Journal of Electronics and Informatics (ISSN: 2582-3825)
www.irojournals.com/iroei/

Design of a Customized Intelligent Electronic Device for Power Circuit Safety

P. Ebby Darney

Associate Professor, Department of Electrical and Electronics Engineering, RajaRajeswari College of Engineering, Bangalore, India

E-mail: darney.pebby@gmail.com

Abstract

The Intelligent Electronic Devices (IEDs) are widely used to control the power circuits through an automated control device. The main motive of IEDs is to monitor the power flow, enable the control process and meter the changes. In some cases, the IEDs are employed as an electronic circuit breaker for providing a reliable operation. It is achieved by operating the relays through digital signals. The traditional methods have been using a mechanical system for operating the circuit breakers, which requires a manual operation for resting the breakers. The modern IEDs are developed to reset the operation by its own but such systems are heavily affected through data intrusions. Therefore, a programmed IED is developed in the proposed work to analyze if the decisions made by the IEDs are original or fake in a simulated observation. It is done with a mathematical averaging algorithm with respect to time for estimating a threshold. The experimental outcome indicates that the performance of the customized IED is better over the traditional IEDs. Moreover, the proposed device saves the energy distribution in a power system by avoiding the fake operations created in the IEDs through external intrusions.

Keywords: Remote terminal unit, cyber-attacks, false data injection, power circuit analysis, hardware safety

1. Introduction

The Remote Terminal Unit (RTU) is a microprocessor based control device that was before the arrival of IEDs. The RTU are used to connect the systems that are located in various places to a common main unit. It enables the user to monitor the status of different systems from the sample place. The RTUs have input and output terminals for connecting the hardware and it also has a communication interface for controlling the connected systems [1,

DOI: https://doi.org/10.36548/jei.2022.3.003
Received: 27.07.2022, received in revised form: 14 .08.2022, accepted: 26.08.2022, published: 05.09.2022

2]. The IEDs are also work same as of the RTU but the number of connecting terminals in IEDS are comparatively more than the traditional RTU model. At the same the data collection speed of IED is also high when comparing it over the traditional RTUs. Hence the implementation of IEDs is preferred by the users in many applications. In general the IEDs are categorized as operational IED and non-operational IED. The operational IEDs are designed to transfer the collected information to a SCADA (Supervisory Control and Data Acquisition) system for future analytics. The non-operational IEDs are structured to record the changes in the connected system [3]. However, such collected information is safe and can be visible only by the user since it requires an ASCII command for the data operation. The major functions of the IEDs are represented in figure 1.

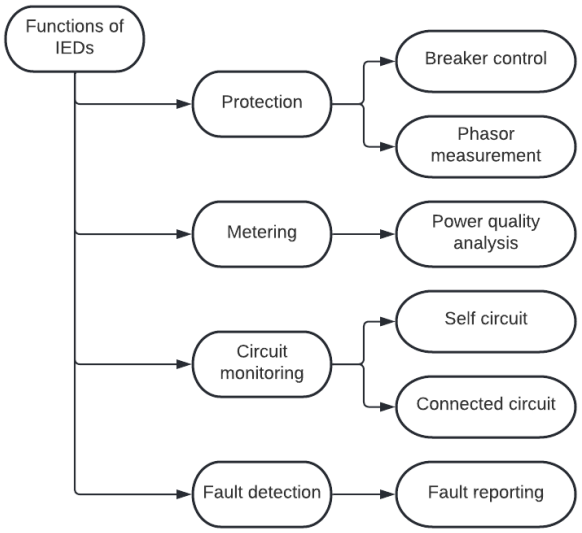

Figure 1. Functions of IEDs

1.1 Protection

The IEDs are primarily designed to give hardware protection to the circuit with minimum count of components. As the IED is a microprocessor based module designed with digital components, its accuracy is comparatively high over the previous equipment. This is achieved by converting the voltage and current waveforms into a required level for operating it with the digital relays for its own safety. The low pass filters are equipped for such work as the microprocessors can operate only logical information. The multiplexer circuits are also utilized in the IEDs for making a digital conversion of from the analog circuits. The microprocessors are also burned with the algorithm for estimating the amplitude and phase angles of the observed readings and that is used to assign the trip logic required for the relay operation.

