International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 14 Issue 6, June, 2025

Intelligent Electrical Circuit Protection Using Advanced Microcontroller Systems

Waleed Abdullah Saeed[1], Mousa Ahmed Alnashri[2], Bandar Mohammed Muayda[3], Abdullah Mohammed Alshalawi[4], Talal Mohammad Alanazi[5]

[1]Electrical Technology Electrical trainer, at TVTC Al JoufCollege of TechnologySaudi Arabi
[2]Electrical Engineering Electrical trainer, at TVTC Al AhsaCollege of Technology Saudi Arabia
[3]Electrical Engineering Electrical trainer, at TVTC Samtah Secondary Industrial Institute Saudi Arabia
[4]Electronics Engineering Electronics trainer, at TVTC Dammam College of Technology Saudi Arabia
[5]Electronics Engineering Electronics trainer, at TVTC Hafer Albatin College of Technology Saudi Arabia

Work at Technical and Vocational Training Corporation, Saudi Arabia

Intelligent Electrical Circuit Protection Using Advanced Microcontroller Systems

New system implementation is to make a change in the process operations, and it is not an exception with electric circuits. Previous systems had problems with being disrupted because the circuitry was less efficient than it could have been.These circuits broke down repeatedly over time, making using traditional protection devices such as fuses, electromechanical relays, and thermal breakers expensive. Therefore, with the advent of intelligent protection systems, better performance is allowed, where faults can be detected even before they occur, and these systems can adjust to new conditions to help maintain operating conditions. Such systems' design has significantly enhanced their communication capabilities, adaptability, and remote monitoring through microcontroller systems.

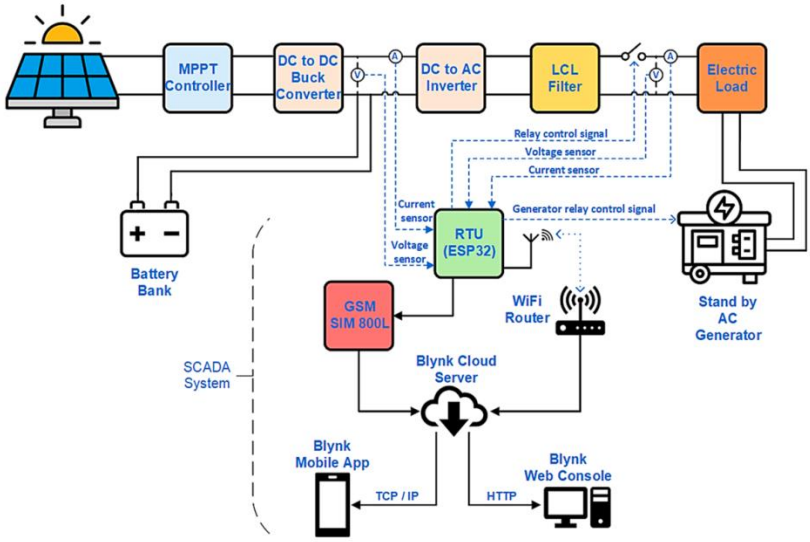
Electronic devices were built to allow individuals to benefit from an electricity supply to their homes, as they added increased convenience to their ability to perform far more tasks at home than they previously could(Pan & Mandal, 2023). While game-changing, these devices depended on the electric power supplied to the house, which presented a challenge because it sometimes varied in current. As a result, it was common for these electric devices to short-circuit due to power surges or outages(Kumar & Srivastava, 2021). Thus, homes and devices were fitted with traditional protection systems such as fuses, relays, and breakers. These systems, while simple, provided an assured fail-safe if the power current surged or there was a sudden outage. However, despite their simplicity, they were often too rigid in their design as they lacked situational awareness, as they relied on single-parameter triggers that were slow to address faults correctly, sometimes leading to unnecessary outages due to trips in the circuitry.

Modern intelligent protection systems provide better protection as they utilize new technology to improve their performance in detecting faults and responding appropriately. These systems use sensing technology with processing to identify complex fault systems. These systems are built to distinguish between a fault that will not last and one that is sustained over a period. This aspect is key because specific faults require appropriate measures, while others only require slight remedial measures (Machidon et al., 2018). Also, while power outages or surges are likely to continue to occur, these intelligence systems are adaptive to the point that they apply trip logic to prevent unnecessary actions from being taken by the circuitry to turn off the power to a house or building. Additionally, these intelligent protection systems are robust to the degree that they allow the entire grid to work seamlessly with the supply functionality(Yin et al., 2022). These systems utilize the networks through which they are connected to monitor changes and ensure that individuals' homes and devices are protected from faults. These intelligence systems reduce the occurrence of downtime and improve the safety of the entire network.

