Advances in IT and Electrical Engineering

vol. 30, 2024, 33-48
https://doi.org/10.7862/re.2023.x

THE FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING
RZESZOW UNIVERSITY OF TECHNOLOGY

Original Research

Custom Perimeter Alarm System: Enhancing Surveillance Across Multiple Checkpoints

Patryk Jaskuła [1], Mariusz Węglarski [2,*]

[1] Department of Electronic and Telecommunications Systems, Rzeszów University of Technology, ul. Powstańców Warszawy 12, 35-959 Rzeszów, Poland, p.jaskulski41@gmail.com
[2] Department of Electronic and Telecommunications Systems, Rzeszów University of Technology, ul. Powstańców Warszawy 12, 35-959 Rzeszów, Poland, wmar@prz.edu.pl

* Corresponding author. wmar@prz.edu.pl

Received: 06 September 2024 / Accepted: 24 November 2024 / Published online: 23 December 2024

Abstract

This work develops an innovative perimeter loop configuration aimed at surpassing the limitations of conventional alarm systems. The proposed design enables the integration of a large number of sensors into a single monitoring loop, using only two connecting wires, and is compatible with the commonly used normally closed (NC) connection. The custom perimeter system features simplified installation with the use of standardized parametrizing resistors, and includes a calibration method to enhance detection accuracy. A prototype was tested with 20 magnetic contacts, demonstrating that wire resistance and the tolerance of parametrizing resistors are critical factors influencing system performance. In practical trials, a maximum of 15 sensors could be reliably detected. However, the introduction of calibration procedure allowed for an increased detection of up to 20 sensors. The system, which can handle numerous closely spaced control points, also features battery backup capability to ensure operation during power failures. Overall, the system effectively manages complex monitoring requirements and provides reliable performance under various conditions.

Keywords: alarm system, perimeter loop, parametrized line, end-of-line resistor, magnetic contacts, reed switches

1. Introduction

Alarm systems play a crucial role in ensuring security in privet residences, workplaces, stores, various industrial facilities, etc. Their primary function is twofold: they act as a deterrent to potential burglars and provide real-time alerts to property owners in the event of a breach of the protected area [1]. Modern systems can also be used for monitoring the current status of various points within the property (e.g., whether doors or windows are open or closed, or the current value of a measured physical parameter, such as temperature in a room). This allows property owners to have greater control and awareness of their environment, even when they are away from the premises. In contemporary technology-driven world, manufacturers are continually developing more advanced solutions that go beyond mere antiburglary functions [2]. Many alarm systems are now integrated with smart home automation features, offering enhanced convenience and functionality [3, 4]. For instance, such systems can be connected to lighting, heating, ventilation or air conditioning systems, allowing users to remotely control and monitor these functionalities through mobile apps or other interfaces.

In the case of perimeter systems, a breach of the designated monitoring zone is detected by utilizing an appropriate number of so-called intrusion sensors [5, 6]. There are various types of these access devices, each designed to meet specific security needs depending on the environment and the level of protection required. These include, among others, contact sensors (magnetic contacts, reed switches)

This is an Open Access article distributed under the terms of the CC-BY-NC-ND 3.0 PL license, which permits others to distribute the work, provided that the article is not altered or used commercially. You are not required to obtain permission to distribute this article, provided that the original work is properly cited.

that detect the opening of windows or doors [7], motion detectors, sound and vibration sensors [8] or infrared barriers [9]. Each of these sensors is carefully selected and positioned to cover potential points of entry or vulnerable areas within the perimeter. The choice and number of sensors depend on several factors, including the size of the area to be monitored, the nature of the threats, and the specific security requirements of the property.

Equally important is the method of connecting intrusion sensors to the central control unit, which oversees the operation of the alarm system [10]. The way in which these connections are established can significantly impact the reliability, responsiveness, and maintainability of the entire security system. In traditional alarm systems, all access devices are typically hardwired directly to dedicated inputs on the control panel or in series with an existing monitoring loop. It should be noted that wired connections are generally more reliable, they are less prone to interference from external sources, such as wireless signals or physical obstacles that can disrupt communication. They are less vulnerable to hacking or signal jamming, which can be a concern with wireless systems. Tampering with a wired connection would require physical access to the cables, making it more difficult for an intruder to disable the system without triggering an alarm. Moreover, in a wired system, sensors typically draw power directly from the central control unit, eliminating the need for individual batteries [11]. This reduces the maintenance required to keep the system operational, as there are no batteries to replace. However, the traditional wired approach also presents certain challenges. Installing a wired alarm system can be labour-intensive and requires careful planning, particularly in large or complex buildings. Wired systems are less flexible when it comes to relocating sensors or making changes to the layout of the system. From an economic standpoint concerning installation costs, both wired and wireless systems have their advantages and disadvantages [12]. In this aspect, only considerations specific to a particular scenario provide a measurable comparison.