1.2 Metering

The accuracy of the IEDs in metering application is better over the regular current and voltage transformer circuits. Rather than observing the RMS, real and reactive measurements, the IED records the current demand, power factor ratio along with long term RMS values and that has been utilized for expansion planning and load profiling. Hence the IEDs are widely applied to power system control, automation and other substation processes also.

1.3 Circuit Monitoring

The IEDs are structured with a software system for self-monitoring the internal problems created in the circuit and that can observe and rectify around 98% of their internal problems. The recent year IEDs are having the capability to identify the interfacing and external circuit problems also. The interfacing verification circuit makes the IEDs to verify the inputs from its peripheral components and the IED can protect the connected system from false tripping scenario by analyzing the deviations. The external circuit monitoring system of IED is attained by monitoring the interruptions on the circuit breaker coil and that can lead to identify the failure of the instrument transformers. The modern IEDs are equipped with different kinds of algorithm in protecting the external devices and it has the ability to record the changes that are required for the future analysis.

1.4 Fault Detection

As the IEDs are having the capability to record the waveforms during the failure time, it is easy for a user to estimate the kind of fault involved in the circuit. To do that a nonvolatile memory space is allocated in the IED. However, there is no possibility in the present non-operational IEDs to monitor the waveform changes on a real-time manner.

2. Literature Survey

Primarily, IEDs were designed to do control operations but later they were implemented for protection applications also. The IED model was utilized to give a control operation same as like of a power switchgear [4] and it was made to collect the change in observations in a power circuit with artificial changes. The IED was also applied to a building automation system for making a communication platform between the sensors and the algorithms. In the building automation system three different kinds of IEDs were used for three different operations like lighting, water supply and air conditioning. The experimental

outcome indicates that the proposed system was efficient in handling the multiple sensor data at a single time [5]. The IEDs are widely employed to the smart grid systems for its reliability on transferring the collected data with minimum loss. A binary tree based SVM model was proposed to observe the type of intrusions present over the smart grid system. The work enhances the security of the connected system by making a reduced computational burden [6].

The IEDs were also enforced to the power substation for predicting the insider attacks and it is achieved by adding a sliding window-based sequential classification mechanism to the architecture. The work has the ability to detect the intrusions on multiple IEDs at a same time and to do that six different features were extracted from the dataset. Finally, a bi-LSTM model was incorporated in the work to observe the classification results from the given dataset and it attains an outcome of 1% of false negative rate [7]. A Bayesian compressive sensing theory was implemented over the data collected from the IEDs to estimate the location of the sparse voltage measurement fault. The performance of the created model was verified with a distribution system of 69-bus,12.66 kV contains six various distributed generations [8]. The electronic diagnosis systems are even applied over the electricity energy meter to identify its fault on measurements. It is achieved by making the electronic circuit to follow the traditional backward fault diagnosis method. The experimental work indicates that there is a relationship in the circuit on its inductance and resistance measurement on obtaining a good prediction accuracy [9].

The IEDs are merged with advanced information and communication technology based networks for accessing the collected information in a fast and efficient manner. However, the attackers are trying to add their manipulated data over the sensor information for making the system to run with a malfunction. Therefore a study experiment was conducted on a 14-bus IEEE system with various machine learning algorithms and it founds random forest algorithm performed better on different cases [10]. An experiment was conducted to observe the computational efficiency of an IED at stressed condition. The stressed condition was created artificially by providing multiple commands at a time and the outcome gives a satisfied result with the operation of the IED [11]. A SCADA based automation system was structured to develop a 132/33 kV substation. The SCADA model utilizes the IEDs for monitoring and control process in the substation. The experimental outcome gives a betterment on providing safety to the operational system [12]. The fuzzy comprehensive evaluation method was designed to estimate the status of the power system

connected with SCADA model. To enable the fuzzy matrix function, the work uses the fuzzy and relative deterioration degree theory. The model was framed to provide the status of the connected system with four different categories and that is used to analyze the operation priority [13].