To create these intelligent systems, some most critical components have a significant role in maximizing their performance and offering numerous benefits over traditional systems. Microcontroller platforms are one of the basic components of these systems. Microcontrollers have a multitude of requirements that enable them to protect devices (Zolotov et al., 2024). ADCs are one such critical component, which offer high-resolution and sampling rate. Also, they need to have timers and hardware interrupt support that are crucial in timing to react when faults occur. Realtime performance has to be ensured to achieve it by using RTOS or bare metal (Kumar & Srivastava, 2021). Moreover, rapid signal processing is facilitated

through a floating point unit or DSP instructions. These microcontrollers have to include essential communication peripherals like CAN, UART, SPI, I2C, Ethernet. Also, hardware cryptography is important for confirmation of firmware integrity. In these microcontrollers, low latency GPIO is important as they aid in managing of ports (Pan & Mandal, 2023). Different families of microcontrollers are used in these intelligence systems and those with dedicated DSP are the most commonly used ones in the market. The reason that pulls the most towards a specific type of DSP is the sample rate, the type of interfacing available, and the processing demands.

Intelligent systems that employ these sophisticated microcontrollers for circuit protection have the characteristic that they feature precise sensing and signal conditioning. This attribute is important as it is the foundation of these intelligent protection systems which makes sure that the faults that happen within a network do not have a major negative impact on the connected electronic devices (Esfahani & Mohammed, 2019).In this context, there are options such as employing existing transformers in the case of using AC systems or taking advantage of hall-effect sensors for DC/AC that can work over a wide frequency range. Additionally, shunt resistors can offer essential low-voltage sensing with high precision. Regardless of the large number of options in the scenario of the sensors, they all require anti-aliasing and other filters, offset compensation, gain stages, and, in some instances, isolation (Yin et al., 2022). The other important element is the analog front-end design that is required to maintain the waveform fidelity. Bandwidth with significant transient fault capturing, noise floor critical in the false detection prevention, and input protection through transient voltage suppressors provide this function.



From Microcontroller-based three-phase smart voltage and current monitoring system using Android App by Opeyemi, 2021

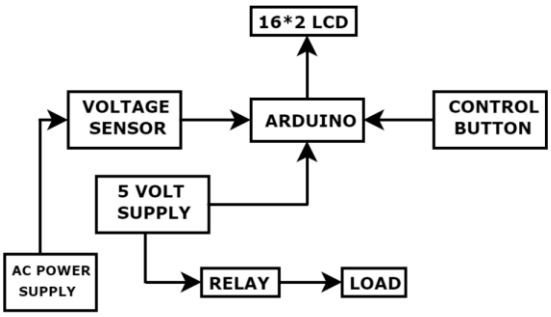
These systems are capable of formulating selective strategies based on using algorithms and reasoning structures on how to defend the devices against destructive impact of excessive flows of electric voltage and electric current. These techniques are the most important in achieving the optimal balance of fault detection and the appropriate response to be formulated and executed within a matter of a few milliseconds to avoid the fault from bringing catastrophic damage. One such algorithmic and paradigms-based approach is the time-domain method, in which an array of methods is used to protect the circuit (Liu et al., 2024). This time-domain method employs approaches of RMS, moving average, and differential calculations to tailor an appropriate response to the fault incident. In the event of an overcurrent, this method assesses the RMS current to determine the adaptive threshold that need to be instituted, which may culminate in an inverse-time trip.

Machidon et al., (2018) suggest that two other techniques used for generating appropriate responses to faults in the system are frequency-domain and DSP techniques. These techniques analyze the current and determine whether the system has a transient or sustained fault. Pan and Mandal (2023) explain that these techniques incorporate the use of the Fourier Transform and wavelets to analyze harmonic and transient signature to determine the difference. Wavelet denoising can isolate a subset of distinguishing features which can be used to identify short-duration faults embedded in noisy signals.

Another way that the protection algorithms work alongside the decision logic is through machine learning and data-driven methods. Regarding machine learning, the algorithm examines the changes in the current state (Zolotov et al., 2024). It explores the impact of the fluctuations on the circuit and what appropriate protections should be used. The algorithm uses the data it has collected from these changes in current to decide on the best protection mechanism (Esfahani & Mohammed,

2019). Therefore, the use of supervised learning methods in this case, through aspects such as decision trees, SVMs, and lightweight neural networks, can be used to classify fault types in terms of spectral energy, kurtosis, and RMS. The challenge with this data-driven approach to labeling the different fault types is that some might not fall in specific categories. As a result, it is essential to provide explanations to ensure safety is maintained.

