

The paper presents the development of a microprocessor-based relay protection device on open architecture. Currently, there is a problem with modern microprocessor relay protection: the impossibility to replace the damaged element with alternatives from other manufacturers. The solution to this problem is the use of devices with open architecture. The study developed a structural model of a microprocessor-based relay protection device based on an open architecture with the industrial Internet of things application. Open architecture is achieved through open protocols and the principle of modularity. The industrial Internet of things technology transfers the control action of triggering blocking. A microprocessor-based relay protection device prototype based on an open architecture was developed. The simulation of the developed device was conducted. The appearance of higher harmonics and aperiodic components in the short-circuit current was not considered during modeling. Due to the study's limitations in the form of lack of load, current and voltage sensors, such as Hall sensors, and inductance coils, the subject of this study is only the speed of operation. A high multiplicity current generation setup was assembled for experimental testing. The developed relay protection device on an open architecture trips faster than the traditional solution. The application of the Internet of Things allowed it to ensure the blocking of non-selective tripping. The obtained results are provided by structural simplification compared to traditional solutions and speed of information transfer with the application of the Internet of things. The developed open architecture device with the industrial Internet of things technology application gives new possibilities for relay protection systems, including flexibility to meet the requirements in connection with the introduction of distributed power

Keywords: protective relay, actuation speed, reed switch, magnetic field, open source, industrial internet of things, electric experimental installation

UDC 621.316.91
DOI: 10.15587/1729-4061.2023.276588

DETERMINATION OF THE SPEED OF A MICROPROCESSOR RELAY PROTECTION DEVICE OF OPEN ARCHITECTURE WITH A REED SWITCH AND THE INDUSTRIAL INTERNET OF THINGS

Alexandr Neftissov

Corresponding Author

PhD, Associate Professor*

E-mail: shurik-neftissov@mail.ru

Assiya Sarinova

PhD, Associate Professor*

Ilyas Kazambayev

Doctoral Student*

Lalita Kirichenko

Doctoral Student*

Oleksandr Kuchanskyi

Doctor of Technical Sciences, Head of Department

Department of Information Systems and Technology

Taras Shevchenko National University of Kyiv

Volodymyrska str., 60, Kyiv, Ukraine, 01033

Adil Faizullin

Master of Technical Sciences, Director of Department

Department of Strategy and Corporate Governance**

*Research and Innovation Center "Industry 4.0"***

**Astana IT University

Mangilik sq., expo C1, Astana,

Republic of Kazakhstan, 010000

Received date 24.01.2023

Accepted date 29.03.2023

Published date 28.04.2023

How to Cite: Neftissov, A., Sarinova, A., Kazambayev, I., Kirichenko, L., Kuchanskyi, O., Faizullin, A. (2023). Determination of the speed of a microprocessor relay protection device of open architecture with a reed switch and the industrial internet of things. *Eastern-European Journal of Enterprise Technologies*, 2 (9 (122)), 20–30. doi: <https://doi.org/10.15587/1729-4061.2023.276588>

1. Introduction

Relay protection is necessary to disconnect faults in an electrical supply network in an emergency. The relay protection provides an opportunity to obtain a stable and safe power supply.

Analyzing the applied systems and devices, we can conclude that these solutions based on closed solutions (proprietary) have some disadvantages in practice. For example, if one element (module) of the system or relay protection device fails, there is no possibility to replace it with alternative elements (modules) of another manufacturer. Also, in connection with the constant

progress and development of technology, it happens that when an element (module) of the device or system installed a couple of years ago fails, it is impossible to find the necessary replacement element due to the change of generations of solutions from the manufacturer. In this case, the only thing left is to update the whole set of equipment.

A current trend is to build solutions based on open protocols and interfaces. So, for relay protection, the way out of this situation is to build a system based on open standards. This approach has successful cases in telecommunication solutions – Open RAN and software – Open Source. Therefore, this direction is relevant.

2. Literature review and problem statement

According to the analyzed literature, [1] proposes intelligent microprocessor relay protection (MRP) based on an impedance plane constructed according to local measurements and the Thevenin method. The calculation is based on the pick-up current, considering which the equivalent voltage is determined, which allows calculating the complex resistance. The advantage of the solution is the ability of the device to adapt to changes in the power supply scheme, as shown in the results. However, not enough attention has been given to the experimental study. Within this solution, the primary measuring devices can only be current transformers. It is known that redundancy is used to increase reliability. It is essential to duplicate the relay protection device and the primary transducer to increase reliability, which must function on a different principle. One of the possible variants can be reed switches.

The known device based on an open architecture is made on the XILINX Zynq7000 FPGA platform [2]. It allows the replacement of modules with alternatives from other manufacturers. In addition, the proposed solution showed high accuracy, low latency of the device, and low implementation cost. Perhaps because it is still only a development, the application of the Internet of Things has not yet been considered.

For example, [3] presents a technology for a SIEMENS protection device that allows IoT for predictive analytics to predict malfunctions and determine their nature.

The construction of relay protection devices and systems with closed interfaces affects maintenance and repair. If one module of the device fails, purchasing a new complete set is often necessary. This is due to the renewal of generations of equipment and certain difficulties for maintenance personnel. Proprietary solutions are advantageous for the manufacturer due to the availability of further customer dependence. The solution uses only a wired communications interface. And the reduced use of the Internet of things, more precisely sending data to the server for storage and display and not using it to decide on the actuation, does not allow the construction of new flexible algorithms to meet the requirements in connection with the introduction of distributed power.

In [4], one of the ways to reduce the errors of CTs in measurement using a comparator was considered. The study showed an increase in the accuracy of measuring transformers, but this approach complicates the design and increases the cost.

The solution [5] considers a more advanced method based on current measurements of higher harmonics. The advantage is the determination of harmonics, which are the primary source of errors in measuring CT. However, the disadvantage is that the construction of the device is more complicated and expensive than the one considered earlier.

To simplify the design of the measuring device, a computing device to process the analog signal by the extended Kalman filter algorithm can be used [6]. The method is based on analyzing the influence of higher harmonics on the sinusoidal waveform. The advantages are a simplified design in comparison with the previous solutions and high measurement accuracy. However, this error reduction method requires additional computational resources, and it is worth noting that the research was conducted only in laboratory conditions. Thus, evaluating the effectiveness of the extended Kalman filter is difficult since the calculation

process may become several times more complicated during the implementation in a working plant.

For the above reasons and because of the high cost of CTs, research is actively being conducted to find a cheaper alternative. One such solution is using a reed switch to build busbar protection [7]. The measuring principle is carried out by determining the short-circuit current by the magnetizing force, depending on the distance of the reed switch installation.

For example, [8] presents a solution for motor protection based on a reed contact trip time comparison of phases. The advantages are the versatility of the approach, allowing to use other sensors, and the ability to detect coil faults, preventing more significant accidents. The disadvantages of this solution are the effect of contact inertia, limiting the time measurement range, and sensitivity to electromagnetic interference, which has more influence than ones of standard solutions.