In scientific literature, the topic of wired perimeter systems in the scope of their construction and operation is rarely addressed in detail. However, certain recent research activities addressed the reliability of reed switches. In these studies, the magnetic contacts were exposed to varying temperatures [13] or multiple switching repetitions [14]. Conversely, there is a substantial body of research focused on wireless solutions, which is quite understandable given the advancements in radio communications technology [15]. Wireless systems offer numerous advantages over traditional wired counterparts, such as greater flexibility in installation and easier adaptation to changing environments. However, they come with their own set of challenges, including the need for regular maintenance to replace power sources (as they operate remotely and are battery-powered) [11], which can be a significant inconvenience, particularly in large protected areas with numerous access points. Additionally, the costs for radio frequency components in sensors and central receiving units must be taken into account in installation projects. Electromagnetic interference generated in the environment [16] or cyber security of communication networks [17] also have a significant impact on the reliable operation of the wireless alarm systems. Nevertheless, there are numerous examples in the literature of research efforts aimed at effectively replacing the components of typical wired perimeter systems by creating novel and unconventional components. For instance, these include the contact glass-break detector [18], which provides a specialized mechanism for detecting vibrations, or a highly sophisticated solution involving autonomous drones working in tandem with a set of video cameras that remain inactive until an event is detected [19]. Another notable example is the use of radar sensors to enable early warning capabilities and track the path of an intruder [20]. These innovative approaches highlight the ongoing quest to enhance security systems by leveraging advanced technologies and optimizing operational efficiency.

Based on the identified limitations and drawbacks of existing alarm systems, an innovative perimeter monitoring installation has been developed by the authors. In the presented work, special attention was given to the number of possible control points that a user can connect to a single input on the control panel or expansion module, as well as the complexity of the wiring required with an increasing number of nodes in a single loop. The analysis led to the development of the custom perimeter system solution that addresses these shortcomings and allows for the connection of the maximum number of intrusion sensors using the fewest possible wires. The primary objective of the presented study is to ensure the system can accurately detect which of the numerous monitored control points has been triggered within an extensive monitoring loop and to communicate this information to the user. In the view of the authors, their proposed solution simplifies the installation process while maintaining the system's reliability.

2. Research Assumptions

2.1. Effectiveness and Limitations of Perimeter Line Configurations

A typical manufacturer of alarm devices offers a range of more or less advanced control panels, designed for applications ranging from the simplest home installations to extensive industrial surveillance areas. These devices primarily differ in the number of inputs, outputs, and built-in functions. This allows the user to select a device that suits their specific needs while taking economic considerations into account.

As an example, the most cutting-edge products from manufacturers active in the local alarm control panel market are present in Table 1 [21-27]. The most advanced control panel, supported by expanders, can handle up to 256 sensors. It is important to note that the manufacturer provides the number of inputs available on the main board alone and additionally the maximum number of inputs that can be supported through additional expansion modules. It should also be noted that the main control panel board can manage only up to 16 wired sensors, while each expander can handle only 8. To utilize the 256 inputs claimed by the manufacturer, it is necessary to use as many as 30 expansion modules. The cost of one expander is about 1/5 of the price of the control panel itself. Therefore, a significant portion of the costs incurred in building a multi-point surveillance system is allocated to input expanders. Consequently, a desirable solution is a system that allows the connection of a large number of alarm sensors without the use of additional expansion modules.

From the perspective of creating a perimeter installation, manufacturers of control panels adhere to established standards that define the types of inputs designed for connecting wired sensors (Fig. 1). These inputs include those operating as NC (Normally Closed), NO (Normally Open), as well as parameterized configurations such as EOL/NC (End of Line/Normally Closed), 2EOL/NC, 3EOL/NC, and their corresponding EOL/NO (End of Line/Normally Open), 2EOL/NO or 3EOL/NO versions [7, 28, 29]. Standards involving more complex resistor configurations, such as 4EOL, 5EOL, etc., are not commonly used in commercial products; whereas 3EOL type is rarely available and only found in the most advanced devices (e.g. in Integra 256 Plus).