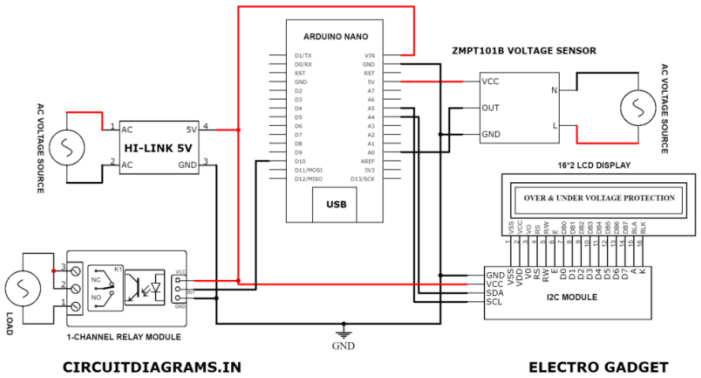
One critical feature of these microcontroller-based intelligent protection systems is that they significantly evaluate how well they administer the correct response. These smart electrical circuit protections can change with the load conditions through adaptive thresholds and self-tuning(Li et al., 2024). Various techniques are employed in such situations, such as applying a percentage response to load baselines to determine if the current is above a critical measure to generate a response. Also, recursive estimators are used to examine the background current to determine if a response to a potential fault is needed. Moreover, using a sliding-window statistical analysis will assist in adjusting the trip setting, which is key as it provides a far more dynamic response to sudden changes based on these settings.



From Overvoltage and Under voltage Protection System Using Arduino by Kundu 2025

An example of the decision logic applied to a situation where a fault occurs involves the intelligent system continuously sampling the current and voltage between 4-20 kHz to determine if it is stable. The system then computes the RMS and detects whether there has been any sudden increases in current and voltage (Esfahani & Mohammed, 2019).When a transient change is detected, a short window FFT is calculated to gauge the spectral signature. If this signature corresponds to the signature of the fault templates that have been collected or the magnitude passes over the threshold within the given time, it asserts a trip in the circuit (Zolotov et al., 2024). The event is based on the outcome logged and communicated to SCADA/DM, and enables configurable retry or a lockout.

These intelligent protection systems are not isolated; they are part of a larger network of safety measures designed to protect the network from failure. Their inclusion in the network is to help ensure that specific faults do not go unrecorded and that appropriate measures are implemented to address customers' concerns(Zhang et al., 2024). Therefore, it is key that these systems can communicate, coordinate, and maintain the standards set throughout the system to prevent major faults from recurring. Despite their capabilities, using these intelligent devices should negate the need for them to follow set standards and procedures concerning current and voltage control (Machidon et al., 2018). These standards are to safeguard not only clients who receive power to their homes and offices but also technicians who conduct repairs. As a result, communication from these intelligent protection systems plays a critical role in informing technicians of faults and their impact on the system.



From Overvoltage and Under voltage Protection System Using Arduino by Kundu 2025 Regarding standards, the IEC 61850, which applies to substation automation and data models, outlines how communication should occur through devices that ensure interoperability across different vendor products. Also, Modbus and DNP3 ensure that the standards surrounding legacy interoperability are maintained(Li et al., 2024). It is also necessary to ascertain coordination through selective tripping and cascade prevention through these systems. Additionally, time synchronization is essential as it aids in aligning various measurements under differential and wide-area protections(Pan & Mandal, 2023). Security is also key in this process and can be enhanced through TLS and secure firmware update mechanisms.

This technology protects the circuit from excessive voltage and current using advanced microcontroller systems. The systems need to be in hardware environments. Therefore, there are some factors that must be satisfied so that it can work in the correct manner. Safety and reliability is one such major factor where the hardware needs to have fail-safe outputs to protect the device from the same faults that it is intended to encapsulate (Das et al., 2020). Therefore, the trip relays should have a standby mechanism that results in a fault secure microcontroller state. This is essential as it creates a state where the system is protected from complete failure in the event something goes wrong. Second, the creation of watchdog timers and redundancy, if possible, creates mechanism that automatically resets the processor whenever it is malfunctioning (Nasrallah et al., 2024). Moreover, initialization of bounded execution times and deterministic interrupt handling imposes explicit constraints on under which the system can run, giving protection in its operation.