It is worth noting that most solutions for building microprocessor relay protection on reed switches are not universal. Despite this, in [9] it was noted that the development of these sensors for the construction of overcurrent protection and distance, differential, directional, and other types of protection is possible. The advantage of the solution is the replacement of current transformers for most relay protection devices, which simplifies the design in weight and size, as well as the high accuracy of short-circuit detection. At the same time, most relay protections, built on reed switches, implemented only the function of protection tripping for various types of short circuits. This is a disadvantage in relation to transformers and Hall sensors, which can measure current and voltage.

For example, the distributed installation of Hall sensors in a circle at some distance from the current conductor allows you to calculate the current by the average of the measurements from all the sensing elements [10]. The advantages of this device are high measurement accuracy and the possibility to install the current conductor in any position inside the circle, which means it can be located not only in the center of the structure.

Another solution is using magnetoresistive sensors as a bridge circuit [11]. The advantages of this solution are the simplicity of design and high measurement accuracy. However, there is still a need for research to say definitively about the advantages and disadvantages. A solution that considers these cases is the use of reed switches to build a device for measuring current [12]. Moreover, the principle of operation is based on the determination of the time of the contact in the closed state, based on which the current is calculated. The advantages are the high measurement accuracy, providing short-circuit detection speed. The disadvantage is the dependence of the response speed on the parameters. The application of the Internet of things has not been considered in the known works on the construction of relay protection on reed switches.

Thus, having analyzed literature sources, the traditional solutions of microprocessor relay protection are built based on proprietary solutions that have closed interfaces, which limit the possibilities of new developments to a wide range of developers. This also affects the replacement of damaged modules. There is no possibility to install alternative modules from other manufacturers. The construction of relay protection devices is based on obtaining information from current measuring transformers, which are expensive and

metal-intensive and can have significant saturation errors. It is necessary to be able to duplicate not only relay protection devices but also primary converters, which will have a different principle of operation, different from the measuring current transformers, to increase the reliability of power supply. Only wired interfaces limit the capabilities of relay protection systems in modern conditions. In some solutions, the application of the industrial Internet of things is considered only for additional functions and does not participate in decision-making, which does not allow the application to use all its capabilities. The problems mentioned above and unresolved issues are covered by the material presented in this study.

3. The aim and objectives of the study

The aim of the study is to determine the actuation speed of an open architecture microprocessor relay protection device with the use of a reed switch and industrial Internet of things technology to make a decision on the operation.

This will open a new direction of development of relay protection on reed switches, including for the distributed power industry. It will increase the reliability of power supply during duplicating not only relay protection systems but also duplicating primary converters. This will make it possible to develop a reed-based relay protection system based on an open architecture with the application of industrial internet of things technologies, precisely to participate in decision-making about triggering.

To achieve the aim, the following objectives were set:

- to build a structural model of a microprocessor-based relay protection device based on an open architecture with the application of industrial internet of things technology;
- to develop a microprocessor-based relay protection device based on an open architecture with the application of industrial internet of things technology;
- to perform modeling and experimental testing of the microprocessor-based relay protection device based on an open architecture with the application of industrial internet of things technology to evaluate its performance.

4. Materials and research methods

The object of the research is a microprocessor relay protection device. This study investigated the possibilities of building a microprocessor relay protection device based on open-source protocols and the possibility of using IIoT technology in relay protection.

The basic principles of graph theory, the theoretical foundations of electrical engineering, electromagnetic transients, electronics, relay protection subjects, and the Bio-Savara-Laplace law were used to solve the first task.

The basic principles of circuit engineering, electronics, relay protection, Bio-Savara-Laplace law, IEC-60870-5,

IEC-61850, RS-485, UART, and IoT standards, were used to solve the second task.

During the implementation of the third task, the basics of statistics, mathematical and physical modeling, software programs Matlab Simulink, Comsol Multiphysics, as well as equipment: oscilloscope GDS-71054B, load transformer NT-2500, digital device relay protection and automation Altey-01, autotransformer (LATR) RESANTA TR/2 (TDGC2-2) were used.

The following assumptions were made during the study: the short-circuit current does not contain higher harmonics and an aperiodic component. At the same time, simplifications were adopted, considering that the operation of the reed switch was not affected by the electromagnetic fields of other installations.

5. Results of research development of microprocessor relay protection

5.1. Structural model of microprocessor relay protection based on an open architecture

The entire process of microprocessor-based relay protection consists of measuring analog signals using current and voltage transformers, which are then filtered using special modules. After filtering, the values are error-corrected for analog-to-digital conversion (ADC). The transformed values are processed and used for calculation by a microprocessor, which makes a decision, considering the task and conditions. Based on this sequence, a process flowchart was developed (Fig. 1).

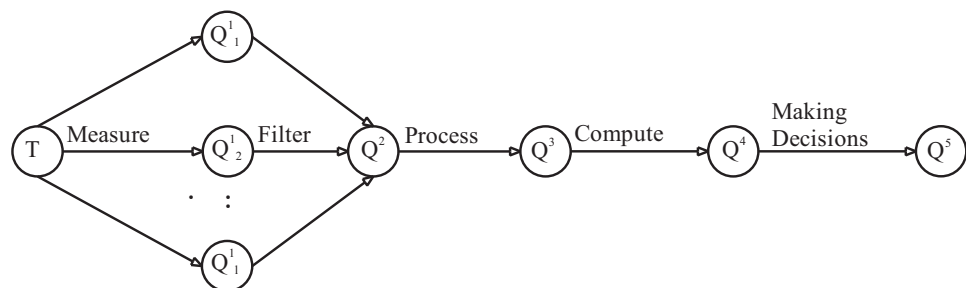


Fig. 1. Structural model of a microprocessor relay protection device

As part of the development, instead of the traditional measurement of the current value, time acts as a measurement parameter, or more precisely the set of moments T . The measurement process is based on determining those elements T at which the contact of the reed switch 1 is closed (Fig. 2). Moreover, the reed contact has the property of inertia, which leads to contact bounce.



Fig. 2. Reed switch with pins 1 and 2

For this reason, the measurement results form many sets of different time moments q_{1i} . Therefore, the filtering based on the RS-trigger (Fig. 3) is chosen to separate the elements of the sets q_{1i} , as well as to combine the elements at which the contact is closed. As a result, the output of this process forms the set q_2 .

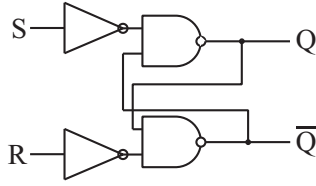


Fig. 3. RS Flip-Flop

Then the time intervals at which contact 1 was closed are calculated from the obtained set, which forms the set q_3 . Based on elements of q_3 and setting the rule of selection of elements of the set, we calculate the current, the values of which are the elements of the set q_4 . Given q_4 and the presence of interlocking, the set q_5 , consisting of ones and zeros, is formed, which determines the state of the tripping signal of the circuit breaker. Mathematically the presented structural scheme can be written as follows.