Table 1. Comparison of control panels with potential for use in wired perimeter alarm systems

Parameters	**Control panel**			
	ROPAM [21, 22] **NeoGSM-IP-64**	**DSC [23, 24]** **HS2128**	**Paradox [25, 26]** **Spectra SP7000**	**Satel [27]** **Integra 256 Plus**
Number of physical inputs for wired sensors on main board of control panel	16	8	16	16
Maximum number of wired inputs that can be managed through expanders	64	128	32	256
Number of partitions / zones	4	8	2	8 / 32
Number of physical outputs on the control panel's main board	8	4	4	16
Number of programmable outputs that can be managed through expanders	40	148	16	256
Permissible configuration of input lines	NC, NO, EOL/NC, EOL/NO, 2EOL/NC,2EOL/NO and 3EOL/NC*, 3EOL/NO* (*only Integra 256 Plus)			

Parameterization involves incorporating additional resistors into the circuit with the sensor's detector / switch [28]. From an electrical standpoint, switching to the additional resistance changes the equivalent resistance of the alarm circuit. In this way, the additional state of sensor activity can be distinguished. Manufacturers of alarm system use this technique to integrate security functions (e.g., tamper detection, beam obstruction, or removal of the device from its mounting surface) directly into the alarm sensor. This allows for monitoring the integrity of the perimeter lines, thereby increasing the system's reliability by preventing tampering or damage to the connection wires.

In alarm systems, NC connections (Fig. 1-a) are more commonly used due to the additional security they provide against potential damage to the alarm loop. Interrupting the continuity of the wire immediately triggers a response from the alarm control panel. In the case of NO inputs (Fig. 1-b), when the circuit's continuity is interrupted, it is not possible to determine if the sensor has been triggered to the close state. Unfortunately, the NC solution also has an additional drawback: if the circuit is normally closed by the sensor's detector / switch (SWx in Fig. 1), current always flows through the alarm loop during standby. The only way to limit this current is to use the resistors. By adding these resistors, the perimeter loop is converted into an EOL parameterized line (Fig. 1-c).

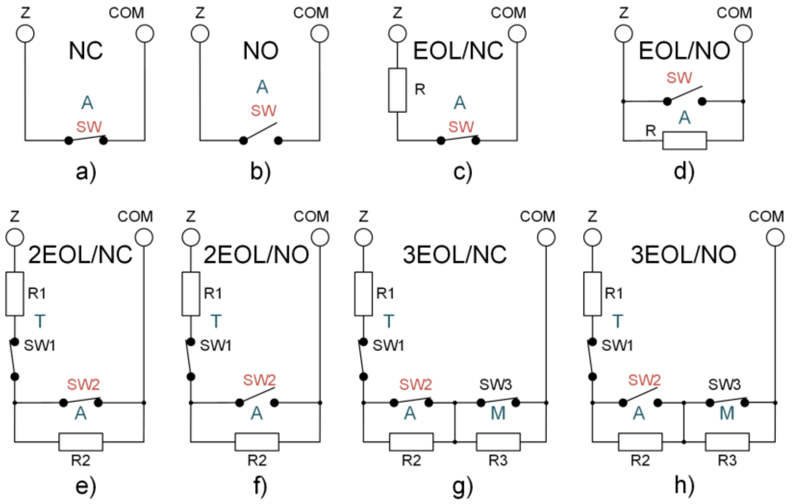

Fig. 1. Types of connections in parametrized lines: a) NC; b) NO; c) EOL/NC; d) EOL/NO; e) 2EOL/NC; f) 2EOL/NO; g) 3EOL/NC; h) 3EOL/NO; A – alarm; T – tamper; M – masking

The parametrizing resistor R is connected either in series (Fig. 1-c) or parallel (Fig. 1-d), depending on the required default standby state (NO or NC sensor). For the NC line (Fig. 1-c), the primary standby state is the closed circuit through the resistor R and switch SW. The second activation state (open state) occurs when the switch SW is open and no current flows. The third state can be triggered if a short circuit, caused by damage to the connection wires, happens between the sensor and the input of the control panel. In the event of wire breakage, it is impossible to distinguish this state from the triggered state, as in both cases, no current flows through the circuit. This approach is advantageous because, as mentioned earlier, it allows for the detection of a short circuit in the installation, caused by accidental reasons or tampering attempts. In the case of the EOL/NO line (Fig. 1-d), the default state is reversed. Additionally, for an NO sensor, it is possible to distinguish the sensor's activation state from the state of a broken connection. Thus, in the EOL/NC configuration, it is possible to detect a short circuit in the perimeter loop, whereas in the EOL/NO configuration, it is possible to detect broken wires.