Keeping the inner workings of these intelligent guard systems beyond the access of malicious entities is even more important because they can use this automated process to inflict damage on the whole network. Therefore, certain cybersecurity protocols need to be developed to protect it from such entities (Zolotov et al., 2024). Some of which involve establishing a secure boot process, implementing signed firmware, and encrypting the communication within this system (Nasrallah et al., 2024). All these will prevent these malicious actors from infiltrating the systems by knowing how these systems are communicating to each other. Moreover, the role-based access control design, even for the configuration tools of these smart systems, will make sure that only the respective authorized individuals can make changes to the system.

Power management is another area that needs protection for these intelligent protection devices from damage. These devices need to be in a position to survive voltage variations, either through sags or transients (Liu et al., 2024).These devices need hold-up capacitors and a battery backup to conduct critical actions despite a power outage. Some of these vital functions that need to be performed include communications.

During the first-time booting of such systems, it is necessary to verify their operation without exposing them to a live setting. These intelligent protection systems are needed to be tested under a controlled setting to verify their resilience and longevity. They must, therefore, be subjected to a simulation to allow them to detect system faults and validate many of its processes (Das et al., 2020). In such a situation, simulation tools are necessary for conducting a number of tests. For example, SPICE is a tool that can be used for analog front-end simulation. For verifying the algorithm, MATLAB can be used, and HIL setups such as OPAL-RT allow real-time testing with simulated faults in the grid.

While performing simulations for the validity and feasibility of such smart systems, multiple test cases are designed to reach the vast numbers of likely scenarios that can take place in real-time situations. These test cases help determine the span of the problems these systems face and provide valuable reference points that can be used in fixing any errors or problems that can arise (Li et al., 2024). A typical test case includes short-circuit faults that develop through a one-phase and phase-to-phase transmission. Transient spikes and inrush currents also occur while transmitting electric currents. In addition to this, sensor failures and communication loss will most likely be encountered (Pan & Mandal, 2023). Additionally, they will at times be false trip conditions developing due to heavy harmonics.

According to the test cases, the abilities of these smart systems can be estimated and their performance can be measured for various scenarios. The results of such test cases are measured against a list of parameters to consider whether such systems achieve the criteria of functionality as a reference point (Nasrallah et al., 2024). One of the most important metrics of this detection time, measured in milliseconds, is instrumental in the level at which these systems are capable of detecting a fault. Another key metric is the false trip rate every 10,000 hours. The higher the number of false trips within that particular time frame, the more it contributes towards the determination of how well this smart system understands to respond and not respond (Das et al., 2020). The chance of missed-trip under deep faults is another important measure used for evaluating the safety attributes of intelligent systems, as it verifies the accuracy with which a trip is initiated, especially under deep faults. Identification of the use of resources by these intelligent protection systems is required because they have to utilize the provided resources wisely (Pan & Mandal, 2023). These smart programs consume CPU memory, and their percentage is the most important factor to identify their efficiency.

It is essential to examine this system in practice to examine the conditions influencing its effectiveness. Through a worked example, it will be possible to determine how, when an overcurrent occurs, the surge protection of these intelligent protection systems that use advanced microcontrollers is as effective as possible in the case where the microcontroller unit is an ARM Cortex-M4 with a 12-bit ADC, DMA, and an Ethernet connection(Li et al., 2024). This system is one of the best in the market and is rated highly. It also includes various sensors, such as a CT with an anti-alias filter and a voltage divider for line voltage (Zolotov et al., 2024). This system's protection logic is based on a dual path, where a fast comparator-based hardware trip has been installed to deal with cases of catastrophic faults, and it has a microcontroller that utilizes adaptive logic in cases of nuanced trips.

It is essential in the testing of this system that it is evaluated based on simulated experience, where various scenarios are thrown at it to check its reliability in making the right decisions based on the circumstances(Pan & Mandal, 2023). The simulation will run an algorithm that mimics real scenarios. In the firstinstance, the intelligent system was capable of sampling the current at 8 kHz through the use of DMA into circular buffers (Nasrallah et al., 2024). This sampling rate ensured that the system was capable of conducting a regulated evaluation of the current based on the baseline. The RMS managed to compute over 50-millisecond windows. This aspect shows that the RMS was capable of identifying sudden changes in voltage over a given period. The short-energy detector that evaluates current every 2 to 10 milliseconds to detect transients is part of the algorithm(Zhang et al., 2024). Transients often occur within this specific timeframe, so this detector is capable of capturing their occurrence. The machine learning classifier, which is a tiny decision tree, is designed to determine the fault type before a non-immediate trip. Categorizing these faults is key to evaluating which types of faults the system is capable of providing adequate protection for and which ones result in a false trip.