The principle of the device is to measure time that can be expressed as a set of moments of time:

$$T = \{t_0, t_1, t_2, \dots, t_n\}, \quad (1)$$

where t_0 – initial moment of time.

The measurement starts when contact 1 of the reed switch trips. Considering that due to the inertia of the reed contacts, a bounce occurs, during which the contact with the small period closes and opens. Moreover, the time, during which the contacts were closed, will be varying. For this reason, instead of one whole set, many sets are generated. Consequently, sets of moments of time after contacts have closed can be written as follows:

$$\begin{cases} (Q^1 \subset T) = \bigcup_{i=1}^k Q_i^1 = \{t_i \in T | x(t_i) = 1\}; \\ i = \{j, j+1, j+2, \dots, m\}, \end{cases} \quad (2)$$

where $x(t_i)$ is a logical value, which equals 1 ($x(t_i)=1$), if the launch took place, and equals 0 ($x(t_i)=0$), if the launch did not occur; k is the amount of the sets created from contact bouncing; t_j is the element of minimum value from (1), during which the contact 1 is closed; t_m is the element of the maximum value from (1), during which the contact 1 is open.

In order to eliminate this disadvantage, an anti-bounce circuit is used based on the RS Flip-Flop. Moreover, pin 1 is connected to the S -input, and pin 2 to the R -input. The direct output Q starts the timer.

Thus, the set of moments of time, according to which the current is measured, is determined by the following expression:

$$Q^2 = \{t \in T | y(t) = 1\} = \{t_j, t_{j+1}, \dots, t_p\}, \quad (3)$$

where $y(t)$ is the output of the anti-bounce circuit.

Moreover, the set's minimum value t_t is when contact 1 is tripped, and the maximum value t_r is when contact 2 is tripped:

$$\begin{cases} t_t = \min(Q^2); \\ t_r = \max(Q^2). \end{cases} \quad (4)$$

It is worth noting that the values obtained in (4) can vary and cannot be predicted. Therefore, the set of the

difference between maximum and minimum values can be written as:

$$Q^3 = \{t' \in T_1 | t' = t_r - t_t\}, \quad (5)$$

where T_1 – set of difference of moments in time when the measurement is made.

Knowing this parameter, the magnetic sensor is placed at the necessary distance, and the reed switch's trip current I_t and return current I_r are determined. Thus, using the values obtained and applying (5), we can determine the current amplitude by the formula [12]:

$$I_m = \frac{\sqrt{I_t^2 + I_r^2 - 2I_t I_r \cdot \cos(\omega t')}}{\sin(\omega t')}. \quad (6)$$

Consequently, the set of current amplitude values can be written as follows:

$$Q^4 = \left\{ I_m \in I \mid I_m = \frac{\sqrt{I_t^2 + I_r^2 - 2I_t I_r \cdot \cos(\omega t')}}{\sin(\omega t')} \right\}, \quad (7)$$

where I is the set of all possible values of current.

The values obtained in (6) are then compared with the set point, and if the current surpasses this value within the set point, and if the current surpasses this value within the set time and provided there is no blocking, then a logic signal will be 1. The blocking signal is transmitted via IIoT. Thus, the circuit breaker tripping signal can be written as:

$$A = \begin{cases} 1, & \text{if } I_m \geq I_s; \\ 0, & \end{cases} \quad (8)$$

where I_s – current set point.

Given (8), the signal to turn off the switch can be written as a logical expression using Boolean algebra:

$$Q^5 = A \cdot \bar{B} \cdot D_t, \quad (9)$$

where B – signal for blocking, D_t – logical time delay.

Decision-making takes place directly on the device where processing and computation take place. However, there is the possibility of influence in the logic chain through the industrial internet of things.

5. 2. Development of a microprocessor relay protection device based on an open architecture

The designed structural model of the microprocessor-based relay protection device was used for development (Fig. 1). According to the developed structural model, the initial data is generated with the help of a reed switch, more precisely the time of the closed state of its contacts, which should be measured. The measurement is made from the reed switch contacts with a frequency of 100 Hz. The filtering process is implemented by eliminating the contact bounce of the reed switch contacts using an RS Flip Flop-based anti-bounce circuit. Thus, a clean signal passes on in the form of pulses. The cleaned data are fed to the microcontroller. The designed device uses an ESP 32 series microcontroller, which performs calculations. Then the data is sent using the industrial internet of things to the database, and the data can also be retrieved, for example, to make a decision considering the received data. The schematic is shown in Fig. 4.

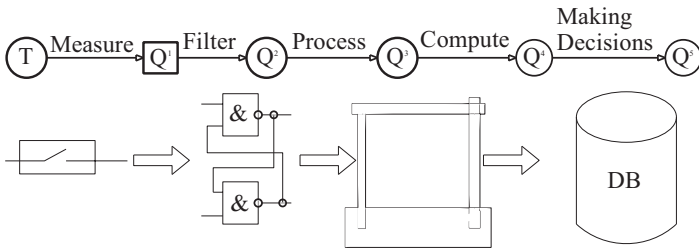


Fig. 4. Implementation diagram of the developed microprocessor-based relay protection system

relay protection system based on an open architecture with the application of industrial internet of things technology. Moreover, the measurement module allows processing data from Hall sensors and current and voltage transformers or reed switches. The calculation, processing of incoming data, and decision-making are performed in the computing module. The system is visualized and configured locally via the HMI. At the same time, inputs can be processed binary signals, and control signals can be generated by outputs via the Input/Output module. Simultaneously with the control inputs, data are transmitted wirelessly to a server for blocking, analytics, and remote monitoring.

Fig. 5 shows the result of the development of the hardware and software complex, which will allow implementing the task. There are data collection, processing, transmission, and reception. Edge nodes transmit information about current, voltage, and frequency parameters. The edge nodes send the collected data to the hub, a device that collects, processes, and analyzes information from neighboring devices and sends it over a Wi-Fi network to the Backend Service. Then the data goes to the database, where the Front-end visualizes it. ESP-NOW is used as a wireless communication protocol.

The designed data flow diagram is shown in Fig. 6. There is the process of acquiring, storing, and displaying data. First, the data comes to the backend server from the hub via Wi-Fi in JSON format. The data includes the state of the reed switch (open/closed), measured current, triggering, and return currents. The information is inserted into the database from the backend endpoint using the INSERT operation. Then, when the user requests, the required information will be taken from the database using the SELECT data(filter) function and transferred to the Frontend chart.js. As a result, the selected data is sent to the graphics engine to create a visualization. At each stage, the integrity of the information is diagnosed by returning a successful completion code if the data transmission was completed, otherwise, an error code will be returned.

