Journal of Electronics and Electrical Engineering
https://ojs.wiserpub.com/index.php/JEEE

Research Article

Smart Building, Nuisance Electrical Failure, Remote Monitoring and Fault Recovery System

Berhane Gebreslassie, Akhtar Kalam, Aladin Zayegh

Department of Electrical Engineering, Victoria University, Melbourne, Australia
E-mail: berhane.gebreslassie@live.vu.edu.au

Received: 30 May 2024; **Revised:** 5 September 2024; **Accepted:** 24 September 2024

Abstract: Smart Buildings are the fastest growing buildings compared to conventional buildings and are expected to grow at a rate of 8.3% for the next decay. The global commercial building automation market was valued at US$32.96 billion in 2020 and is expected to reach US76.49 billion by the year 2031. The implementation of technological advancement, demand for energy-efficient construction, low operational cost, and occupant comfortability have helped Smart Building to grow. However, Smart Buildings are still facing issues, from various sensor network diversity, clear definitions of Smart Buildings, and continuous smartness during full or partial electrical internal fault occurrence. This indicates the building is smart as long as a continuous power supply is present. Thus, this research study investigated Smart Building's drawbacks and designed a circuit to be a solution to one of the drawbacks to rectify the issues. The design provides full monitoring for real and nuisance failures and enables the performance of fault recovery procedures remotely. The circuit interfaces with the safety Residual Current Devices (RCD) and the wireless smart Wi-Fi-controlled socket outlets. Food industries, hotels, and restaurants could be the beneficiaries of this circuit. This is due to cold stores and fridges, which can lead to significant production loss/reduction when failure time increases.

***Keywords*:** Smart Building, electrical fault remote monitoring, residual current device nuisance fault recovery, electrical earth-leakage remote fault investigation

1. Introduction

Smart Buildings are the fastest-growing buildings compared to conventional buildings and are expected to grow at a rate of 8.3% for the next decade [1]. The global commercial building automation market was valued at US$32.96 billion in 2020 and is expected to reach US76.49 billion by the year 2031 [2, 3]. The rise was driven by demanding energy efficiency and penetration of internet data into Eco-friendly buildings [4]. This is practically proven, especially in well-developed cities. Furthermore, Smart Buildings and Smart cities are major contributors to smart environmental living. However, there are no clear standard specifications of regulation setup that Smart Buildings should include or exclude. In other words, to be called a Smart Building, what criteria have to be satisfied? A number of recent research papers prove that Smart Buildings are implemented with various different smart technology network protocols. Researchers of these papers examine buildings equipped especially with large data from various sensor networks that face drawbacks [5]. This is because the diversity of the protocols is not easily compatible. For example, Smart Building operates interoperability from sensor networks such as Internet of Things (IoT) networks. The IoT network can interface with healthcare bio-data,

DOI: https://doi.org/10.37256/jeee.3220245043

and another IoT network can interface to the extent of Machine Learning data [6, 7]. In both networks, data collection is done by the IoT sensors. Assuming that both networks use different manufacturers that have incompatible protocols, how to communicate directly between these different protocols is the issue. However, this research paper focused on the advantages of buildings smart networks, such as IoT sensors, heading in the near future. Nowadays, IoT networks are heading to replace humans' professional skills; analysis and decisions are made by the IoT machines/sensors according to the data come from, such as in the health system, the machine will be provided with the activity and treatment required. This is because IoT machines gather all the information from the world. Currently, the life of humans depends on Doctors for treatment, but in the future, human life treatment will depend on the IoT [8].

Currently, besides the IoT networks, several others operate in modern buildings. For example, the Building Automation System (BAS) is one of the major players in energy consumption controller network technology inside the building. BAS network interoperability interfaced with BIM [7] to monitor energy and to enable to consume wisely [9]. A similar Building Security System Network (BSSN) is one of the main contributors to Smart Buildings. With the introduction of IoT networks, Smart Buildings are not only physically secured using surveillance cameras and motion detector sensors but are also highly secure from cyber internet attacks [10]. Building Multimedia Entertainment System (BMES) is another smart technology system that contributes to Smart Buildings by transmitting audio and video streaming data wirelessly inside/outside of the building, which provides the occupants with fast and reliable information [11]. Thus, the contribution of those modern technology networks makes the buildings be named "Smart Building". Even though Smart Buildings are widely accepted and growing fast, including most recently designed Smart Buildings, still suffers (1) from sensor diversity [3] and (2) from a lack of clear standards or guides from the Government side to define the classification of Smart Buildings. Consequently, Smart Building names are mostly monopolized and operated by different competitive commercial private companies or private organizations, using various names and concepts, such as, digitize/Intelligent Building, Green Building and BlueIoT. Due to the various companies uses different sensors and brands to build their unique network system, some Smart Building owners implemented the "K-means clustering technique", which is used to identify the variant equipment/sensors connected to the building [12]. In addition, organizations such as Leadership in Energy and Environmental Design (LEED) [11] and Green Building Council Australia (GBCA) developed equipment's energy rating and certification system to define the consumed energy, especially for Green Building achievements. In fact, adopting that certification made a significant contribution to Greenhouse gas emission reduction. (3) Smart Building also suffers from being continuously smart; during full or partial internal fault occurrence, it loses, its smartness. This indicates the building is smart as long as a continuous power supply is present, for example, when part of safety wiring installation protection devices in the main switchboard is tripped by a nuisance fault [13]. The smart equipment connected to that part line loses its smartness, and remote access points go down, and no information can be retrieved.

Further, exploring the literature review of nuisance tripping, several studies have been conducted focused on the RCD nuisance tripping issues. For instance, a recently published research study focused on "tripping characteristics of RCD under different working conditions". The paper's research aim and objectives were to investigate the influence of frequencies, harmonics and surge currents [14], which cause nuisance tripping. The research method used was Neutral-line current injection from an external source to create an unbalanced current flow within the RCD's coil. The paper investigates the minimum current and frequency for different working conditions and recommends that RCDs should be redesigned with better engineering to minimize nuisance tripping. This research uses the current injection for the proposed research rather than for mitigation. A Similar research paper focused on the "effect of higher frequency residual currents on the operational RCD" [15] investigates the RCD's tripping responses caused by higher frequencies over the fundamental frequency. The research methodology uses simultaneously injects earth leakage current loads associated with higher frequencies. The main goal of this study is to find out the nuisance tripping characteristics of different types of RCDs that are from different manufacturers. The injected current was again used for the purpose of the study. Furthermore, another recently published paper, "Impact of Residual Harmonic Current on the operation of RCD" [16]. Similarly, this research goal also focused on the influence of harmonic residual currents related to crest factor tripping sensitivities. The research conducted experimental nuisance tripping tests of 300 mA, 30 mA, and 100 mA, proving that the 100 mA test showed better performance. However, most of these research papers in this field are concentrated on analyzing the tripping characteristics of RCDs as the primary mitigation method to reduce the number of nuisance tripping. The time and the economic loss after the RCDs were tripped by nuisance faults were not considered. Thus, this research study is designed to rectify the problem of enabling motoring remotely and performing fault recovery procedures remotely. This means the building will not lose its smartness for a longer period. This method could be significantly beneficial to commercial businesses, such as pharmaceutical companies, food industries, hotels, and restaurants, where fridges and cold stores could be exposed to significant production loss when failure time increases.