Another variation is the 2EOL configuration (Fig. 1-e, f), which uses two resistors R1 and R2 and two switches SW1 and SW2. Typically, the additional switch is used by the alarm sensor as an extra protection to detect tampering attempts, such as opening the enclosure or detaching it from the wall. Each subsequent state is distinguished by a different equivalent resistance R_Z value observed between the ‘Z’ and ‘COM’ terminals and for 2EOL/NC configuration (Fig. 1-e) it is equal:

- $R_Z = R_1$ – SW1 closed, SW2 closed => standby state,
- $R_Z = \infty\Omega$ – SW1 opened, SW2 closed or opened => temper state or broken line,
- $R_Z = 0\Omega$ – short circuit in the installation, state of SW1 and SW2 any => fault state,
- $R_Z = R_1 + R_2$ – SW1 closed, SW2 opened => alarm state.

Similar considerations can also be applied to the 2EOL/NO line (Fig. 1-f):

- $R_Z = R_1 + R_2$ – SW1 closed, SW2 opened => standby state,
- $R_Z = \infty\Omega$ – SW1 opened, SW2 closed or opened => temper state or broken line,
- $R_Z = 0\Omega$ – short circuit in the installation, state of SW1 and SW2 any => fault state,
- $R_Z = R_1$ – SW1 closed, SW2 closed => alarm state.

As can be observed, the standby and alarm states for the 2EOL/NC circuit are reversed compared to the 2EOL/NO circuit. In both circuits, it is not possible to detect a separate case of a break in the continuity of the connection wiring. In either case, this state is always associated with tampering. It should also be noted that the values of both resistors can be the same, as this does not affect the ability to distinguish between the individual states. In one case, the equivalent resistance of the circuit is equal to R_1, while in the other case it is the sum of the series connection of R_1 and R_2. Regardless of the resistor values used, it is always possible to differentiate between these two states.

The 3EOL configuration (Fig. 1-g, h) is supplemented with an additional switch and resistor, which allows for the differentiation of an extra state. However, this modification introduces some complications. When resistors with the same values are used, it becomes impossible to distinguish between the activation states of switches SW2 and SW3. In both cases, the equivalent resistance is equal to the sum of the resistances. Therefore, manufacturers recommend that resistor R3 should have a value equal to the sum of R_1 and R_2 in series. Nevertheless, to correctly distinguish between states, it is sufficient to apply different values to the mentioned resistors and for 2EOL/NC configuration (Fig. 1-g) the resistance equivalent R_Z is equal:

- $R_Z = R_1 -$ SW1 closed, SW2 closed, SW3 closed => standby state,
- $R_Z = \infty\Omega$ – SW1 opened, SW2 and SW3 closed or opened => temper state or broken line,
- $R_Z = 0\Omega$ – short circuit in the installation, state of SW1 and SW2 any => fault state,
- $R_Z = R_1 + R_2$ – SW1 closed, SW2 opened, SW3 closed => alarm state,
- $R_Z = R_1 + R_3$ – SW1 closed, SW2 closed, SW3 opened => antimasking state,
- $R_Z = R_1 + R_2 + R_3$ – SW1 and SW2 and SW3 opened => alarm with antimasking state.

Similar considerations can also be applied to the 3EOL/NO line (Fig. 1-h):

- $R_Z = R_1 + R_2$ – SW1 closed, SW2 opened, SW3 closed => standby state,
- $R_Z = \infty\Omega$ – SW1 opened, SW2 and SW3 closed or opened => temper state or broken line,
- $R_Z = 0\Omega$ – short circuit in the installation, state of SW1 and SW2 any => fault state,
- $R_Z = R_1$ – SW1 and SW2 and SW3 closed => alarm state,
- $R_Z = R_1 + R_2 + R_3$ – SW1 closed, SW2 opened, SW3 opened => antimasking state,
- $R_Z = R_1 + R_3$ – SW1 closed, SW2 closed, SW3 opened => alarm with antimasking state.

As with the 2EOL line, the alarm and standby states for NO and NC are reversed. This also applies to the additional states present only in the 3EOL line. This type of parameterized line is most commonly used by manufacturers for infrared barriers and motion detectors, incorporating anti-masking to detect attempts to obstruct the emitted infrared beam.