Open interfaces will allow smaller companies to make solutions and enter the market. Fig. 7 shows the designed structural model of the developed microprocessor-based

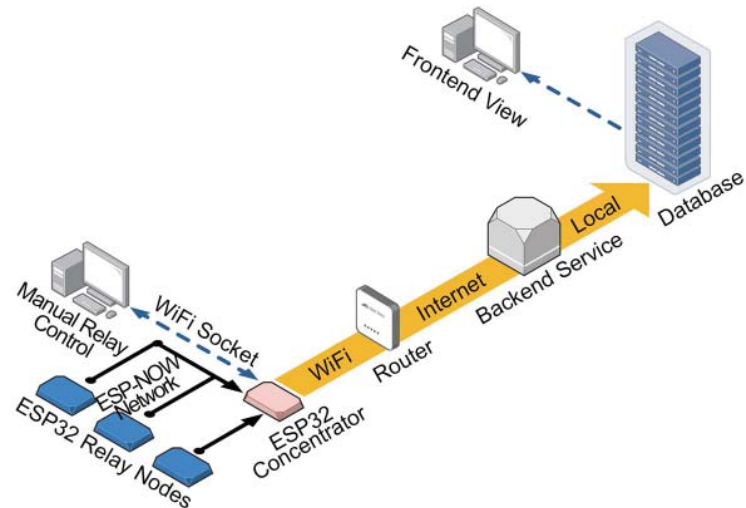


Fig. 5. Block diagram of the hardware and software complex

We would like to note that the designed structure will allow applying the internet of things directly to relay protection device operation.

Considering the peculiarities of relay protection design, the openness of the architecture is achieved by using interfaces based on international standards IEC 60870-5, IEC 61850, RS-485, UART (RX/TX standards) or I2C, SPI to transmit data between modules of the device, as well as wireless interfaces to enable cloud technology application.

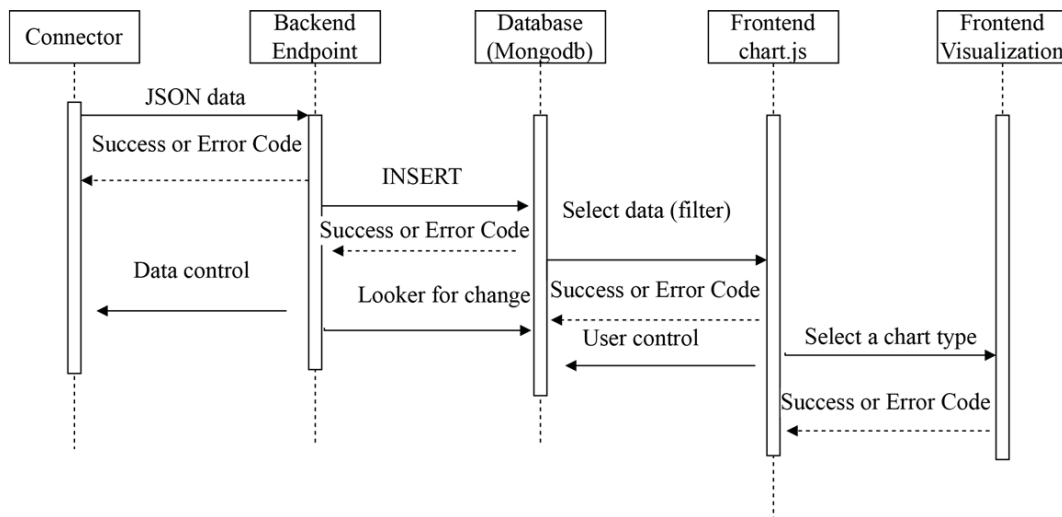


Fig. 6. Diagram of information flows from the field level to the front-end

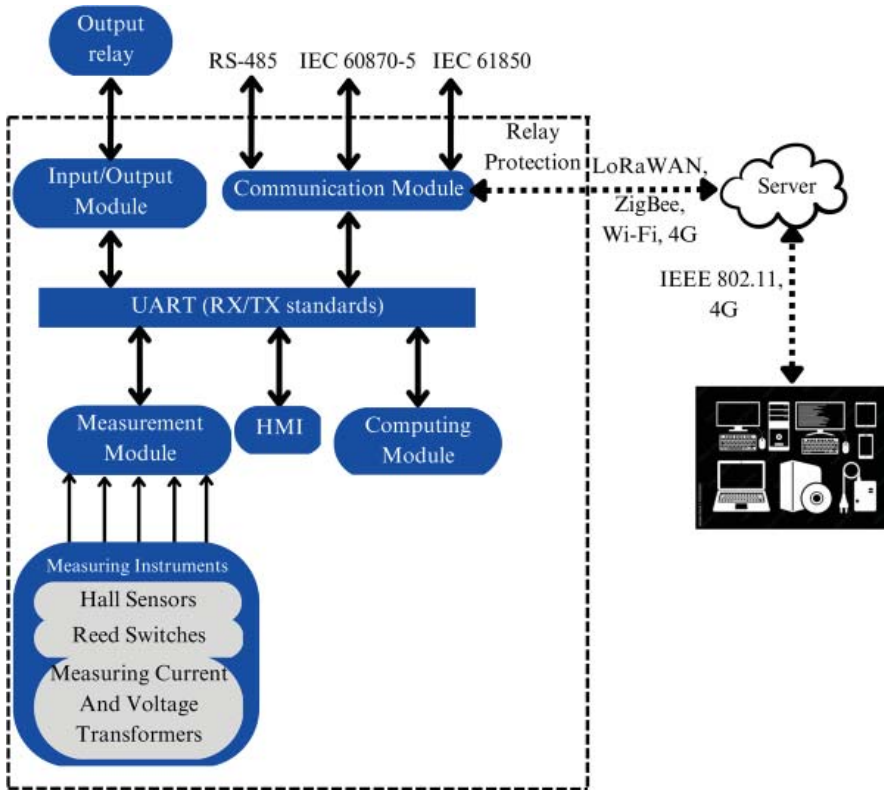


Fig. 7. Structural model of the developed microprocessor-based relay protection system based on an open architecture with the use of industrial internet of things technology

5. 3. Modeling and experimental testing of micro-processor-based relay protection for performance evaluation

As part of the study of the developed relay protection based on an open architecture, mathematical modeling and experiment were conducted to evaluate the speed and to compare it with the traditional solution. As a result, it is necessary to determine the following points:

- optimal simulation environment;
- the speed of operation of the proposed device in relation to the low-cost version of the traditional microprocessor-based relay protection device, in this study Altey-01;
- the possibility of blocking non-selective tripping of relay protection using the Internet of Things.

It is necessary to choose an environment for modeling to develop a microprocessor-based relay protection device based on an open architecture with the industrial internet of things technology. The following environments are considered within the framework of mathematical modeling of relay protection and its parts: Ansys Maxwell, Comsol Multiphysics, and MATLAB.

As initial data for mathematical modeling, it was assumed that single-phase short circuits of

a multicore cable, which in the normal mode conducts a current of 1 kA and its frequency is 50 Hz. During a fault, only the amplitude increases up to 2 kA. The delay of operation of relay protection is accepted to be 150 ms from the moment of the reed switch closing. The delay of non-selective tripping blocking is taken as equal to 100 ms after reed switch actuation.

Ansys Maxwell and Comsol Multiphysics allow you to perform 2D and 3D modeling and integrated numerical calculation of electromagnetic fields. Fig. 8 shows the distribution of the magnetic field in the conductor and beyond it, made in the Ansys Maxwell environment, which allows evaluating the work of the primary measuring transducer – a reed switch.