The IEDs were primarily implemented to the substation SCADA systems for avoiding the security threats presence in the TCP/IP carrier. A re-configured IED was framed to provide security to the substation transformers as a circuit breaker. The experimental analysis of the re-configured IED indicates betterment over the response speed of the traditional IEDs [14]. An unsupervised learning algorithm was utilized to observe the nature of a relay event in the substations. The data that are extracted from the SCADA systems are incorporated in the work for analysis and the experimental analysis founds a 41% of the total relay events are found irrelevant with false alarm [15]. The IEDs are incorporated with IEC61850 communication standard to create an alert message over the received intrusions. It is created by transferring the sample values for analyzing such values over the other IEDs. This change in deviation makes the system to identify the particular IED that is affected [16]. A simulation setup was created to develop artificial intrusions over the IEDs and the samples are generated using address resolution protocol. A statistical analysis was performed in the work to detect the intrusions and their natures in the IEDs [17].

3. Proposed Method

The proposed work aims to detect the intrusion presence on IEDs by comparing their random data samples. The architecture of the proposed work is equipped with 3 different IEDs that are connected in series as shown in figure 2. Each IED represents a connection over a substation and that sends their voltage and current measurements to the intrusion detection algorithm for analysis. As the supply line voltages are in heavy range that cannot be considered directly for an algorithm analysis. Therefore, the signals are extracted through the sensors and those are processed with amplifiers and filters for removing the ripples presence in the signal. Also the signals are converted into digital parameters for an easy access to the detection algorithm. Before that, the converted digital signals are processed with a digital signal processing unit for stabilizing the collected data.

The intrusion detection algorithm compares the values observed from the different IEDs. In general, the collected information may vary a bit due to transmission loss and load variations. At the same time the collected information may vary in large numbers when the

system is intruded with an attack. It is analyzed in the proposed work with a threshold value to identify the change deviations in the intrusion algorithm. The performance of the proposed work is verified with a MATLAB analysis and the experimental work is interfaced with a hardware setup for creating an alert signal in the substation.