2.2. Perimeter Loop with Numerous Intrusion Sensors

In the alarm system market, it is difficult to find products that efficiently handle a large number of intrusion sensors installed across multitude windows and doors within a single monitoring zone. If the requirements specify that each window in a hall must be protected by contact sensors or more advanced monitoring units (such as a vibration, glass break, or ultrasonic sensors), and if it is necessary to distinguish which access point has been breached, there is no other option but to use separate inputs on the alarm control panel for each sensor. When designing a perimeter alarm circuit under such requirements, several challenges have to be addressed. The first one is the complexity and significant expansion of the wiring circuit, as separate cables must be run to each access point (Fig. 2). For example, in parallel perimeter loop, a bundle of wires coming directly from the alarm control panel in a configuration with multiple windows have a large diameter due to the high number of individual cores within the cable. The second, and more serious, problem is the limited availability of alarm inputs, especially in budget versions of commercial control panels.

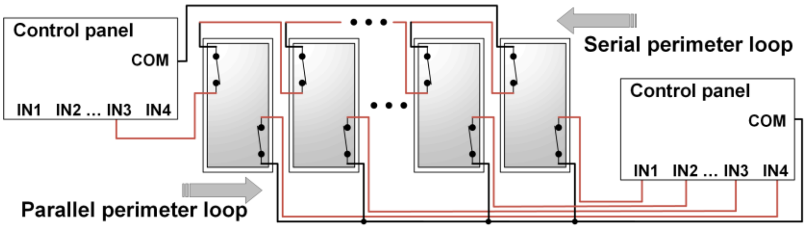

Fig. 2. Example of perimeter alarm line diagram for multiple windows protected by reed switches: parallel perimeter loop – each sensor connected separately to one input of control panel; serial perimeter loop – connection of sensors in series to one input of control panel

A potential solution to the above-mentioned problems is to connect the intrusion sensors in series (Fig. 2). This approach reduces the number of inputs used on the alarm control panel. It also simplifies the wiring installation, as only two wires extend from the control panel. The drawback of this configuration is the inability to determine which sensor in the series is triggered at alarm moment. Typically, this limitation is of minor importance, as the most crucial information for the user is that the perimeter loop has been interrupted, possibly indicating the monitored zone or room, rather than the precise location of the triggered sensor. This holds true for a simple installation with only a few sensors. However, in the case of a complex installation with a large number of control points, this system limitation can become problematic. For example, servicing the entire installation becomes challenging. In the event of a sensor failure, each sensor has to be checked individually, which is time-consuming. The ideal configuration is a circuit in which, despite connecting multiple sensors using only two wires, it is still possible to identify which monitoring point is triggered during an alarm. This capability is partially provided by the 3EOL parameterized line (Fig. 1-g, h), which could be further modified with additional sections to an nEOL type. The expansion method, allowing to manage a larger number of sensors, is illustrated in Figure 3. The modification involves implementing additional sections of switches with resistors connected in parallel to the existing setup. Each switch corresponds to each alarm detector.

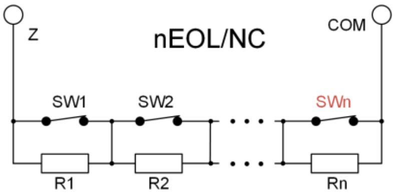

Fig. 3. The modified nEOL/NC configuration, which includes additional sections

The equivalent resistance R_Z of the nEOL circuit depends on which of the switches is open. When one of the switches is open, the resistor connected in parallel with it is no longer short-circuited by the circuit branch. This modification requires that each resistor has a different resistance value, because only then it is possible to determine which switch has been opened. The need to use different resistor values is not the only challenge here. When two or more switches are open, the value of R_Z equals the sum of the series-connected resistors that are not short-circuited. It is possible that the obtained sum could match the resistance value of another open section. This would result in an incorrect identification of the breach point within the supervised zone. To ensure accurate detection when multiple monitoring points are triggered simultaneously, each subsequent section should be equipped with resistors of progressively increasing resistance. Mathematically, this relationship can be expressed as follows:

$$R_Z > \sum_{i=1}^{n-1} R_i \,, \tag{1}$$

where n denotes the index of successive resistance R_i in the system.

In order to determine which sensor has been activated, each possible state must be defined and distinguished. Therefore, the nEOL configuration is challenging to implement due to the large number of possible combinations 2^n (e.g., 1024 for 10 points) that need to be distinguished. Additionally, there is a problem during the installation of the alarm system. Each loop section requires different resistor values, which complicates the assembly process and increases the likelihood of errors by installers.