2. Design and modelling of remote monitoring system

Modern building switchboards are fitted with one primary switch, which is known as the main switch circuit Breaker; one or more RCD breakers, depending on the size of the installation; and many sub-division installation overcurrent controller circuit breakers. Each part has its own specific functions. The main switch controls the whole building installation and is likely to be affected by a fault occurrence inside the building by the appliance. Its primary purpose is to isolate the supply power, especially during maintenance. The individual sub-deviation line controller circuit breakers are mainly affected by dead short or overcurrent in the circuit, and it is rare to occur unless there are overload currents or incorrect wiring in the circuit. The most fault that can occur is on the RCD. The RCD can be temporarily or permanently affected by a nuisance spike or real earth leakage current [17]. Due to it being designed for safety, it is not designed for automatic reset; it is designed to be reset manually. Hence, the design is not helpful for a fault spike temporary and intermediate fault. The fault downtime could cause significant production loss. Therefore, it is necessary to re-design the RCD and the WI-FI-controlled sockets and lighting switches to interoperate during failure occurrence on the sub-division zone circuits, as shown in Figures 1–4. Where Figure 2 flow chart shows the design, monitoring and fault-resolving procedures. The remote app monitors the status of the building's electrical system, but for the purpose of this study, the 10 A, 2400 W heating appliance is selected, and the operating current is continuously monitored, as shown in Figure 5. The consumed load variations are registered as full load, partial load and no load. Hence, outside these ranges can be considered abnormal current.

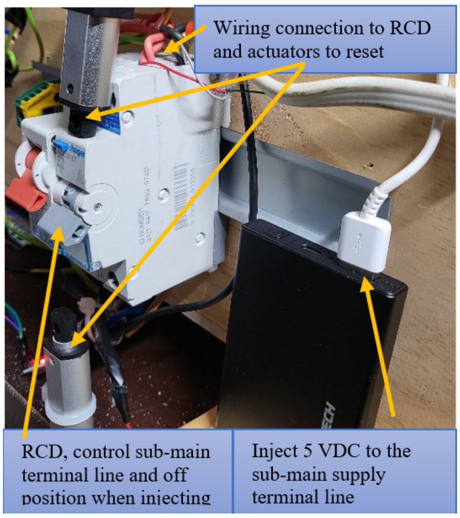

Figure 1. Socket outlet, node voltage fault identification testing components. The 5 VDC is injected at the RCD terminal. The arrows indicate the type of device used

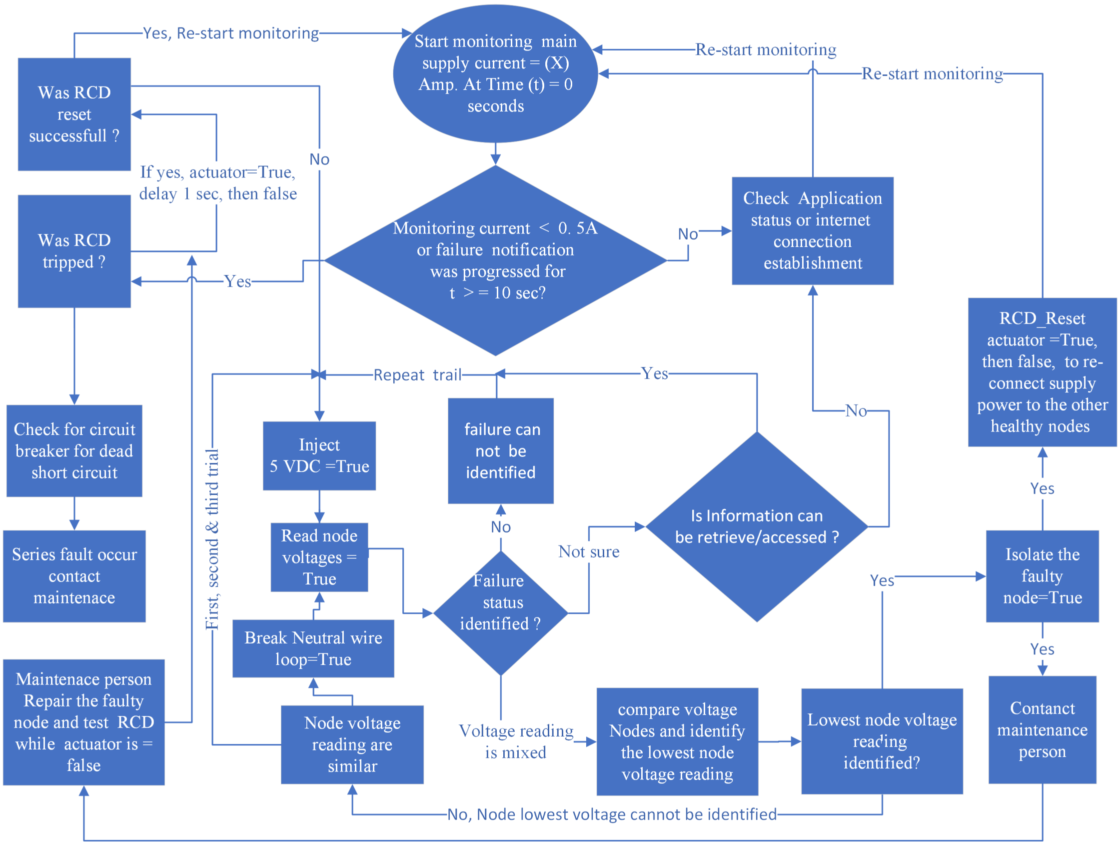

Figure 2. Remote monitoring and fault rectification design flow chart

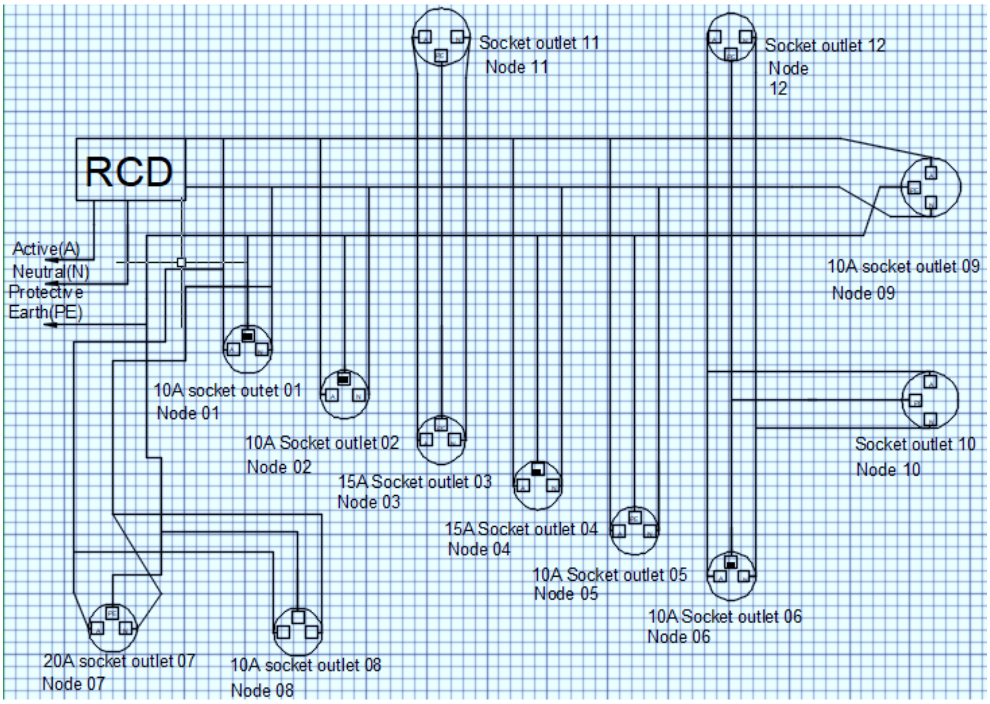

Figure 3. RCD sub-division socket outlet wiring network nodes, where one RCD controls different rating loads

