ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 5 Issue 3 July 2025 / Page No: 63-68
Paper Id: JETA-V5I3P109 / Doi: 10.56472/25832646/JETA-V5I3P109

*Original Article*

# Cyber Secure Substation Distributed Line Protection Relay

**Dr. S. Ganesh[1], Gomathi. A[2]**

[1,2]*Associate Professor, Department of Electrical and Electronics Engineering, Grace College of Engineering, Mullakkadu Thoothukudi. Tamil Nadu, India.*

Received Date: 25 April 2025 Revised Date: 15 June 2025 Accepted Date: 18 July 2025

***Abstract:*** *Intelligent Electronic Devices play a critical role in substation protection, control and monitoring functionalities. Smart grid deployments need the seamless flow of data between relays and controllers, through public communication networks. This kind of deployments lead to inherent requirements for secure communication, strong user authentication and authorization to be considered in distributed line protection and control relays. The cyber security protocols used for communication between devices have to be secured. Securing data over the network involves ensuring confidentiality, integrity and authenticity. This requires strong authentication and encryption algorithm. There are many security tools available but in this project we implement "TLS" (Transport Layer Security) and "IPsec" (IP Security). We have implemented a simple prototype model of distributed line Protection and control in the event of Overload plus Earth Fault Relay. In our project we have used current sensors with feeders in series in order to intellect the fault like short circuit condition or over load condition. After detecting the fault, our microcontroller will send signals to overload unit for tripping the relay instantaneously through secure communication with the help IOT module.*

***Keywords:*** *Substation Automation, Distributed Line Protection, Cybersecurity, Intelligent Electronic Devices (IEDs), Smart Grid, Transport Layer Security (TLS), IP Security (IPsec), Internet of Things (IoT), Protection and Control Relays, Secure Communication, Overload and Earth Fault Detection, Atmega328p Microcontroller, Defense-in-Depth Strategy, IEC 61850, SCADA Systems.*

## I. INTRODUCTION

Protection and control relays, which are the first level intelligent devices in substations, play a critical role in substation protection, control and monitoring functionalities. Relays are an important component of the substation at the bottom of the hierarchical communication network as they have first-hand access to the power systems. They not only play the role of protection which isolates the faulty section of subsystems from the rest of grid but also play an active role in post-fault power restoration and self-healing networks with the help of supported communication network. They aid in the optimized management of substation devices, as well as the overall transmission and distribution power network, which is integral to the smart grid vision and framework. Concepts such as remote configuration/parameterization, remote SCADA communication, remote diagnostics and firmware updates are becoming important requirements for relays. Smart grid deployments need the seamless flow of data between various devices like protection relays, controllers, gateways, smart meters etc. over private and public communication networks. These kind of deployments leads to inherent requirements for Confidentiality, Integrity and Availability (CIA triad part of Information Security concept) of information and data in Substation automation systems network. The implementation of Ethernet based protocols in the relay and exchange of information over public and private networks have brought huge benefits from an operational perspective, but they have also introduced cyber security concerns previously known only from office or enterprise IT systems. Cyber security risks are inherited as soon as we connect the relay on the Ethernet network. Securing relay communication is part of the Defence-In-Depth strategy which is essentially a layered security approach. It uses multiple layers of network security to protect the power system/substation automation network against intrusion from physical and cyber-borne attacks while connected to public and private networks. It also highlights importance of development of security architecture and maintaining the architecture design in-line with current and upcoming cyber security standards like NERC CIP regulations, IEEE 1686, IEC 62351 etc. as parts of these standards define the cyber security capabilities to be adapted by relays in the substation and distribution systems. Secure communication, strong user authentication, authorization, logging and reporting have to be considered in the design and development of protection and control relays. This paper covers secure communication design aspects which are a part of overall cyber security architecture in a relay as well as power system network.

## II. NETWORK COMMUNICATION AND PROTOCOLS

Communication of relays in Substation and distribution Automation Systems with remote gateways and controllers is mostly through Ethernet and TCP/IP based protocols these days. Some of these protocols are power system domain specific which are used for operation purposes. They facilitate exchange of real-time information continuously and consistently

throughout and they are always operational for monitoring and control purposes. Some application protocols are just used for configuration/parameterization, to retrieve data like events/disturbance records for analysis and some basic monitoring for certain period of time.

**A. Operation Protocols**

Protocols such as IEC 61850, Modbus, DNP3, IEC 60870- 104 etc. are predominantly used in Substation automation scenario to provide end users with comprehensive real-time information for monitoring and control of power system network. This allows for higher reliability and greater level of control. These systems have become more and more interconnected.