The anticipation from this simulated case is that, during its operation, there existed various fault sizes that were computed in the range of 1-50ms depending on the magnitude of the current and depending on the path utilized in the algorithm (Liu et al., 2024). Detection rate accuracy confirmed that effective electric circuit protection had been provided by the smart protection systems through such advanced microcontroller systems (Pan & Mandal, 2023). The response rate was within the usual response curve. There were sensitivity and false-trip probability compromises, however.

In brief, the foregoing analysis of the microcontroller-based intelligent protection systems shows that the systems can provide the assistance required so that electronic devices are not ruined due to unanticipated fluctuations in current or voltage. The systems have the deep benefits of velocity, flexibility, observability, and capability of integrality. The systems play a crucial role in making the electricity networks competent for supplying stable electricity. Sophisticated microcontroller systems are one main reason behind increasing the precision of such smart protection systems. Most devices in the MCUs family provide sampling and processing specifications. Sophisticated front-end analog protection and fidelity have to be provided in these systems. Grasp these systems with standards, and also prioritize cybersecurity as a main concern.

REFERENCES

[1] Das, T. K., Debnath, R., & Biswas, S. D. (2020). Modeling and implementation of an advanced electronic circuit breaker technique for protection. In *Lecture notes in networks and systems* (pp. 15–26). https://doi.org/10.1007/978-981-15-6198-6_2

[2] Esfahani, M. M., & Mohammed, O. (2019). An intelligent protection scheme to deal with extreme fault currents in smart power systems. *International Journal of Electrical Power & Energy Systems*, *115*, 105434. https://doi.org/10.1016/j.ijepes.2019.105434

[3] Kumar, A., & Srivastava, V. M. (2021). An efficient model for low voltage distribution smart feeder overcurrent protection system using microcontroller. *IOP Conference Series Materials Science and Engineering*, *1152*(1), 012015. https://doi.org/10.1088/1757-899x/1152/1/012015

[4] Kundu, T. (2025). Overvoltage and undervoltage protection system using Arduino. *Electro Gadget*. https://circuitdiagrams.in/overvoltage-and-undervoltage-protection-system/

[5] Li, P., Zhou, M., & Zhang, R. (2024). Research on the development Trend of intelligent Circuit Breaker in building installation. *Academic Journal of Science and Technology*, *12*(2), 67–71. https://doi.org/10.54097/ffs6wb97

[6] Liu, Y., Dang, D., & Lee, S. (2024). Research on the protection system for smart Grid based on Phasor information at circuit breakers. *Energies*, *17*(14), 3455. https://doi.org/10.3390/en17143455

[7] Machidon, O. M., Stanca, C., Ogrutan, P., Gerigan, C., & Aciu, L. (2018). Power-system protection device with IoT-based support for integration in smart environments. *PLoS ONE*, *13*(12), e0208168. https://doi.org/10.1371/journal.pone.0208168

[8] Nasrallah, M., Abdelaleem, A., Ismeil, M. A., & Hussein, H. S. (2024). Adaptive electronic relay for smart grid based on self-healing protection. *PLoS ONE*, *19*(10), e0309966. https://doi.org/10.1371/journal.pone.0309966

[9] Opeyemi, O. (2021). *Microcontroller-based three-phase smart voltage and current monitoring system using Android App*. Opstep. https://opstep.com/microcontroller-based-three-phase-smart-voltage-and-current-monitoring-system-using-android-app/

[10] Pan, P., & Mandal, R. K. (2023). Intelligent Short-Circuit Protection with Solid-State Circuit Breakers for Low-Voltage DC Microgrids. *IETE Journal of Research*, *70*(3), 3187–3203. https://doi.org/10.1080/03772063.2023.2181228

[11] Yin, J., Lang, X., Xu, H., & Duan, J. (2022). High-Performance breaking and intelligent of miniature circuit breakers. *Sensors*, *22*(16), 5990. https://doi.org/10.3390/s22165990

[12] Zhang, R., Li, X., Ding, J., Chen, S., Yang, H., & Guo, H. (2024). Review of IGBT Intelligent Gate Drive and Protection Strategies. *IEEE Transactions on Power Electronics*, *39*(6), 7392–7403. https://doi.org/10.1109/tpel.2024.3372254

[13] Zolotov, A. R., Ledovskikh, A. A., Zhukov, A. N., Zharkov, A. A., Kazemirova, Y. K., & Anuchin, A. S. (2024). Development and implementation of algorithms for an intelligent IGBT gate driver using a Low-Cost microcontroller. *Applied Sciences*, *14*(10), 4247. https://doi.org/10.3390/app14104247