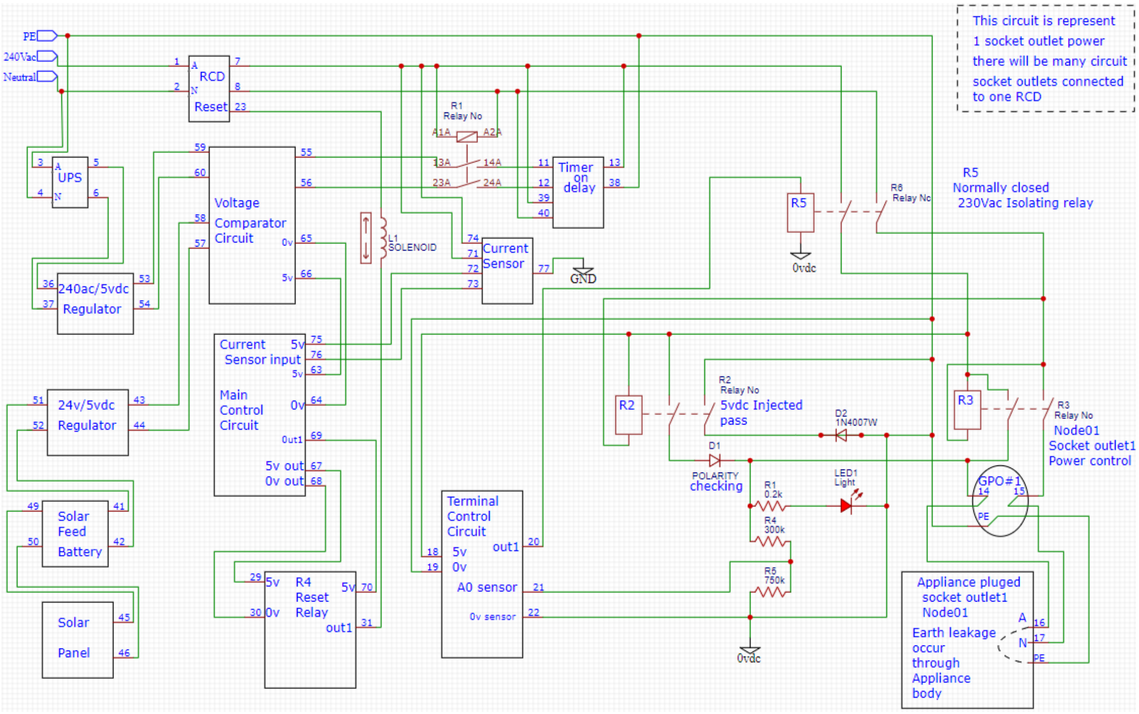

Figure 4. Remote monitoring and automatic reset for nuisance fault recovery circuit

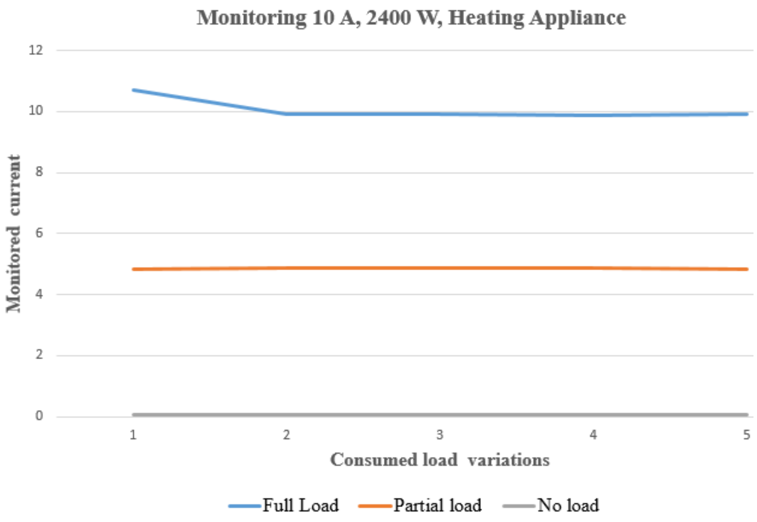

Figure 5. Remote current monitoring test for 10 amp 2400-watt heating appliance. Threshold no load is close to zero

2.1 *Current monitoring analogue sensor*

The main circuit current is constantly monitored using the ACS712's current sensor component. ACS712 is an electronic industrial and commercial current-measuring device [18]. The device is installed at the main supply, which will monitor the overall current passing through the building. However, when a fault occurs in one of the socket outlet nodes, the current changes due to either the RCD or circuit breaker trips. The last current before tripping occurs can be recorded to identify the type of fault, as shown in Equation (1). When no signals are received for a longer period, the apps execute self-checks for the internet connection. When a current outside the specification or a failure signal notification is received, the app checks for RCD failure. If RCD failure occurs, examine the short and overcurrent values for the circuit breaker current rating and tripping characteristics. Reset the RCD and examine for another fault occurrence. If the fault was a nuisance, it should be cleared. If the fault persists, follow the next steps.

2.2 *Logical statement and equation*

Main supply voltage $\leftarrow$ 230 V
Monitor the main supply current $\leftarrow$ 10 Amp
Sub-division line impendence (Z) $\leftarrow$
Monitor no load threshold current $\leftarrow$ 0.5 Amp

If (Monitor no load threshold current is < 0.5 Amp or connection not established for greater than ten seconds), then the application or the WiFi fails. Check, for application correct operation, WiFi-connection and resume monitoring.

If a failure notification message is received, execute Equation (1) and analyze the last recorded fault current.

$$\text{monitored fault current } (\mathrm{X}) = \frac{\mathrm{V}}{\mathrm{Z}} \tag{1}$$

where V is the RCD volts, and Z is the impedance of the line cable connected to the RCD and the socket outlets.

$$\text{Current monitoring 10 A node} = \begin{cases} \mathrm{X} \geq 10 \text{ A is earth leakage} \\ \mathrm{X} < 11 \text{ A is over current} \\ \mathrm{X} < 15 \text{ A is short current} \end{cases}$$

$$\text{Current monitoring 15 A node} = \begin{cases} \mathrm{X} \geq 15 \text{ A is eart leakage} \\ \mathrm{X} < 16 \text{ A is over current} \\ \mathrm{X} < 19 \text{ A is short current} \end{cases}$$

$$\text{Current monitoring 20 A node} = \begin{cases} \mathrm{X} \geq 20 \text{ A is earth leakage} \\ \mathrm{X} < 21 \text{ A is over current} \\ \mathrm{X} < 25 \text{ A is short current} \end{cases}$$

If the RCD fails, the linear actuator is set to True for t = 10 s, and then the actuator is set to false. Then wait for the response for 2 min. If the response is positive, the nuisance fault is cleared, and monitoring is resumed. If the response is negative, then inject 5 VDC is set to True. Read socket outlet node voltages set true. If failure type is not identified, repeat the process; else, if the read lowest voltage cannot be identified and node voltages are similar, set neutral loop wire true, then read node voltage individually. If the lowest voltage is identified and fault typed identified then isolate the faulty node is set to true, and resume power.