2.3. Concepion of Custom Perimeter Alarm System

The custom perimeter alarm system (Fig. 4-a), as proposed by the authors, is structurally similar to the 3EOL configuration. The states of the perimeter loop are distinguished by changes in the equivalent resistance R_Z observed at nodes A and B (Fig. 4-b).

In the performed analysis, zero resistance R_x is assumed for the wires and switches in the branches. When all switches are closed, the equivalent resistance R_Z of the circuit is infinitely small because all resistors are bypassed. If any switch is open, the electrical potential at node A differs from that at node B. All resistors from the terminal Z to the open switch are not bypassed and actively contribute to the equivalent resistance. Meanwhile, all resistors to the right of the open switch remain unchanged – they are still bypassed and do not affect the value of R_Z. In the example (five monitored access node, the third section triggers alarm) shown in Figure 4-b, the equivalent resistance of the circuit is equal to the parallel combination of R_1, R_2, and R_3.

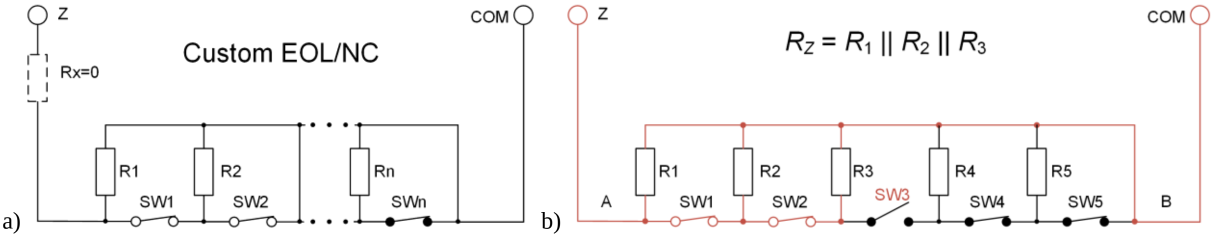

Fig. 4. Diagram of custom perimeter loop: a) Idea; b) Example of five nodes; SW3 open; current flow is marked in red

In the Custom EOL configuration, the equivalent resistance R_Z for any open switch, regardless of its number, is described by the following relationship:

$$R_Z = \frac{1}{\sum_{i=1}^{n} \frac{1}{R_i}} \tag{2}$$

where n denotes the index of the switch that is open, and R_i represents the resistances of the various resistors in the circuit. If resistors with equal values are used instead of different ones, the relationship (2) simplifies to the form:

$$R_Z = \frac{1}{\frac{n}{R}} = \frac{R}{n}, \tag{3}$$

where R represents the common resistance value for all resistors. Using identical pull-up resistors to the COM terminal means that for the n-th active switch, the equivalent resistance of the circuit is equal to the resistance of a single pull-up resistor divided by the index number of the open switch, counted from the terminal Z.

Each section in the perimeter loop corresponds to a single access point. Each subsequent switch has a lower priority compared to the previous one, meaning that when multiple points are activated simultaneously, the circuit's state is defined by the section with the smallest index. For example, if switches SW1, SW3, and SW5 are open, the equivalent resistance of the circuit corresponds only to the open state of SW1. This is a limitation of the Custom EOL configuration, as it is not possible to differentiate multiple monitored nodes being activated at the same time. Nevertheless, it is possible to detect each triggered alarm individually, one by one, according to their ascending numbers. At the moment the alarm loop is first interrupted, it is possible to determine where the breach occurred, which is crucial. This information allows for addressing the breach and moving on to manage next access points if they have also been activated.

The developed configuration of perimeter loop is simple to service. If an access point is damaged or the installation wires are interrupted, locating the fault is straightforward. It is only necessary to check the indicated access point and the wires between adjacent points. An additional advantage is the simplicity of implementing this solution compared to the 3EOL system and its extended modification (Fig. 3). The Custom EOL configuration does not require resistors with various values, also simplifying the assembly process. The limitation of these extended configurations is that they only support sensors with NC (normally closed) outputs.

3. System Evaluation

3.1. Design of Custom Perimeter Alarm System

The method of installation in real conditions (supervised zone secured with a perimeter loop of NC-type reed switches) is shown in Figure 5. The developed Custom EOL configuration requires additional pull-up resistors between the switches and the neutral point of the COM circuit. However, it is important to emphasize that, unlike in nEOL, the resistance value is the same for all resistors.

