Abstract

This thesis focuses on two case studies; the first case study presents the real-time series arc fault detection in a low voltage distribution system. An arc fault is a high-power electricity discharge between two or more conductors, which generates heat and can trigger an electrical fire. Loose electrical connections and frayed conductors are typical root conditions that lead to series arcing. It is immune to the existing conventional over current protection devices. The research work presented in this thesis aims to address the susceptibility of the low voltage (230 V, 50 Hz) distribution network toward series arcing. Therefore, a real-time, low-cost, and IoT-enabled arc-fault detection device is needed to detect and report the arc-fault occurrence in low voltage distribution system. Arc-fault generates electromagnetic radiation. This EMR can be categorized into two parts: conducted EMR and radiated EMR. The conducted EMR is transmitted through conducting wire that can be acquired by a current transformer. In the proposed method, we have considered conducted EMR current for analysis. The current flowing in the cable was captured using a current sensor, and then empirical mode decomposition was used to extract the conducted EMR as the arc-fault signature from the captured current. A detection algorithm based on analysing the conducted EMR signal using the EMD and support vector machine is presented in the thesis. Next, the design and development of a low-power, low-cost embedded platform-based real-time series arc detection device are reported. The SVM-based arc detection method is adapted for edge machine learning deployment in an edge micro-controller unit STM32F429 Discovery board. An appropriate signal conditioning circuit is designed for interfacing EMR input data and the microcontroller. The proposed system performs well for real-time arc-fault detection, sending the arc-fault status to the users through Internet of things communication. The offline and real-time results have been reported. The second case study presents the non-technical loss due to unauthorized connection in low voltage distribution system. The unauthorized connection has always been a prime threat for power distribution companies and has affected the country's economy, and innocent customers suffer from high tariffs and unreliable power supplies. Shorting the input-output terminals of the energy meter and connecting an unauthorized load before the energy meter are two popular methods for unauthorized connection. Therefore, a real-time, low-cost, and IoT-enabled unauthorized connection detection device is needed to detect and report unauthorized connections. The proposed method in this work entails injecting a test signal into customers' power line cables. This injected test signal is restricted between the electric pole and the energy meter's output terminal by appending the traps. This injected test signal plays a key role in detecting unauthorized connections. The current flowing in the consumers' power line cable is captured with a current sensor. A band-pass filter separates the injected test signal, and the fast Fourier transform extracts features. An SVM classifier is trained with the extracted features, and unauthorized connection and normal load conditions are subsequently classified. The proposed detection algorithm based on SVM was implemented in an edge microcontroller by exporting it into C/C++. The proposed approach has been validated with traditional household loads for unauthorized load connections. Then, the status of the unauthorized connections is sent through the IoT communication. Both case studies have been successfully implemented on real-time platforms. The detection algorithms and the embedded device have been validated with data generated from a laboratory setup.

Keywords: *Low voltage, distribution system, monitoring, arc detection algorithm, electrical fault detection, electrical safety, electromagnetic radiation, embedded systems, real-time systems, series arcing, unauthorized connection, non-technical loss, power theft detection, fast Fourier transform, Internet of things, micro-controllers, edge machine learning, support vector machine.*