3. The safety RCD operating principals

RCD is an electromechanical safety device that is designed to provide protection against electrocution and electrical fires by cutting off the flow of electricity automatically when it senses a leakage of current in the circuit. RCD functions on the principle that the incoming current is the same as the outgoing current. RCD incorporates a core balance transformer (CT) having primary and secondary windings with a sensitive relay for instantaneous detection of fault signals [19, 20, 16] as shown in Figure 6.

RCD primary winding lies in series with the supply mains and load. The secondary winding is connected to a very sensitive relay. During faultless conditions, the magnetizing current passing through the current-carrying conductors cancel each other. There is no residual magnetic field that can induce a voltage in the secondary coil. However, during the flow of the leakage current, an imbalance occurs in the circuit, which gives rise to leakage flux in the secondary coil. This leakage flux generates an electrical signal that is sensed by the relay, and it trips the mechanism and then disconnects the supply voltage. The trip mechanism is operated at a residual current between 60–80% of its rated leakage current [21]. Nowadays, the implementation of RCD in residential and commercial buildings is compulsory for the purpose of electrical circuit safety fault monitoring. RCD controls multiple line circuits in a residential or in nonresidential electrical switchboard. Furthermore, it is installed to protect from electrical shock and save life from electrical death. However, the safety device experiences real and non-real faults, especially when heating devices with lower impedances are connected or when higher harmonic and temporary transient is present in the circuit [15, 16]; then, it isolates the circuit from flowing currents without analyzing the type of failure causes. RCD controls multiple subdivision terminals, and when a fault occurs, it is difficult to analyse the fault from which the terminal is occurring. In some cases, it takes a long time for experienced tradesmen or electrical engineers to find the fault. This can lead to some unnecessary running costs for commercial building operators and owners.

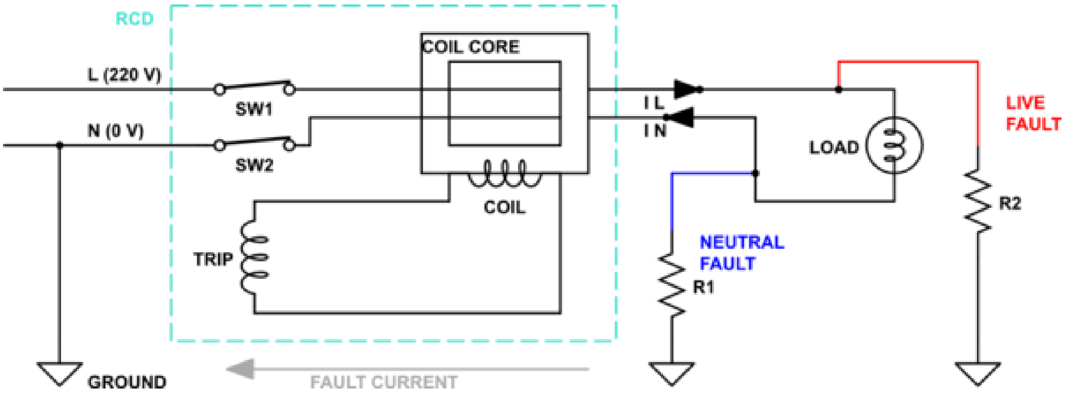

Figure 6. RCD operating principle: 220–240 V active and neutral is supplied to the RCD terminals (SW1 and SW2). Both the active and the neutral wire pass through the coil core connected to the load via polarity diodes (1L and 1N), creating a balanced magnetic field in the core coil. When the active (R1) contacts the ground, the return current becomes < than the supply current and the magnetic field through the coil becomes less and causes the trip current to vary, which further causes RCD to trip. Source adapted from https://i.stack.imgur.com/uBjLA.png

RCD, Nuisance tripping, and response to the steepness of rise of the distorted current depend [20]:

$$\frac{di_1}{di_2} = \frac{2\sqrt{2\pi I_1 f_1}}{\sqrt{\sum_{k=1}^{n} h_k^2}} \sum_{k=1}^{n} \left(h_k k cos\left(\varnothing_k\right)\right) \tag{2}$$

where

I_1 = the effective value of the primary current distorted by harmonics with a share of $h_k = \frac{I_{mk}}{I_{m1}}$,

φ_k = the angle of the k^{th} harmonic

k = the number of next harmanic

$\frac{di_1}{dt}$ = The actual rate of changes of the currents with respect to time-variant. This can be defined as the actual speed of the current in the circuit.

3.1 *Nuisance fault occurrence in the power system*

Circuits containing capacitance and inductance have one or more resonant frequencies. When any of the resonant frequencies correspond to the harmonic frequency produced by nonlinear loads, harmonic resonance can occur [22]. Voltage and current during resonant frequency can be highly distorted. This distortion can cause nuisance failure in an electrical power system [23]. Furthermore, nuisance failure can be caused by transient current from the entire electrical network or from the branch of the electrical network if the transient peak value is above the ground base/threshold of the RCD, which subsequently causes the RCD to fail. The transient or the harmonic frequencies may be only a few milliseconds in duration, but the combination of the transient spike magnitude and duration of disturbances causes the RCD to trip and remove power from the building. Further, in a circuit with distorted residual current, the tripping characteristic of RCD changes. The theoretical mathematical expression of RCD relay tripping operation under the influence of harmonics depends on the residual current as a function of time, the amplitude of residual current, the harmonic frequencies and harmonics phase angles [3]. The distorted residual current can be expressed as:

$$i_{\Delta} = I_{\Delta amp}\ \left[\sin\left(\omega t + \varphi_1\right) + C_3 \sin\left(3\omega t + \varphi_3\right) + C_5 \sin\left(5\omega t + \varphi_5\right) + \ldots + C_h \sin\left(h\omega t + \varphi_h\right)\right] \tag{3}$$

where:

i_{Δ}, residual current as a function of time.

$I_{\Delta apm}$, the amplitude of the residual current

C_3, C_5, …, C_h are the content of the amplitude to fundamental frequency due to the 3rd, 5th… hth harmonics.

$\varphi_3,\ \varphi_5,\ \ldots,\ \varphi_h$ are the phase angles of the corresponding harmonic 3rd, 5th… hth harmonics.

3.2 *Cause of harmonies and transients*

Harmonics are created by electronic equipment with nonlinear loads drawing in current in abrupt short pulses. The short pulses cause distorted current waveforms, which in turn cause harmonic currents to flow back into other parts of the power system [24]. Harmonics degrade the level of power quality and its efficiency, particularly in commercial buildings or industrial facilities. In general, most buildings can withstand nonlinear loads of up to 15% of the total electrical system capacity without RCD failures. If the nonlinear loads exceed 15%, non-apparent negative consequences can result in the circuit. On the other hand, transients can be caused by external and internal influences. External transients can be produced in the line by travelling voltage waves produced by statistic charges; for example, negatively charged clouds can induce transient. Internal transients are produced by sudden changes in the circuit; then, unnecessary oscillation occurs due to the inductance and capacitance of the circuit.