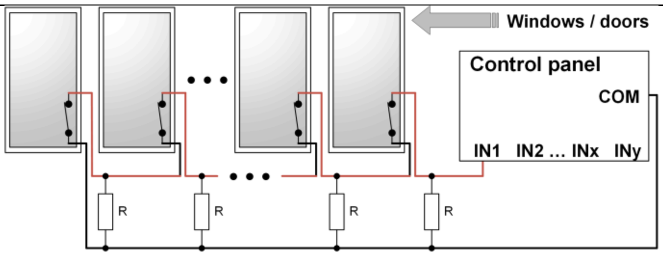

Fig. 5. Diagram of Custom EOL configuration of perimeter line secured with type NC reed switches

Because the alarm state of any access point is determined by changes in the equivalent resistance R_Z of the perimeter loop, it is necessary to propose an appropriate measurement method. Values of R_Z can be obtained using a voltage divider circuit combined with an analog-to-digital converter (ADC, Fig. 6-a). By carefully selecting the resistance ratio, it is possible to maximize the voltage change for the alarm state of each subsequent intrusion sensor.

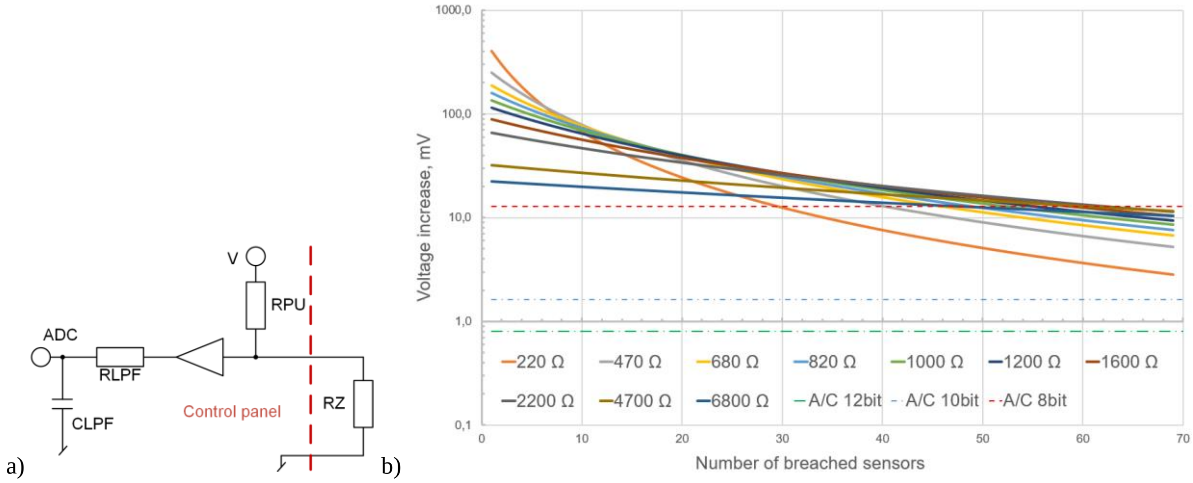

Fig. 6. Measurement of equivalent resistance R_Z: a) Signal conditioning circuit diagram; RPU – pull-up resistor; RLFP and CLPF– low-pass filter resistor and capacitor; V – supply voltage; ADC – analog-to-digital converter; b) Voltage change increment at divider's output relative to the next activated sensor for various resistor R values in perimeter loop; R_{PU} = 47 Ω

The change in voltage increment relative to the next activated sensor for several different resistance values R added to each section of the perimeter loop is presented in Figure 6-b. Thus, all resistors that make up the equivalent resistance R_Z have the same resistance value, and the upper resistor RPU in the voltage divider circuit has a constant value for all cases. As can be observed, the voltage increment is negative and changes in an exponential manner. The voltage decrement for sensor in the alarm state that is closer to the beginning of the loop is significantly larger than for that one that is closer to the end.

Therefore, the shape of the increment curve can be modelled by adjusting the resistance values in the divider. The optimal value is the one that provides the greatest voltage change for a given number of sections. In most cases, the method for selecting resistance involves finding (Fig. 6-b) the point on the curve corresponding to the greatest increment. If two or more curves intersect near the found point, the one that provides the greatest voltage change for the initial sensors is chosen. For example, for a loop with 30 sections, the optimal resistance is $R = 1600\ \Omega$. Nevertheless, the smallest possible values are preferred due to their lower susceptibility to interference, which can be induced in the connecting wires, for example, through inductive or capacitive coupling. Therefore, the upper resistor in the divider should be small, on the order of several tens of ohms. For this reason, $R_{PU} = 47\ \Omega$ is used in the calculations. The R_Z resistance can also be included in the voltage divider (Fig. 6-a) as the upper resistor. By maintaining the resistance ratios, only the sign of the voltage increment will change.