**B. Engineering/Configuration and Monitoring Protocols**

The configuration and monitoring tools use application protocols like FTP, HTTP, ODBC etc. to download device configuration, upload firmware, retrieve Disturbance/fault record information etc. Web server support shall use HTTP protocol to connect to remote web client. They also enable connectivity to external networks, such as office intranet and internet.

**C. Communication Security**

With enhanced communication in the transmission and distribution power network, cyber-security becomes an essential part of the overall communication network associated with power system. The main idea of communication security is to create a secure channel over an unsecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided adequate cipher suites are used and that the server certificate is verified and trusted. A secure product is however not sufficient, as potential vulnerabilities may arise from insecure integration into existing infrastructures. While a substation can form a separate secured island for energy distribution, it must also provide a robust information firewall for parties communicating with the substation and the associated distribution network.

Substation network architecture must be based on the approach of “Defence-in-Depth” which advocates the use of multiple layers of protection to guard against failure of single security component. Secure communication is just one part of this approach. Designing robust security architecture in the relay should also complement with robust and secured network setup when we are connecting our substation system to external internet network.

**D. Proposed System**

- We have implemented a simple prototype model of distributed line Protection and control in the event of Overload plus Earth Fault Relay.
- In our project we have used current sensors with feeders in series in order to intellect the fault like short circuit condition or over load condition.
- After detecting the fault, our microcontroller will send signals to overload unit for tripping the relay instantaneously through secure communication with the help IOT module.

**E. Securing Protocols With TLS**

The protocols used for engineering the relay and also protocols used for communication between devices have to be secured. Securing data over the network involves ensuring confidentiality, integrity and authenticity. This requires strong authentication and encryption algorithm. There are many security tools available but most famous and widely deployed are “TLS” (Transport Layer Security) and “IPsec”(IP Security).

TLS security protocol based systems are more interoperable compared to IPsec based secured devices. Since Interoperability is an important requirement in Substation and distribution automation domain, TLS based secure communication is a better option for Protection, Control and Monitoring relays. TLS is a protocol that provides a secure channel between two devices. It has facilities for protecting data and identifying the peers. The secure channel is transparent, which means that it passes the data through, unchanged. The data is encrypted between client and server, but the data written at one end is exactly the same as the data read at the other end. Today we have capability to support TLS 1.2 which would be the most secure form as defined in RFC 5246.

TLS is a new network layer that runs in-between applications and TCP/IP. The fact that TLS is a top level network layer has two significant consequences:

- TCP/IP sockets are now used by TLS, on behalf of the higher-level applications
- Application layer modules/protocols like FTP, Web Server, and DNP etc. needs to be specifically designed to use TLS.

**F. Block Diagram**

In this block description we are going to discuss about the block diagram and the process which are done in substation control through distributed unit. In the block diagram of distributed unit into Sensor and measurement unit. The sensor and measurement unit consists of current sensor, earth current sensor and current attenuator circuit. The current attenuator circuit get the input from the current sensor, there is a shunt resistor which is placed in the current attenuator circuit, it converts the sensed current variations into AC voltage, this AC voltage is converted into DC by using rectifier circuit and then this DC is given as a current input to the embedded controller. Same process of earth current measurement to the input of embedded controller. The microcontroller gets the input from the I& Earth current attenuator circuit in its ADC port. The microcontroller which is used in our project is Atmega 328 p, it is a 28 pin, 8bit embedded controller, it consists of 6 ADC pins. In this 6 ADC pins we use 2 pins to get input from attenuator circuit. The voltage and current values are getter from the attenuator circuit and then it is converted into power by using the formula P=v*I. The power values and the frequency values are displayed by using 16 x 2 LCD display. These values are also send to IoT by using Wi-Fi Module (ESP8266).The user can able to see the power and frequency values through IoT webpage. In the control unit we use ULN2003 (Relay Driver)IC to control the relay, because the operating voltage of ATMEGA 328p is 5v dc, It can able to get 5vDC as input and it can deliver 5v dc as output and so our embedded controller cant able to switch on a 12dc Relay.