3.3 *RCD's main nuisance is failure contributors*

(1) Residual current denotes the disparity in current flow between the live and neutral wires within an electrical circuit. Commonly referred to as leakage current, it arises when electricity travels back through an unintended route, circumventing the designated load. The presence of residual current raises safety alarms, as it may signify a ground fault [25], which can lead to potential electric shock and fire risks

(2) Higher frequency component harmonics and shorted period duration transient spikes generated by computer [23] equipment, power supplies, power converters, motors with speed regulators, and fluorescent lighting systems are among the main contributors. In addition, in the vicinity of high power switching devices and reactive energy compensation banks [14, 20]. Hence, part of these high-frequency currents flow to Earth/ground through the parasitic capacitances. These currents can cause the nuisance failure of differential current devices [14, 20]. The failure of differential current devices starts when an initial energization of the capacitances rises to high-frequency transient currents for a short duration; as shown in Figure 7, the transient current rises to 90% in about 0.5-microsecond duration.

(3) Electrical grids may experience overvoltage as a result of lightning strikes or sudden shifts in operational circumstances, leading to significant transient voltages and currents in circuits with inductive and capacitive components [12, 18]. As shown in Figure 8, transient voltage spikes to its maximum. The transient will cause frequency uncertainty due to harmonics. In addition, non-linear loads cause current and voltage distortion, leading the RCD to trip.

(4) Upon energizing the specified capacitances, rapid high-frequency transient currents are generated. This especially occurs in an IT-earthed system with the abrupt onset of an initial fault similar to a high-frequency transient earth leakage current, as the two unaffected phases experience a sudden increase in voltage relative to the earth.

(5) In addition, Transient currents may lead to voltage spikes, electromagnetic interference (EMI), and potential harm to delicate electronic parts if not adequately controlled or mitigated. Electrical networks can experience overvoltage

as a result of lightning strikes or sudden fluctuations in operating conditions. These abrupt changes frequently lead to significant transient voltages and currents within inductive and capacitive circuits.

(6) Moisture penetrates the electrical components, resulting in current leakage, which causes the RCD to trip. This moisture intrusion may originate from multiple sources. Moisture can disrupt the RCD's effective operation, leading to unwanted tripping events.

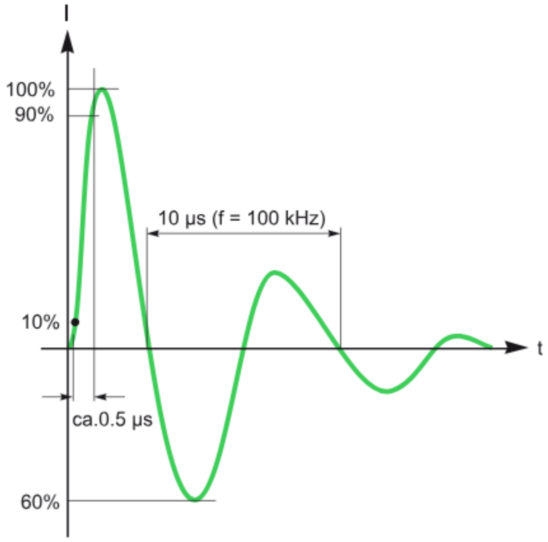

Figure 7. RCD sensitivity to the short duration of the transient current spike: The RCD's dynamic response characteristic during transient, SI-type RCD is designed to allow a small portion of spikes up to 0.5 µs. 90–100% of the short-duration spikes fall with the 0.5 µs. The source was adapted from https://www.electrical-installation.org/enwiki/SensitivityofRCDstodisturbances

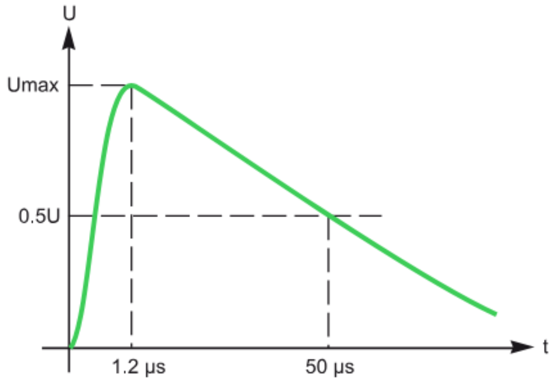

Figure 8. RCD, Common mode overvoltage nuisance tripping characteristics. The voltage rises sharply at the starting time, and its maximum is 1.2 µs. The overvoltage spike decays exponentially until it stabilises to a steady state after 50 µs. In this figure, the vertical axis is represented by the letter U, which represents the overvoltage. Source adapted from https://www.electrical-installation.org/enwiki/SensitivityofRCDstodisturbances

4. Design a circuit that interfaces with the safety residual current devices and the wireless Wi-Fi-controlled terminal socket outlets

This research paper investigates the drawbacks of RCD and designs a voltage-sensing circuit that is installed on each of the smart socket outlet terminals and current sensors in the main circuit breaker/RCD, as shown in Figure 4. Whenever failure happens, the circuit sends a remote alert signal to the responsible person through the Wi-Fi web application. The responsible person examines the status of the fault currents and then identifies whether the RCD is experiencing real earth leakage or one of the six nuisance undesired temporary tripping faults listed in Section 3.2; the RCD isolates the circuit to protect from electrical dangers; then, at this time, the responsible person can remotely analyses the type of fault and determine whether the fault is real or non-real using few steps. Step (1) reads the last fault current from the main circuit controller, resets the RCD, and attempts to identify the failure status. If the failure status cannot be analysed using the first step, move to the next step procedures. Step (2) Inject 5 VDC into the circuit while the RCD is in an off-position and read the status of the terminal socket outlets. Step (3) compares and identifies the fault terminal by reading the returning voltage from the injected 5 VDC from all terminal nodes. Step (4) if all socket outlet's terminal nodes read the same/slightly similar, break the neutral loop wire and supply the injected voltage to the nodes to read individually. Step (5) if the failure status is a nuisance failure, reset the RCD. Step (6) if the failure status is real, isolate the fault terminal only and reset the RCD to allow power to the rest of the subdivision terminals. Then wait for a response status. Step (7) fault is identified, and supply power is resumed to the other healthy terminals/nodes. Sensors of these healthy terminals should read similar voltages. If there is no failure in another terminal, the control circuit will send a notification. Step (8) if failures occur in more than one terminal, repeat the step procedures for each failure terminal. The main circuit in Figure 4 shows the RCD's practical presentation of these steps. As shown in the figure, the 5 VDC is supplied at the RCD terminal through the active wire and the earth wire. Hence, if there is a real earth leakage current, the leak current will be conducted from the active wire to the body of the appliances/devices and will return through the earth wire.

4.1 *RCD and sub-division line wiring method*

Assuming the RCD controls 4–12 socket outlets, as shown in Figure 3. According to AS/NZS3000 standard wiring rules. The minimum size cable is 2.5 m^2, and the maximum circuit breaker to protect the cable is 20 A. The current rating of socket outlets that can be connected to a 2.5 m^2 cable is 10 A, 15 A, or 20 A. Then, any current greater than 20 A passing through the circuit is automatically assumed overcurrent. Hence, the short current value depends on two parameters. The impedance and the base current of the circuit. These two parameters can be calculated using Ohm's law. During the fault, the impedance of the supply line goes near zero Ω. Perhaps it will be 1 Ω or less than 1 Ω [26]. Hence, the fault current will be increased [27] over the circuit breaker rating, in this case, over 20 A; then, it can be treated as a short current. For instance, the fault current increase for 20 A base current is 25 A, and for overcurrent, it can be treated with less than 25 A. These parameters can be programmed into the smart circuit controller, according to Table 1. Then, any current outside of these can be assumed to be a nuisance or earth-leakage current. In the case the fault is real, the circuit will isolate the socket outlet that is connected to the fault device remotely. This will allow the site to resume power to others and minimize a significant amount of production.

