchange of telecontrol messages between telecontrol equipment and systems using point-to-point communication over serial links. The standard specifies the protocols and formats for exchanging data and commands between telecontrol equipment and systems. This also describes the procedures for establishing and maintaining communication between them[8].

5.2 IEC 60870-5-104

This is an international standard for the exchange of telecontrol messages between telecontrol equipment and systems using the TCP/IP (Transmission Control Protocol/ Internet Protocol). The standard specifies the protocols and formats for exchanging data and commands between telecontrol equipment and systems. This also describes the procedures for establishing and maintaining communication between them[9].

5.3 IEC 60870-5-7

This standard describes messages and data formats for implementing IEC/TS 62351-5 for secure authentication as an extension to IEC 60870-5-101 and IEC 60870-5-104. IEC 60870-5-7 is also used with the definition of IEC/TS 62351-3, in conjunction with IEC 60870-5-104[10].

6. Summary

This paper addresses the major challenges of the Indian power distribution system, explains the SCADA system architecture for the power distribution system, and outlines the cyber security objectives for the power system based on the security requirements as per NIST guidelines. It also describes the NIST framework core structure to develop a strategic view of the cybersecurity risk management lifecycle for an organization. Furthermore, the paper explains the common cyber-attacks on power distribution systems.

The power distribution system provides electricity to the end consumers and cyber-attacks on this system can disrupt the large consumer base. So, the prevention of power distribution systems from cyber-attacks is of utmost importance. In view of this, standards for communication protocols & security implementation for telecontrol equipment and systems used in power systems are also described.

7. Acknowledgment

We are very thankful to Central Power Research Institute for the support extended in carrying out this study.

8. References

1. PFC report on performance of power utilities, FY 2020-21.
2. Saxena S, Sajal B, Gupta R. Cybersecurity analysis of load frequency control in power systems: A survey. Designs. 2021; 5(3):52. https://doi.org/10.3390/designs5030052
3. György D, et al. Challenges in power system information security. IEEE Security and Privacy Magazine. 2012; 10(4):62-70. https://doi.org/10.1109/MSP.2011.151
4. Pandey RK, Misra M. Cyber security threats- Smart grid infrastructure. IEEE 2016 National Power Systems Conference (NPSC); 2016. https://doi.org/10.1109/NPSC.2016.7858950
5. U.S. NIST. Framework for improving critical infrastructure cybersecurity. NISTIR-7628 Revision 1; 2014; 1.
6. U.S. NIST. Guidelines for smart grid Cybersecurity (Version 1.1); 2014.
7. Available from: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/
8. IEC 60870-5-101: Telecontrol equipment and systems-Part 5-101: Transmission protocols- Companion standard for basic telecontrol tasks.
9. IEC 60870-5-104: Telecontrol equipment and systems- Part 5-104: Transmission protocols-network access for IEC 60870-5-101 using standard transport profiles.
10. IS/IEC/TS 60870-5-7: Telecontrol equipment and systems-Part 5: Transmission protocols-section 7 security extensions to IEC 60870-5-101 and IEC 60870-5-104 Protocols (applying IEC 62351).