Ansys Maxwell and Comsol Multiphysics use the finite element method for calculations and allow simulating one part of the relay protection, in our case, the conductor and the primary measuring transducer, but do not allow simulating the operation of the remaining relay protection under development, integrating atypical elements such as reed, and modern solutions, such as IIoT. Therefore, the MATLAB Simulink mathematical modeling environment was chosen.

MATLAB Simulink is a popular design tool, including various traditional and renewable energy systems. For the design of mathematical models, it uses a library of graphical block diagrams. It is possible to create new block elements using the C++ programming language and mathematical functions. Simulink allows the simulation of the power supply circuit, measuring part, and logic part. Fig. 9 shows the mathematical model of the developed relay protection device.

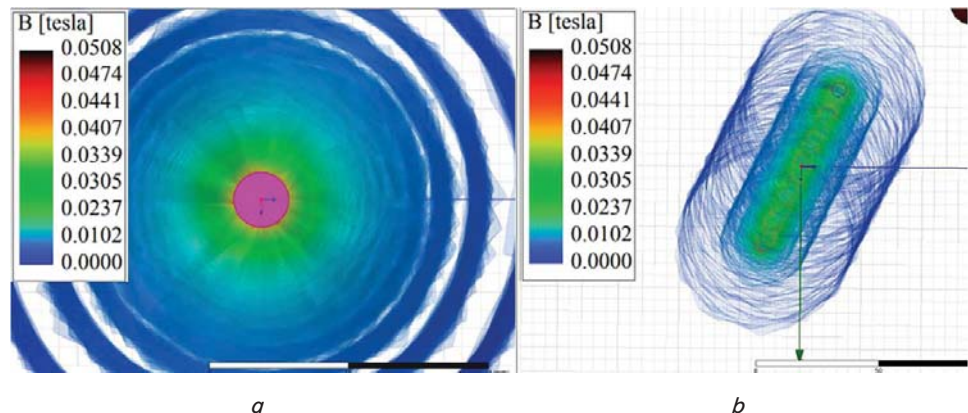


Fig. 8. Distribution of the magnetic field in and around the conductor: a – 2D model front view; b – 3D model

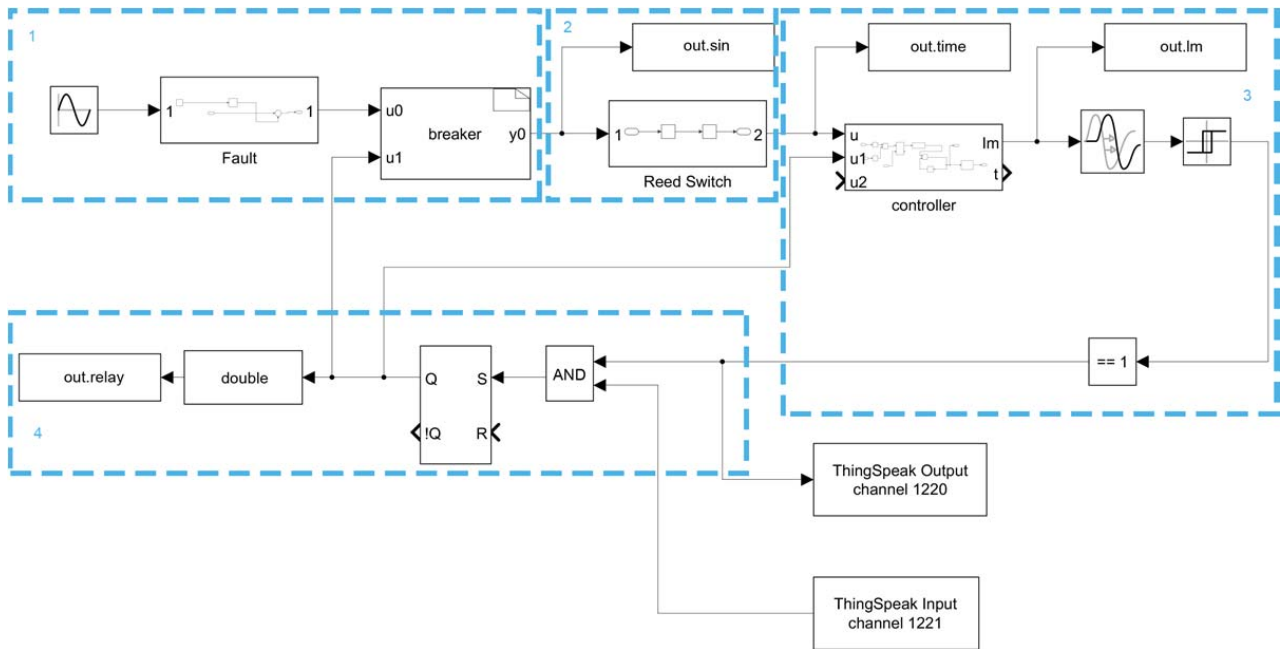


Fig. 9. Functional block diagram of the simulated relay protection device

The model contains elementary circuit 1, measuring part 2, logic part 3, and breaker circuit 4. Elementary circuit 1 consists of a power supply, conductor, and consumer. The Fault block allows the simulation of the process of a short circuit. The breaker unit is a switch, opening, and closing, done by the control signal from the executive part's RS Flip-Flop. A reed switch acts as a measuring element. The logic part of the circuit is the controller and the comparison element block. The blocks Thingspeak Output and Thingspeak Input are the elements of IIoT, which allow the transmission and receiving of information from the server. Simulation results in the form of graphs are shown in Fig. 10, 11.

The time range of the relay protection operation was considered in milliseconds. In normal operation, the current dependence in the first graph of Fig. 10 has a sinusoidal form with an amplitude of 1 kA and a frequency of 50 Hz. Short-circuit simulation, as indicated earlier, was carried out with simplifications such as the absence of an aperiodic component and higher harmonics in the Fault block. Consequently, in the short-circuit mode at 200 milliseconds, the current amplitude increases to 2 kA at a constant frequency. Due to the sinusoidal pattern of change in current, it periodically closes its contacts. Therefore, the timer begins to operate and count when the contact reed contact is closed. Based on the measured time at the moment of 200 milliseconds, the current calculation begins, shown in the second graph. According to the simulation result, the amplitude of the calculated current is 2 kA. However, the dependence of current on time has a non-sinusoidal shape. Despite this, the blocking occurs after 100 ms as shown in Fig. 10 on the 5th graph. Consequently, the current amplitude decreases to 1 kA, as shown in graph 1 of Fig. 10, and the calculated current in graph 2 of Fig. 10

continues to show the last measured value. In the case of selective tripping, after a delay of 150 ms, as the output relay trips, according to graph 4 of Fig.11, the amplitude of the current of the studied object in graph 1 of Fig. 11 at the time of 420 ms decreases to 0. Moreover, the calculated current, as in the case of Fig. 10, continues to show the last measured value.