Table 1. The control unit must be coded with RCD overcurrent, short current, and nuisance current values

Type of Fault	10 A Rating	15 A Rating	20 A Rating
Earth leakage	E10	E15	E20
Short current	15 A	19 A	25 A
Over Current	11 A	16 A	21 A
Nuisance	N10	N15	N20

4.2 *The building's power supply maximum current is constantly monitored using a practical test study*

The main power supply current is constantly monitored using the current sensor component, as mentioned in Section 2.1. An electronic current is commonly used in industrial and commercial [18]. For the purpose of this study, the sensor is installed at the RCD infeed terminal, and the consumed maximum current passing into the building is measured. As shown in Figure 5, 10 A, 2400 W heating element is tested. Hence, the last current before tripping occurs can be recorded to identify the type of fault. The 10 A, 2400 W heating appliance is used for this study purpose, but in reality, the method can function with higher currents.

4.3 *Terminal line socket outlet node voltage and cable length resistivity measurement during the fault*

5 VDC is injected to identify the terminal voltage, which is donated as a terminal node. Injected voltage is measured during the fault occurrence and present using analog voltage sensor/detector devices, as shown in Figures 9 and 10. The sensor can detect up to 25 VDC [28], but for the purpose of this study, 5 VDC is used. This is to comply with the smart Wi-Fi-controlled socket outlet. The sensor is connected to the esp32 analogue input. Complying with ASZ/3000 wiring rules, the cable size that connected the main circuit breaker where the injected voltage is supplied to the socket outlet node is 2.5 mm^2, and its length is approximately 0.5 m.

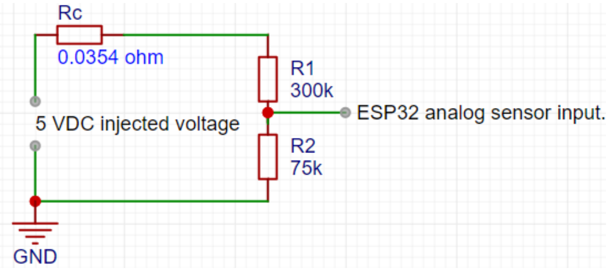

Figure 9. Injected voltage sensing resistance circuit

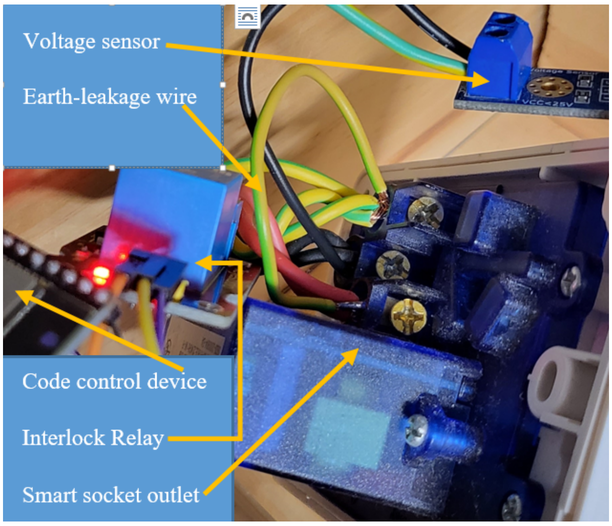

Figure 10. Smart socket out voltage interlocking method

$$\text{The resistance of the cable is } (\mathrm{R_c}) = \frac{\rho \mathrm{L}}{\mathrm{A}} \tag{4}$$

where $\mathrm{R_C}$ is the resistance of the cable, ρ is the resistivity of the cable, and A is the cable cross-sectional area. The resistivity of copper wire at standard temperature is 1.77×10^{-8} Ω/m. The cross-sectional area of 2.5 mm^2 converting in square meters is $(2.5)^2 \times \frac{1}{1000} = (2.5)^{-6}$

$$R = \frac{1.77 \times 10^{-8}}{2.5^{-6}} \times 0.5 = 0.0354\ \Omega \tag{5}$$

The inject circuit cable resistance is in series with the sensor voltage divider resistor (R_1 = 300 k and R_2 = 75 k), as shown in Figure 9. The voltage drop with the 0.5 m is V_d = 00000472 V. Hence, the drop voltage is not significant; it has been assumed to be a lossless circuit. However, for non-research projects, it is necessary to consider that the length of the cables increases by a factor of 20 or 30. Remote fault identification was conducted with respect to time (t), as shown in Table 2 and Section 2.2. At t <= 30 s, 5 VDC is injected into active and earth wires, and then the reading from the sensor is examined. At t < 60 s, the signal is sent to break the neutral-wire loop. Then, the readings from the sensors are examined again to identify the fault node.

Table 2. Socket outlet node fault identification method, where t is the testing/measuring time

Node number	At t = 0	At t = 30 a	Fault status
1	5 V	5 V	Fault exist
Activate the push button to disconnect the neutral wire loop at t < 60 s			
2	5.16 V	0.16 V	No fault
3	5.15 V	0.16 V	No fault
Second trial			
1	5 V	5 V	Fault exist
Activate the push button to disconnect the neutral wire loop at t < 90 s			
2	5.16 V	0.16 V	No fault
3	5.16 V	0.16 V	No fault
Third trial			
1	5.16 V	5.16 V	Fault exists
Press the button to disconnect the wire loop at t < 120 s			
2	5.16 V	0.14 V	No fault
3	5.16 V	0.16 V	No fault

5. Smart Building's electrical wiring performance improvement, contribution and discussion

Re-designing the safety, RCD and wireless Wi-Fi-controlled socket outlets will reduce the current failure breakdown time, such as in pharmaceutical manufacturing factories, food industries, hotels, and restaurants, where cold store fridges could lead to significant production reduction when failure time in the RCD increases. A machine with a higher availability assures higher production. It signifies that the machine is consistently operational during production periods, whereas nuisance equipment failures can negatively impact its availability. Machine effectiveness is determined mostly by multiplying the scores of availability, quality, and performance. A machine exhibiting a higher effectiveness score of efficiency operates with minimum or negligible defects. Moreover, implementing the re-designed RCD and WiFi-controlled smart socket outlet circuit will contribute to the positive mitigation of Smart Building drawbacks related to electrical device performance evaluations.

Further study, discussion and evaluation of RCD's nuisance tripping issues. A number of researchers have shown interest in developing mitigation methods that can improve RCD's nuisance tripping characteristics caused by high-frequency transient currents. RCDs are sensitive to a higher frequency. However, RCDs fail to trip the test when the high frequency is pure tone. This is proven by a recent study that conducted measurement tests on various types of RCDs using 4 to 40 KHz [29] and frequency mapping methods to examine the spectrum uncertainty of residual current (RC) for non-fundamental frequency. The study indicates that the primary cause of nuisance tripping is not the transient spike itself [15, 23]. The main cause of the trip is the magnitude of the transient current combined with its duration. In addition, the frequent occurrence that results in nuisance tripping is the inrush currents. When electrical loads are powered ON after being on OFF-state for a while, the resulting inrush current can be greater than the normal steady-state current. This is true for de-energized equipment, which is normally either cold or possesses low impedance, which leads the transient current to drift in higher amounts. Improvement to overcome the current rush is in progress, especially for the new RCD design. Moreover, several studies have conducted mitigation to improve nuisance tripping. For instance, a research paper published this year focused on the study of a three-phase nonisolating transformer electric vehicle charger. The study uses AC/DC and the Current Source Rectifier (CSR) circuit that switches the Pulse Width Modulation (PWM). The PWM switching process uses the third harmonic injection method, which generates the low frequency (LF) common mode (CM) currents via the parasitic capacitor of the DC output circuit, which could be over the RCD's threshold amount. To overcome LF CM, the study developed a virtual control circuit that suppresses the LF CM to the ground before approaching the RCD's circuit [29]. Similarly, a recently published study developed a method of DC output parameter limitation that filters out the average leakage currents [30]. The method helps RCDs to improve the rate of tripping. Another similar study focused on lighting strike transient spike developed an Auto-reclosing RCD circuit [31]. The circuit helps to recover from nuisance tripping but fails to consider serious real earth leakage. Thus, this study's mitigation method differs from other studies' methods in that it provides comprehensive coverage of the RCD's failure.