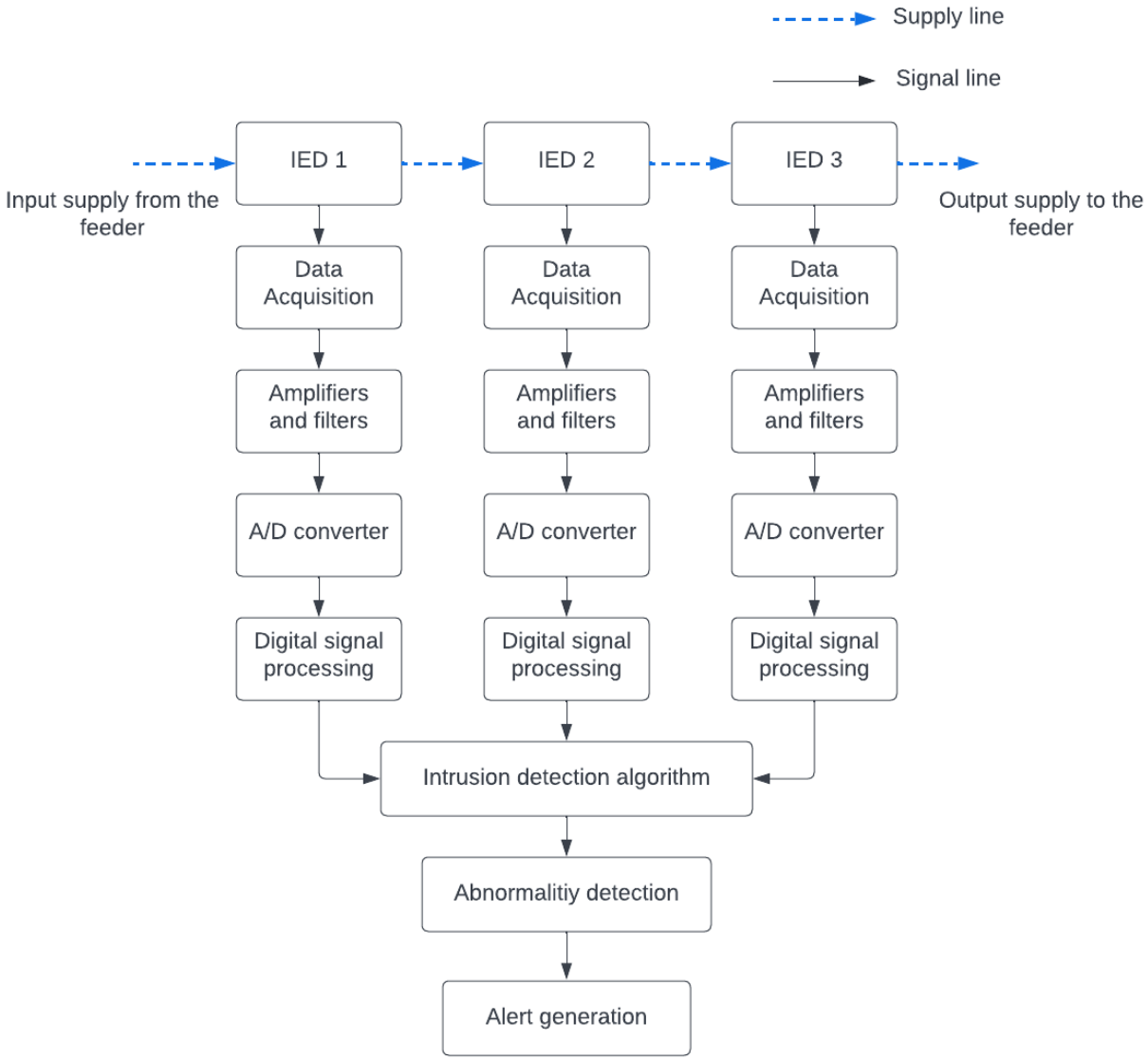

Figure 2. Architecture of the proposed system

4. Experimental Analysis

The performance of the proposed work is verified with a simulation study in MATLAB. It is performed by adding three substations in series for transferring the power supply from one place to another place. The model includes a set of sensor module on each substation for transferring the observed voltage and current values to the processing algorithm. Similarly a digital module is added to each substation for making a control

operation same as like of an IED. A group of manual control options are also connected over the simulated IEDs for generating an artificial intrusion. Based upon the values observed from the connected IEDs an average value is calculated and considered as a threshold value for generating the alert signals. The proposed intrusion detection algorithm is designed to update their threshold value by analyzing the recent deviations observed on the connected IEDs. A threshold parameter of 25% over the regular value is considered in the work as the IED is hacked. Table 1 explores the observations received from the simulation study on various scenarios.

Table 1. Study of the proposed method on various conditions

Scenario	IED 1		IED 2		IED 3		Status	Action
	Voltage	Current	Voltage	Current	Voltage	Current		
1	231	4.1	235	4	229	4.15	No Fault	No action
2	234	3.8	228	5.2	228	3.9	Intrusion	IED 2 disabled
3	225	3.8	227	2.1	229	2	Fault	IED 2 enabled
4	224	5.1	226	6.8	230	4.9	Intrusion	IED 2 disabled
5	229	1.4	229	1.3	231	1.4	No Fault	No action
6	230	2.8	228	1.4	227	1	Fault	IED 2 enabled
7	231	3	230	1.1	225	3.3	Intrusion	IED 2 disabled
8	239	1.5	235	4.2	232	4.2	Fault	IED 2 enabled
9	227	2.3	229	2.2	228	1.9	No Fault	No action
10	222	2	231	6.2	230	2.1	Intrusion	IED 2 disabled

Table 2. Speed response of the proposed system

Scenario	Response time (Seconds)	Action
1	0	No action
2	2.35	IED 2 disabled
3	1	IED 2 enabled
4	2.8	IED 2 disabled
5	0	No action
6	1.1	IED 2 enabled
7	2.45	IED 2 disabled
8	1.05	IED 2 enabled
9	0	No action
10	2.6	IED 2 disabled

The experimental outcome indicates that the proposed system has the ability to identify the intrusion in an efficient way. Though, the experiment is performed to record the time taken to respond over the connected system. All the given scenarios are designed to operate in the IEDs for continuous 60s and the responses of IED 2 with respect to time is shown in table 2 and figure 3 represents the time taken by the system for enabling and disabling the IED 2 on various conditions.