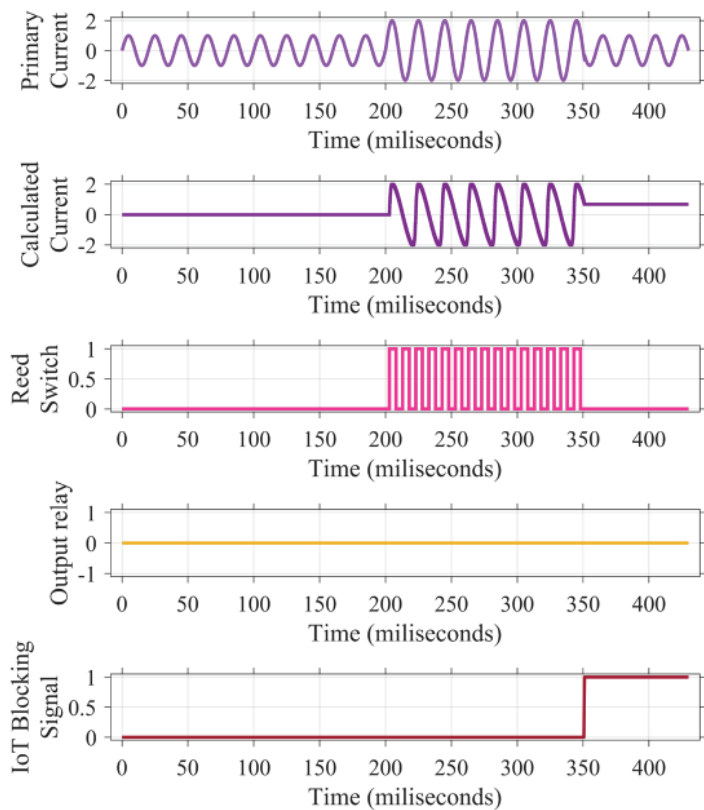


Fig. 10. Simulation results of the relay protection device when the interlock is triggered

During the experiment, the current in a four-core cable with diameters of 35 mm for three cores and 16 mm for the fourth core was observed. Moreover, the current amplitude value varied from 5 A to 1 kA. An increase in current during the experiment was carried out gradually using the developed experimental setup, the principle of which is described as follows.

The experimental setup is started by closing the circuit breaker Q1. Then via automatic unit Q3 to terminals X11.4 and X11.5 of traditional micro-processor-based relay protection, ALTEY-01 MRP voltage of 220 V is supplied, starting a digital device. Then using automatic circuit breaker Q2, through normally closed contacts K1.1 and K1.2, a line autotransformer TGDC2-2 (LATR) voltage is supplied to the primary winding. By turning the rotary lever, the voltage of the secondary winding of the LATR is regulated from 0 to 250 V, which goes to the primary winding of the load transformer HT2500 (LT). As the voltage on the primary winding increases, the current on the secondary winding begins to increase. This simulates the increase of current to a critical value. Moreover, the secondary winding is connected to a current transformer T0.66-U M3 (CT), which converts the measured range of 0 to 2,000 A into a range of 0 to 5 A. The CT is connected with the protected single-phase cable in series. Thus, the current from the CT secondary winding goes to the input X1.1 and X1.2 in the MRP, which closes the contacts of the discrete output X4.1 and X4.2 when the setpoint is exceeded. Consequently, the signal from the 12 V power supply connected to a separate 220 V AC voltage source goes to the relay K1, which by opening its contacts, disables the LATR and, respectively, LT.

The installation makes it possible to simulate the occurrence of a short-circuit current for a short period. It also allows the relay protection to operate by sending a signal to the starter, ensuring the power supply is switched off. The installation also includes an industry-used solution ALTEY-01 (MRP), which allows evaluation of the developed solutions. In the experiment, the hardware-software set was assembled as shown in Fig. 12.

The value of the current flowing through the cable was recorded with a UNI-T clamp meter UT204+. The closed time of the reed switch was measured with an oscilloscope GDS-71054B. The current and the time from the reed switch's activation to the installation's disconnection were determined using an oscilloscope and the built-in software monitor.

During the experiment, the results were obtained in the form of time intervals. The time intervals required for sending and receiving information were recorded during data transmission.

The prototype could transfer data from the local device to the hub in 10 ms. It took up to 40 ms for the data to be processed at the concentrator and to get feedback as a blocking signal.

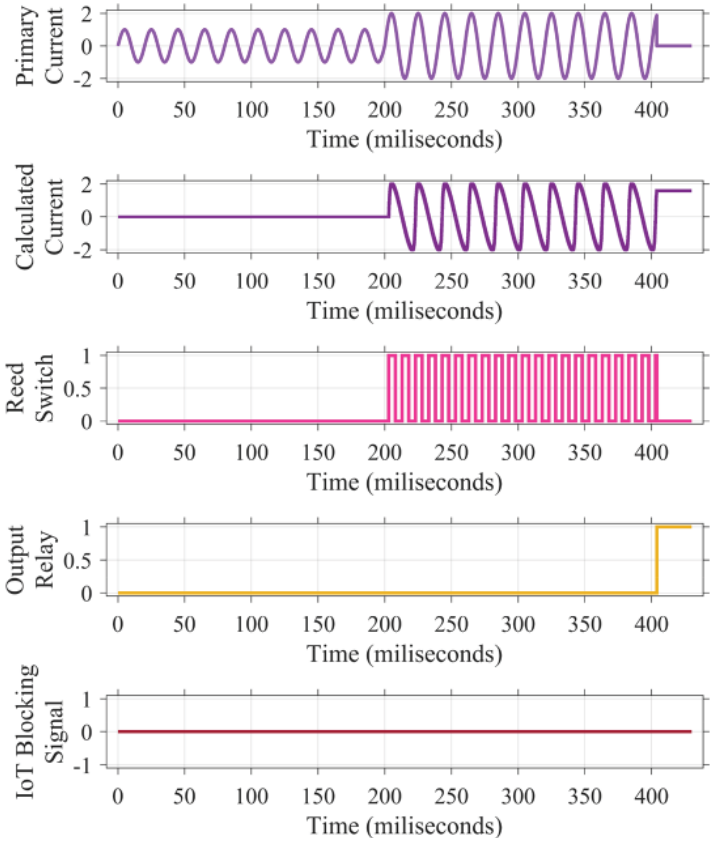


Fig. 11. Simulation results of the relay protection device without interlocking participation