For example, assume a particular pharmaceutical cold store has five machines connected from one line connected to one RCD via five socket outlets. Assume that the machines also store products that require a specific temperature tolerance range, and any temperature outside the specific range is intolerable. For the purpose of this study, two scenarios are conceptually attempted, and in both scenarios, each machine temperature is set differently as the machine stores different products that require different temperature specifications. In the first scenario, these five machines experience RCD nuisance failure during the night when there is no technician or operator on site to reset the RCD. Let's assume the plant is implemented with advanced technology that sends an alert message to the responsible technician. By the time the technicians receive the message and drive to the site, the temperature of the products increases by 5 °C above the allowed upper tolerance, as shown in Figure 11 by the yellow colour. All the products incurred production loss, whereas in the second scenario, the technician reset the RCD nuisance fault remotely, and only a 1 °C temperature rise occurred. Except for one machine, which has the lowest upper-temperature tolerance, as shown in Figure 12 number 3, the other machines are within the allowed temperature.

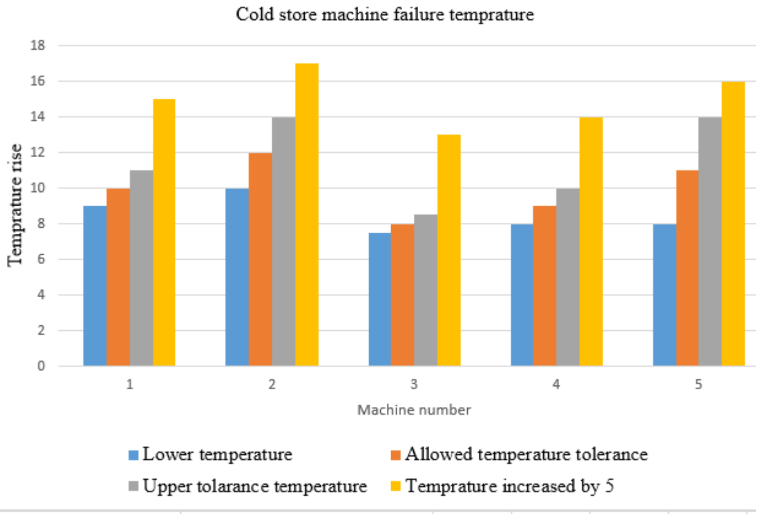

Figure 11. The temperature of a pharmaceutical cold store machine that is experiencing nuisance failure rises by 5 °C until rested manually. The temperature rise goes beyond the upper limit tolerance in all machines. Incurred to significant production loss

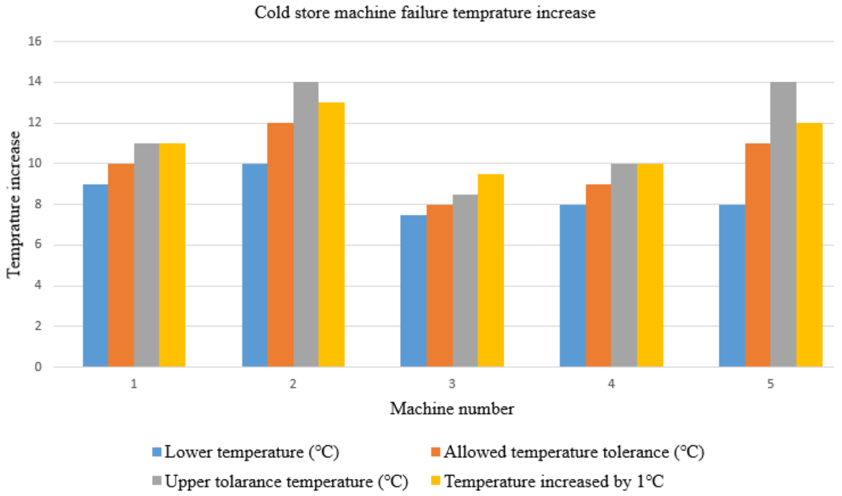

Figure 12. The temperature of a pharmaceutical cold store machine experiencing nuisance failure rises by 1 °C until reset remotely. The temperature rise goes beyond the upper limit tolerance in machine 3. All other machines have a limit. Production loss is incurred only in one machine

6. Conclusions

Smart Buildings minimize occupant activities due to the building being assisted by a computerized automation network, i.e., dynamic, interoperable responses with limited human physical interaction actions. In addition, smart commercial building offers more convenient, productive, secure and comfortable business. However, Smart Building experiences a number of drawbacks that require mitigation. One of the drawbacks from the electrical side is the RCD nuisance tripping, which this study is developed failure time minimizing a mitigation method. Further, this research paper has attempted to investigate the failure characteristics of RCD that are caused by influencing higher frequencies, distorted harmonics, and transients, especially related to nuisance tripping. Hence, these failures were classified as drawbacks of the Smart Building. In response, the research developed a mitigation method that interfaces with the safety, RCD, and wireless Wi-Fi-controlled terminal socket outlets to investigate, identify the failure type and reset remotely caused by real or nuisance faults. The designed circuit will be useful in pharmaceutical cold stores, food industries, restaurants, and hotels, where cold store fridges could lead to significant production loss/reduction when failure time increases. The circuit was practically tested using three smart socket outlets, three voltage sensors, two linear actuators and one current sensor. The measured values of these sensors are remotely monitored, and a test was conducted to identify which, in response, to isolate the faulty devices connected to the socket outlet or to isolate the socket outlet itself. Hence, this allows the fast recovery of power to the other healthy socket outlets.

Fault investigation in commercial complex wiring is a series of issues that consume time and incur production loss. The fault analysing method and the fast power supply recovery process are knowledge contributions of this study, and it is significant improvements for nuisance RCD tripping.

Conflict of interest

The authors declare that there are no conflict of interest.

References

[1] "Building Automation System Market Estimated to Garner $194,864.1 Million and Grow at 10.0% CAGR in the 2022 to 2030 Forecast Period | Report [300-Pages] by Research Dive," in *China Weekly News*. Atlanta, GA, USA: NewsRX LLC, 2022, p. 933.

[2] *Commercial Building Automation Market to Rise at CAGR of 8.3% During Forecast Period, Observes TMR Study*. New York, NY, USA: PR Newswire US, 2022.

[3] C. Stanislaw, "Testing Sensitivity of A-Type Residual Current Devices to Earth Fault Currents with Harmonics," *Sensors*, vol. 20, p. 2044, 2020.