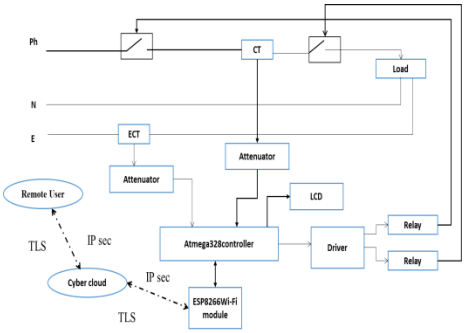


***Figure 1 : Block Diagram***

In this block description we are going to discuss about the block diagram and the process which are done in substation control through distributed unit. In the block diagram of distributed unit into Sensor and measurement unit. The sensor and measurement unit consists of current sensor, earth current sensor and current attenuator circuit. The current attenuator circuit get the input from the current sensor, there is a shunt resistor which is placed in the current attenuator circuit, it converts the sensed current variations into AC voltage, this AC voltage is converted into DC by using rectifier circuit and then this DC is given as a current input to the embedded controller. Same process of earth current measurement to the input of embedded controller. The microcontroller gets the input from the I& Earth current attenuator circuit in its ADC port. The microcontroller which is used in our project is Atmega 328 p, it is a 28 pin, 8bit embedded controller, it consists of 6 ADC pins. In this 6 ADC pins we use 2 pins to get input from attenuator circuit. The voltage and current values are getter from the attenuator circuit and then it is converted into power by using the formula P=v*I. The power values and the frequency values are displayed by using 16 x 2 LCD display. These values are also send to IoT by using Wi-Fi Module (ESP8266).The user can able to see the power and frequency values through IoT webpage. In the control unit we use ULN2003 (Relay Driver)IC to control the relay, because the operating voltage of ATMEGA 328p is 5v dc, It can able to get 5vDC as input and it can deliver 5v dc as output and so our embedded controller cant able to switch on a 12dc Relay.

**G. Circuit Diagram**

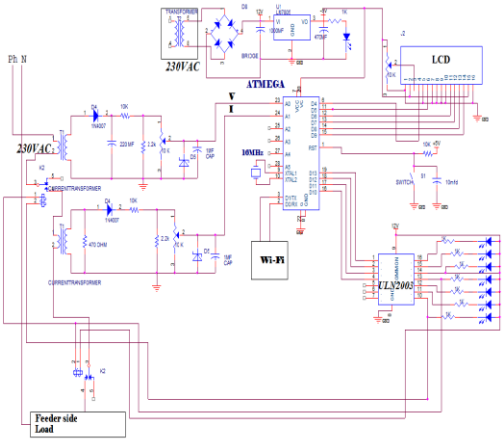

***Figure 2 : Circuit Diagram***

In this project we monitoring and controlling cyber secure substation distributed line protection relay through IoT. Power supply gives supply to all components. It is used to convert AC voltage into DC voltage. Transformer used to convert 230V into 12V AC.12V AC is given to diode. Diode range is 1N4007, which is used to convert AC voltage into DC voltage. LM 7805 regulator is used to maintain voltage as constant. Controller we use Atmega328 controller. It has 28 ports. Reset switch is connected to controller port 1. Current is measured by using current transformer. Current transformer is connected in series with the load. A resistance of suitable value is connected across the secondary of the current transformer. Here the current is converted into voltage. It is given to attenuator unit. In the attenuator circuit is used to reduce the voltage as required level and the output is connected to controller port A0. Earth current sensor is used to measure the earth leakage current of transmission line, it is connected to controller port A1. If over current passed in transmission line or short circuit fault is detected, the controller to trip the power line through driver unit. ULN2003 is used as driver, is connected to controller port D10 to D13. It is used to drive the load through relay. Relay is act as a switch. Two relay we used. It is connected to driver output port 16 & 15. First relay is used to trip the load, and the second relay to use main power source of transmission line. The information is send to IoT Server through Wi-Fi. It is interfaced to controller port 2 & 3. LCD display is used to display the short messages in our project. The LCD display connected to follow pin no.8, 9, 4, 5, 6, and 7. We are used LCD connection 4bit connection.