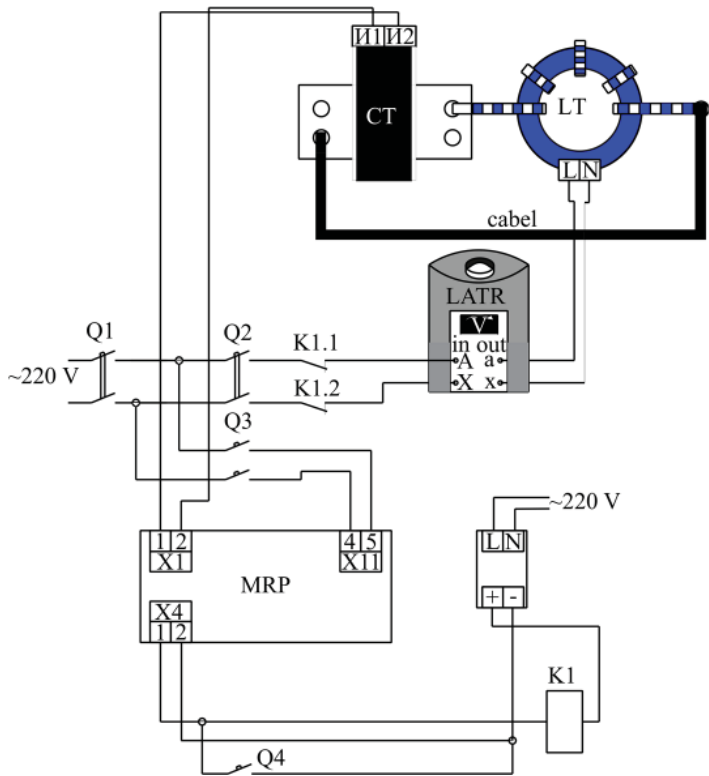


Fig. 12. Experimental installation for testing relay protection

6. Discussion of experimental results of microprocessor relay protection based on open architecture

The developed structural model of the sequence of operations in the measurement allowed us to optimize the resources required to construct the device to achieve the speed of operation. Moreover, from the model shown in Fig. 1, the delay t_1 of the process between (1) and (2), and between (2) and (3) – t_2 , between (3) and (5) – t_3 , between (5) and (7) – t_4 , between (7) and (9) – t_5 was determined. Therefore, the sum of these delays determines how long the device can signal to trip the circuit breaker. In addition, the developed model can identify the process that takes the longest to execute. The application of the structural scheme of processes will allow you to calculate the time of operation for any type of relay protection. The result of the first task was obtained through known structural schemes for traditional relay protection [13, 14]. It should be noted that the process sequence schemes proposed in these sources have many different types of information processing, storage, and recording elements required for processing analog signals. Although they perform the function of noise elimination and error correction, the structural model in Fig. 1 has a simpler structure, computation and decision-making processes. However, the solutions [4–6] as well as [7–9, 12] consider the efficiency only by end parameters, not covering the problems in providing the requirements of relay protection. Consequently, the considered solutions only have reliable results under certain laboratory or simulation conditions. It is worth noting that the application [4–6] for traditional solutions is also complicated because the architecture of the devices is closed, and it is impossible to assess compliance with the requirements of relay protection. As a result, the proposed structural model allows you to build a microprocessor-based relay protection device on different platforms, expanding the possibilities for developers. However, during the development of the structural model (Fig. 1), simplifications were taken as the absence of electromagnetic disturbances caused by the operation of neighboring installations, which in further studies will be considered eliminated. At the same time, the structural model in future studies will also allow evaluating sensitivity, selectivity, and reliability for more situations.

On the other hand, the result of the first task allowed us to develop a structural model of the device (Fig. 7). At the same time, using open protocols and standards allowed us to ensure the solution's modularity. This design will allow using a different number of measuring devices without using intermediate modules for processing the input signals. The use of open communication standards, such as UART, allows the application of device modules built on different platforms, such as STM32, XILINX, ALTERA, Arduino, Raspberry Pi, ESP32, and ESP8266. It should be noted that the measurement module, in contrast to traditional solutions used with [4–6], as well as solutions based on reed switches [7–9] and [12], allows for connecting not only a current transformer or reed switch but also a Hall sensor, inductance coils, making the replacement of current and voltage sensors undependable from the functionality and manufacturer, which in turn allows you to make multiple reserves of measuring instruments. At the same time, the developed structural diagram of the device can be used to build it on the FPGA platform, but unlike [2], it can produce blocking, which is one of the control actions, and analytics using Internet Things. It is also worth noting that in the case of [2],

additional intermediate devices that perform pre-processing are required to obtain information from sensors, which can lead to dependence of the smooth and reliable operation of the relay protection on the measuring device. Additional advantages are also the simpler design, containing fewer filters for processing analog signals, namely the elimination of noise caused by electromagnetic interference, as well as the implementation of a communication module that allows the implementation of the Internet of things not only within the analytics but also within the formation of the blocking signal, which, according to (9), provides a higher speed in tripping of the circuit breaker. One possible direction for further research is the study of devices built on different platforms.

Based on the results of the second problem, the simulation of the distribution of the magnetic field around the conductor, allowing to choose the optimal distance for installing the reed switch (Fig. 8) and the operation of the device itself was carried out. In doing so, the block diagram in Matlab Simulink presented in Fig. 9 allowed the simulation to be performed. In turn, the results of this simulation, presented in the form of graphs in Fig. 10, showed that the blocking of the microprocessor relay protection using IoT, which is implemented based on the derived equation (9), can be performed faster than the non-selective actuation of protection due to the data transfer rate. Moreover, the blocking can operate even after increasing the device's speed, which was confirmed during the experiment and carried out using the assembled setup shown in Fig. 12, which can pass current up to 2000 A. Thus, it will be possible to determine the optimal delay time for actuation using the circuit built in Matlab. At the same time, it is worth noting that the results obtained in the simulation showed a high speed of blocking the operation of relay protection due to the data exchange rate using the Internet of Things. The clock rate of the microprocessor provides the fast-tripping speed of the circuit breaker. At the same time, unlike the solutions [7–9, 12], where no simulation was presented, the proposed solution provides the simulation result in the form of five graphs, which allows identifying the tripping and blocking moments. On the other hand, unlike the solutions of [1, 2], and [4–6], this study adopted several simplifications for simulation and experiment. However, using a traditional microprocessor-based device allows you to carry out a performance analysis, based on which the device with the fastest response speed can be chosen. It is worth noting that the developed device should not only be able to work with modules built on different platforms but also, firstly, to meet the main requirements of relay protection and, secondly, be superior in relation to the traditional solutions within the framework of these requirements. The developed block diagram of Fig. 9 allows you to test the efficiency of applying the Internet of things within the framework of control actions. At the same time, in the future, this scheme can be applied to evaluate the implementation of other opportunities using the Internet of Things.

Despite this, the study of the developed microprocessor-based relay protection device based on an open architecture with the application of industrial internet of things technology was carried out only by one of the criteria for evaluating the effective operation of relay protection, namely, speed, due to such limitations as the need for a load, as well as the consideration of other sensors (Hall sensor, optical sensors) to evaluate the sensitivity; conducting field tests to evaluate selectivity, as the need for a long time period of research to assess reliability, as to calculate the reliability

index the data on the parameters of the flow of false alarms and failures in the operation of the device. In this case, one of the reliability indicators is durability, which is difficult to check within the framework of this study. Moreover, field tests are necessary to evaluate the selectivity criterion. For these reasons, conducting a complete device analysis without sensitivity, selectivity, and reliability data is complicated. Therefore, further studies will focus on sensitivity, selectivity, and reliability. In this case, when determining the selectivity and sensitivity, the main difficulty may lie in the sensitivity due to the complexity of the computational process since the reed contact can be affected by many interferences of electromagnetic nature. It is also worth noting that the ESP32 and ESP8266 applications have speed limitations. Moreover, the FPGA from XILINX 7 generation has a higher data processing speed than the considered platforms. Consequently, the application of this platform for data processing will be considered in further research. At the same time, improving the experimental setup in further research will allow additional analysis of several devices built on different principles and platforms in the sensitivity and selectivity framework. On the other hand, mathematical modeling will consider the presence of non-sinusoidal primary current, for which it is necessary to apply the data obtained in field tests.