[4] "Building Information Modeling Market Growing at 11.2% CAGR to Reach $22.9 Billion by 2034 | Fact.MR Study," in *Information Technology Newsweekly*. Austin, TX, USA: NewsRX LLC, 2024, p. 105.

[5] R. A. Abdelouahid, O. Debauche, and A. Marzak, "Internet of Things: a new Interoperable IoT Platform. Application to a Smart Building," *Procedia Comput. Sci.*, vol. 191, pp. 511–517, 2021.

[6] D. Djenouri, R. Laidi, Y. Djenouri, and I. Balasingham, "Machine Learning for Smart Building Applications," *ACM Comput. Surv.*, vol. 52, no. 2, pp. 1–36, 2019.

[7] T. Su, H. Li, and Y. An, "A BIM and machine learning integration framework for automated property valuation," *J. Build. Eng.*, vol. 44, p.102636, 2021.

[8] E. Simeoni et al., "A Secure and Scalable Smart Home Gateway to Bridge Technology Fragmentation," *Sensor*, vol. 21, no. 11, pp. 3587–3587, 2021.

[9] N. Zaeri, A. Ashouri, H. B. Gunay, and T. Abuimara, "Disaggregation of electricity and heating consumption in commercial buildings with building automation system data," *Energy Build.*, vol. 258, p. 111791, 2022.

[10] S. Yasuda, "The Design and Application of a Mimetic Network Environment Construction System Security Verification Environment Building System and Contribution to Human Resource Development," *J. Natl. Inst. Inf. Commun. Technol.*, vol. 63, no. 2, pp. 93–101, 2017.

[11] *Entertainment Everywhere: Streaming Media Players (Also Known as Digital Media Receivers) Let You Move Multimedia Files throughout Your Home over a Wireless or Ethernet Network*. Melbourne, VIC, Australia: Victoria University, 2007, pp. 92–114.

[12] G. Zhang, Y. Li, and X. Deng, "K-Means Clustering-Based Electrical Equipment Identification for Smart Building Application," *Information*, vol. 11, no. 1, p. 27, 2020.

[13] V. Gurevich, "RCD nuisance tripping: who's guilty and what needs to be done?," *Radio Electron. Comput. Sci.*, vol. 2, no. 29, pp. 7–16, 2014, https://doi.org/10.15588/1607-3274-2013-2-1.

[14] P. Xie, Z. Fang, J. Hu, J. Yang, and G. Zhu, "Tripping Characteristics of Residual Current Devices Under Different Working Conditions," in *Proc. 2019 IEEE 3rd Conf. Energy Int. Energy Syst. Integr. (EI2)*, Changsha, China, Nov. 8–10, 2019, pp. 2765–2769.

[15] X. Luo, Y. Du, X. H. Wang, and M. L. Chen, "Tripping Characteristics of Residual Current Devices Under Nonsinusoidal Currents," *IEEE Trans. Ind. Appl.*, vol. 47, pp. 1515–1521, 2011.

[16] Y. Xiang, V. Cuk, and J. F. G. Cobben, "Impact of residual harmonic current on operation of residual current devices," in *Proc. 2011 10th Int. Conf. Environ. Electrical Eng.*, Rome, Italy, May 8–11, 2011, pp. 1–4.

[17] Z. Wang et al., "A leakage protection method for low-voltage power supply systems based on flexible regulation of the neutral point voltage," *Int. J. Electr. Power Energy Syst.*, vol. 151, 2023, https://doi.org/10.1016/j.ijepes.2023.109157.

[18] O. S. Shereefdeen, O. O. Kehinde, and M. Ismail, "Design and Implementation of Home Appliance Energy Monitoring Device," *Int. J. Electr. Energy Power Syst. Eng.*, vol. 2, pp. 1–6, 2019.

[19] L. Xiang, Y. Du, X. H. Wang, and M. L. Chen, "Tripping Characteristics of Residual Current Devices Under Nonsinusoidal Currents," *IEEE Trans. Ind. Appl.*, vol. 47, pp. 1515–1521, 2011.

[20] A. Szczesny and E. Korzeniewska, "Validation of the method for measuring the effectiveness of residual current protection," in *Proc. 2019 Appl. Electromagn. Mod. Eng. Med.*, Janow Podlaski, Poland, Jun. 9–12, 2019.

[21] S. Czapp and K. Borowski, "Verification of safety in low-voltage power systems without nuisance tripping of residual current devices," *Electric Power Syst. Res.*, vol. 172, pp. 260–268, 2019.

[22] C. Roldan-Porta, G. Escriva-Escriva, F.-J. Carcel-Carrasco, and C. Roldan-Blay, "Nuisance tripping of residual current circuit breakers: A practical case," *Electric Power Syst. Res.*, vol. 106, pp. 180–187, 2014.

[23] G. Escrivá-Escrivá, C. R. Porta, and E. C. W. De Jong, "Nuisance tripping of residual current circuit breakers in circuits supplying electronic loads," *Electric Power Syst. Res.*, vol. 131, pp. 139–146, 2016.

[24] E. Zamiri, A. Sanchez, M. S. Martínez-García, and A. de Castro, “Analysis of the aliasing effect caused in hardware-in-the-loop when reading PWM inputs of power converters,” *Int. J. Electr. Power Energy Syst.*, vol. 136, p. 107678, 2022.

[25] G. Escrivá, C. Porta, and E. de Jong, “Nuisance tripping of residual current circuit breakers in circuits supplying electronic loads,” *Electric Power Syst. Res.*, vol. 131, pp. 139–146, 2016, https://doi.org/10.1016/j.epsr.2015.10.012.

[26] L. Neamt, A. Neamt, and O. Chiver, “Improved Procedure for Earth Fault Loop Impedance Measurement in TN Low-Voltage Network,” *Energies*, vol. 14, no. 1, p. 205, 2021, https://doi.org/10.3390/en14010205.

[27] F. Möller, A. M. Blanco, and J. Meyer, “Characteristic leakage current of household devices and their impact on the tripping behaviour of residual current devices,” *Electric Power Syst. Res.*, vol. 214, p. 108832, 2023, https://doi.org/10.1016/j.epsr.2022.108832.

[28] C. N. Oton and M. T. Iqbal, “Low-Cost Open Source IoT-Based SCADA System for a BTS Site Using ESP32 and Arduino IoT Cloud,” in *Proc. 2021 IEEE 12th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Dec. 1–4, 2021, pp. 681–685.

[29] D. Zhang, D. Cao, J. Huber, J. Everts, and J. W. Kolar, “Nonisolated Three-Phase Current DC-Link Buck-Boost EV Charger With Virtual Output Midpoint Grounding and Ground Current Control,” *IEEE Trans. Transp. Electrification*, vol. 10, pp. 1398–1413, 2024.

[30] S. Erwin, K. Ain, M. Aziz, and G. EscrivÁ-EscrivÁ, “A Study on DC Limit Parameters in RCD Operation Using Capacitor,” *J. Eng. Sci. Technol. Rev.*, vol. 12, no. 4, pp. 7–14, 2019, https://doi.org/10.25103/jestr.124.02.

[31] Y. Liu and R. Chen, “Application of auto-reclosing residual current device in lightning protection for communications power supply,” in *Proc. 2017 IEEE 5th Int. Symp. Electromagn. Compat. (EMC-Beijing)*, Beijing, China, Oct. 28–31, 2017, pp. 1–2, https://doi.org/10.1109/EMC-B.2017.8260379.