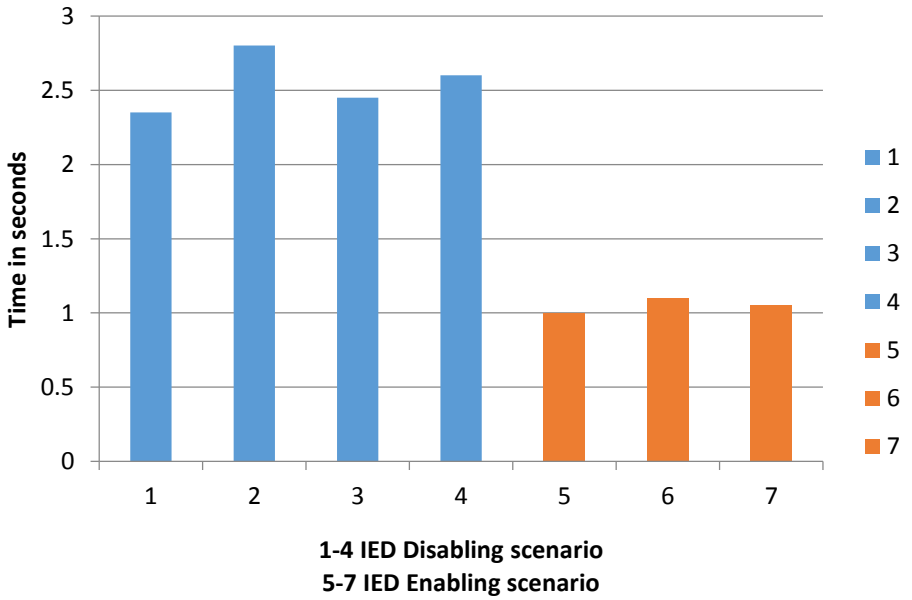

Figure 3. IED response time

The response time of the IEDs at their disabling condition is comparatively higher than its enabling time. It is observed that the disabling actions are done after the IEDs are enabled in the circuit. Hence the time taken for enabling the IED is also added to the action of IED disabling. Therefore the operational time on disabling is higher when comparing to the enabling process. The time delay in the operations can be minimized by implementing a less computation algorithm with enhanced peripheral devices. The proposed work is connected with a buzzer unit for providing an alert signal when an abnormality is observed.

5. Conclusion

The Intelligent Electronic Devices (IEDs) are designed to control and automate the substation processes at different conditions. To do this, the IEDs are incorporated with a microprocessor and digital sensors. The predetermined threshold value decides the operational outcome done by the IED. The proposed work aims to vary the threshold value by considering the voltage and current values of the neighboring stations. Therefore, the fake

and intruded signals are omitted in the proposed model to save the transmission of electrical supply. An experimental analysis is performed based on the proposed work in a MATLAB simulation and is found satisfied with its operational accuracy. However, the work is not satisfied with its response time and that will be rectified in the future work by enhancing the model with a less computational algorithm and enhanced electronic circuits.

References

[1] Kim, Sung-Wan, Bub-Gyu Jeon, Da-Woon Yun, Woo-Young Jung, and Bu-Seog Ju. "Seismic Experimental Assessment of Remote Terminal Unit System with Friction Pendulum under Triaxial Shake Table Tests." Metals 11, no. 9 (2021): 1428.

[2] Uma, Uma Uzubi, Arthur Ekwue, Daniel Nmadu, and Ngozi Clara Eli-Chukwu. "Adaptive distance protection scheme setting in presence of SVC using remote terminal unit." Journal of Electrical Engineering & Technology 16, no. 4 (2021): 1867-1877.

[3] Hor, Ching-Lai, and Peter A. Crossley. "Knowledge extraction from intelligent electronic devices." In Transactions on Rough Sets III, pp. 82-111. Springer, Berlin, Heidelberg, 2005.