7. Conclusions

1. A structural model of a microprocessor-based relay protection device based on an open architecture with the industrial internet of things technology was built due to the application of graph theory and Bio-Savara-Laplace law. Unlike known ones, this model allows building microprocessor-based relay protection devices on various primary sensors, including reed switches. The structural model contains 5 stages of set formation, from the closed state time measurement to the circuit breaker trip signal formation. Available studies on the construction of relay protection devices did not offer structural models, which previously complicated further development.

2. A microprocessor relay protection device based on an open architecture with the application of industrial internet of things technology was developed. The following were proposed: graph implementation scheme of the developed microprocessor relay protection system; scheme of information flows from field level to front-end; block diagram of the hardware-software complex and structural model of the developed microprocessor relay protection system based on an open architecture with the application of industrial internet of things technology. The result has been achieved by applying the approach based on Open RAN. Openness is ensured by using interfaces based on international stan-

dards IEC 60870-5, IEC 61850, RS-485, UART (RX/TX standards), or I2C, SPI for data transfer between device modules. Unlike known proprietary solutions, the modules are interchangeable without dependence on the vendor. The Internet of Things is used to transmit data about the state of the blocking, which is involved in the decision of tripping. It allows building new algorithms for the relay protection operation of distributed power systems.

3. Simulation and experimental testing of a prototype microprocessor-based relay protection device based on an open architecture using the Industrial Internet of Things technology were performed. ThingSpeak blocks were used when modeling the device, which allowed the implementation of IIoT. The speed can be provided by the peculiarities of the functioning of the reed switch because for the operation of the relay protection device, it is enough to measure one half-wave of the AC sinusoid. The simulation showed and the experiment confirmed the result of 40 ms to actuation. The obtained result corresponds to the permissible tripping time used in industry and is considered relay protection. The simulation and experimental testing results showed the fundamental possibility of using open architecture devices with the application of the Industrial internet of things to construct relay protection systems, which will provide the flexibility to meet the requirements in connection with the input of distributed energy.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The paper was written within the state order for the implementation of the scientific program under the budget program of the Republic of Kazakhstan 217 “Development of Science”, subprogram 101 “Program-targeted funding of the scientific and/or technical activity at the expense of the national budget” on the topic: “Development of technology for building microprocessor-based resource-saving relay protection devices based on an open architecture” Grant IRN AP13067967.

Data availability

Data will be made available on reasonable request.

References

1. Rahmati, A., Dimassi, M. A., Adhami, R., Bumblauskas, D. (2015). An Overcurrent Protection Relay Based on Local Measurements. *IEEE Transactions on Industry Applications*, 51 (3), 2081–2085. doi: <https://doi.org/10.1109/TIA.2014.2385933>
2. Jahn, I., Hohn, F., Chaffey, G., Norrga, S. (2020). An Open-Source Protection IED for Research and Education in Multiterminal HVDC Grids. *IEEE Transactions on Power Systems*, 35 (4), 2949–2958. doi: <https://doi.org/10.1109/TPWRS.2020.2970477>
3. Energy goes digital. SIEMENS. URL: <https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/energy-is-going-digital.html>
4. Isaiev, V., Velychko, O., Anokhin, Y. (2019). Comparator effect on equivalence of results of calibrating current transformers. *Eastern-European Journal of Enterprise Technologies*, 5 (5 (101)), 6–15. doi: <https://doi.org/10.15587/1729-4061.2019.177415>

5. Kaczmarek, M., Stano, E. (2020). Nonlinearity of Magnetic Core in Evaluation of Current and Phase Errors of Transformation of Higher Harmonics of Distorted Current by Inductive Current Transformers. *IEEE Access*, 8, 118885–118898. doi: <https://doi.org/10.1109/ACCESS.2020.3005331>
6. Naseri, F., Kazemi, Z., Farjah, E., Ghanbari, T. (2019). Fast Detection and Compensation of Current Transformer Saturation Using Extended Kalman Filter. *IEEE Transactions on Power Delivery*, 34 (3), 1087–1097. doi: <https://doi.org/10.1109/tpwrd.2019.2895802>
7. Kletsel, M., Kabdualiyev, N., Mashrapov, B., Neftissov, A. (2014). Protection of busbar based on reed switches. *Przeglad Elektrotechniczny*, 90 (1), 88–89. doi: <https://doi.org/10.12915/pe.2014.01.21>
8. Kletsel, M., Kaltayev, A., Mashrapov, B. (2017). Resource-saving protection of powerful electric motors. *Przeglad Elektrotechniczny*, 93 (5), 40–43. doi: <https://doi.org/10.15199/48.2017.05.09>
9. Kletsel, M., Borodenko, V., Barukin, A., Kaltayev, A., Mashrapova, R. (2019). Constructive features of resource-saving reed relay protection and measurement devices. *Rev. Roum. Sci. Techn. - Électrotechn. et Énerg*, 64 (4), 309–315. URL: http://revue.elth.pub.ro/upload/97922702_MKletsel_RRST_4_2019_pp_309-315.pdf
10. Li, Z., Zhang, S., Wu, Z., Abu-Siada, A., Tao, Y. (2018). Study of Current Measurement Method Based on Circular Magnetic Field Sensing Array. *Sensors*, 18 (5), 1439. doi: <https://doi.org/10.3390/s18051439>
11. Muşuroi, C., Volmer, M., Oproiu, M., Neamtu, J., Helerea, E. (2022). Designing a Spintronic Based Magnetoresistive Bridge Sensor for Current Measurement and Low Field Sensing. *Electronics*, 11 (23), 3888. doi: <https://doi.org/10.3390/electronics11233888>
12. Neftissov, A., Biloshchytskyi, A., Talipov, O., Andreyeva, O. (2021). Determination of the magnitude of short-circuit surge current for the construction of relay protection on reed switches and microprocessors. *Eastern-European Journal of Enterprise Technologies*, 6 (5 (114)), 41–48. doi: <https://doi.org/10.15587/1729-4061.2021.245644>
13. Blackburn, J., Domin, T. (2006). *Protective Relaying: Principles and Applications*. CRC Press, 664. doi: <https://doi.org/10.1201/9781420017847>
14. Phadke, A., Thorp, J.S. (2009). *Computer relaying for power systems*. John Wiley & Sons. doi: <https://doi.org/10.1002/9780470749722>