## III. RESULTS AND DISSCUSSION

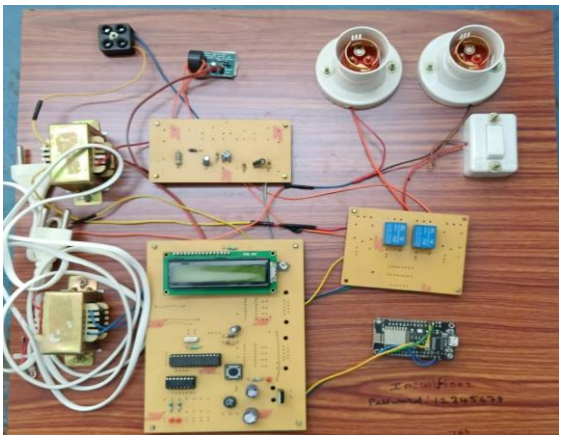

***Figure 3 : Hardware Kit***

The above image is our project demo kit model

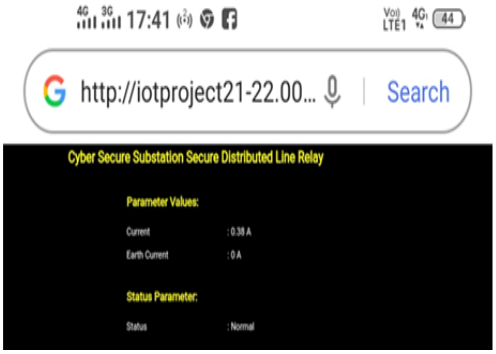


***Figure 4 : IoT Monitoring & Control Page***

The above figure monitoring &control panel page of IoT.


***Figure 5 : LCD Monitoring***

- The above image monitoring in hardware side CUR means Load side current. ECR means Earth current monitor and A is Automatic mode.this condition is Normal condition.
- The below image 5.4&5.5 is an load current is 1.amps above the load current is high.to display the load current high detected.


***Figure 6 : Current High Monitoring.***


***Figure 7 : Load current High Notification***

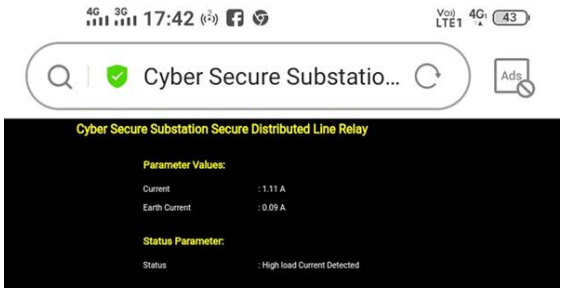


***Figure 8 : The Above Figure is IOT Notification Side High Load Current Detected.***


***Figure 9 : The Above is Earth Current is a High in Display.***


***Figure 10 : To display notification of Earth Leakage Detection.***

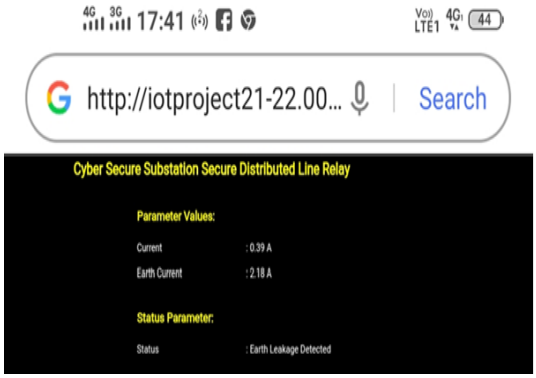


***Figure 11 : The Above Image is Earth Leakage Detection Status Display in IOT Side***

## IV. CONCLUSION

The secured communication mechanism can be developed using available security technologies and seamlessly integrate it to relay architecture to realize certain cyber security requirements. It's true that Cyber security environment is most dynamic and development efforts should be constantly vigilant and check for technology trend and re-build strong security mechanisms and "defence-in-depth" strategy will need to be applied where each system component is an active participant in the creation of secured system in order to overcome the threats to make strong and robust power system networks.

## V. REFERENCES

[1] Jacques Benoit, Meeting IED Integration Cyber Security Challenges: Eskom Southern Africa Power System Protection Conference; November 12- 14, 2008

[2] Markus Braendle, Steven A. Kunsman, White paper Balancing the Demands of Reliability and Security Cyber Security for substation Automation, Protection and Control Systems

[3] AbdelNasir Alshamsi, Takamichi Saito ,A Technical Comparison of IPSec and SSL: Tokyo University of Technology:19th International Conference on Advanced Information Networking and Applications;2005.

[4] [RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000, http://www.ietf.org/rfc/rfc2818.txt

[5] [RFC4217] Ford-Hutchinson, P., "Securing FTP with TLS", RFC 4217, October 2005, http://www.ietf.org/rfc/rfc4217.txt

[6] [RFC2228] Horowitz, M., and Lunt, S., "FTP Security Extensions", RFC2228, October 1997, http://www.ietf.org/rfc/rfc2228.txt