[4] Bogdanov, Dimitar, and Ivaylo Popov. "Aspects of intelligent electronic device based switchgear control training model application." In IOP Conference Series: Materials Science and Engineering, vol. 313, no. 1, p. 012010. IOP Publishing, 2018.

[5] Suhanto, S., F. Faizah, and K. Kustori. "Designing a building automation system with open protocol communication and intelligent electronic devices." In Journal of Physics: Conference Series, vol. 1381, no. 1, p. 012006. IOP Publishing, 2019.

[6] Wang, Yong, Jun'E. Li, Xiong Chen, Hai Lin, Fajiang Yu, and Jianbo Luo. "Remote Attestation for Intelligent Electronic Devices in Smart Grid Based on Trusted Level Measurement." Chinese Journal of Electronics 29, no. 3 (2020): 437-446.

[7] Wang, Xuelei, Colin Fidge, GhavameddinNourbakhsh, Ernest Foo, Zahra Jadidi, and Calvin Li. "Anomaly Detection for Insider Attacks From Untrusted Intelligent Electronic Devices in Substation Automation Systems." IEEE Access 10 (2022): 6629-6649.

[8] Jia, Ke, Bin Yang, Xiongying Dong, Tao Feng, Tianshu Bi, and David WP Thomas. "Sparse voltage measurement-based fault location using intelligent electronic devices." IEEE Transactions on Smart Grid 11, no. 1 (2019): 48-60.

[9] Shi, Zhengang, Chaofei Wu, Wenjie Fu, Peng Tao, Linhao Zhang, and Bo Gao. "Analysis on the Application of Electronic Diagnosis Technology in the Components of

Energy Meters in Intelligent Equipment." In International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy, pp. 652-659. Springer, Cham, 2021.

[10] Amin, BM Ruhul, M. J. Hossain, Adnan Anwar, and Shafquat Zaman. "Cyber attacks and faults discrimination in intelligent electronic device-based energy management systems." Electronics 10, no. 6 (2021): 650.

[11] Sanchez-Acevedo, Santiago, Salvatore D'Arco, NargisHurzuk, and RannveigLøken. "Performance Evaluation of Intelligent Electronic Devices under Stressed Conditions." In 2021 IEEE Madrid PowerTech, pp. 1-6. IEEE, 2021.

[12] Mnukwa, Siphokazi, and Akshay K. Saha. "SCADA and substation automation systems for the port of durban power supply upgrade." In 2020 International SAUPEC/RobMech/PRASA Conference, pp. 1-5. IEEE, 2020.

[13] Gu, Jyh-Cherng, Chun-Hung Liu, Kai-Ying Chou, and Ming-Ta Yang. "Research on CBM of the intelligent substation SCADA system." Energies 12, no. 20 (2019): 3892.

[14] PLN, PT, and Blok MI JalanTrunojoyo. "Re-Configuration of IED for Decreasing Cyber Security Threat at SCADA based Substation." information technology 29, no. 7s (2020): 3769-3777.

[15] Andrade, J. R., C. Rocha, R. Silva, J. P. Viana, Ricardo J. Bessa, C. Gouveia, B. Almeida et al. "Data-Driven Anomaly Detection and Event Log Profiling of SCADA Alarms." IEEE Access 10 (2022): 73758-73773.

[16] Hong, Junho, and Chen-Ching Liu. "Intelligent electronic devices with collaborative intrusion detection systems." IEEE Transactions on Smart Grid 10, no. 1 (2017): 271-281.

[17] Premaratne, Upeka Kanchana, Jagath Samarabandu, Tarlochan S. Sidhu, Robert Beresh, and Jian-Cheng Tan. "An intrusion detection system for IEC61850 automated substations." IEEE Transactions on Power Delivery 25, no. 4 (2010): 2376-2383.

Author's biography

P. Ebby Darney is working as an Associate Professor in the Department of Electrical and Electronics Engineering, RajaRajeswari College of Engineering, Bangalore, India. His area of research includes Image Processing, Artificial Intelligence, Control Systems, Radio Networks, and cloud computing.