Additional lines, corresponding to the minimum voltage values that can be distinguished by ADC converters with resolutions of 8, 10, and 12 bits, are included in Figure 6-b. As can be observed, the 8-bit converter does not provide sufficient resolution for correct operation across the entire intended range. Its line intersects the voltage increment curves in all cases. If the loop configuration is limited to 20 sections, an 8-bit converter could theoretically suffice. However, the difference between the voltage change upon sensor activation and its voltage resolution is too small for proper alarm state detection, especially with higher resistance, such as R = 6800 Ω. The 10-bit and 12-bit ADC converters have sufficient resolution and can be used in the considered operating scenarios. The best results are obtained using the 12-bit converter, as it allows for a more precise determination of the voltage difference.

3.2. System Efficiency in Real Conditions

The measured voltage value for a given state of perimeter loop is slightly different from the ideal value obtained from calculations. This is due to the influence of real-world parameters such as resistor tolerance, non-zero wire resistance, uncertainties in the ADC, and interferences. For this reason, it is necessary to determine the voltage ranges within which the value must fall in order to correspond to the perimeter loop state associated with the activated intrusion sensor. The boundaries of these ranges are calculated by dividing the increment between two adjacent states in half and adding the resulting value to the previous state (Fig. 7-a). The width of these ranges defines the correct operating limits of the system.

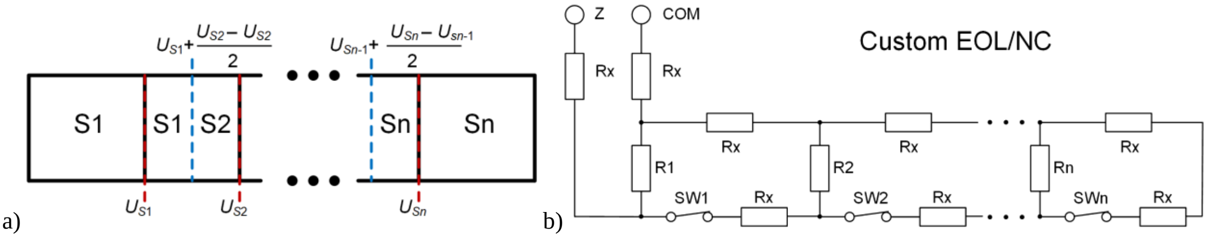

Fig. 7. System efficiency in real conditions: a) Method for calculating the voltage ranges for each state; b) Electrical equivalent of perimeter loop, taking into account resistance of wires R_x

To examine the impact of real-world parameters, the effect of wire non-zero resistance and resistor tolerances is considered for the worst-case scenarios (Fig. 7-b). The worst-case scenario is defined as the combination of extreme tolerance values for both the upper resistor in the divider and the resistors on the alarm loop side. The extreme resistance values are determined by the common resistors' tolerance.

The resistance of the connecting wires R_x depends on the type of wire used in the alarm installation. Typically, multi-core cables of type YTDY 6x0.5 mm (with a single wire diameter of 0.5 mm) are used. Knowing the diameter and material of the wire, it is possible to calculate the resistance for a given length using the following mathematical formula:

$$R = \rho \frac{l}{A}, \tag{4}$$

where ρ means resistivity of copper, l – length of conductor, A – cross-sectional area. Thus, for YTDY 6x0.5 mm, the resistance per meter is equal 89.35 mΩ.

Since resistance depends on the length of the wire between successive sensors, numerical calculations were conducted for several lengths: 1 m, 3 m, and 5 m. Tolerances of 1% and 5% were also considered. Simulations were conducted for a perimeter loop with 30 sensors, and the results were compared with those of the ideal case without accounting for wire resistance. The obtained results are presented in four graphs in Figure 8. The curves on the graphs labelled 'Upper boundary value' and 'Lower boundary value' define the range within which the voltage can vary from the ideal value for each activation state. If the voltage for a given state falls outside this range, the alarm control panel will incorrectly determine the number of the breached sensor. The intersection points define the maximum number of sensors that can theoretically be handled without inaccuracies.

The obtained results are summarized in Table 2. Since two extreme values were considered for each case, the maximum number of sensors that can be handled is taken as the smaller value obtained for a given tolerance. This approach ensures that no value will exceed the boundary for correct detection. Such an occurrence might happen because, in the minimal extreme case, the wire resistance for the middle sensors in the line partially offsets the tolerance effect, artificially increasing maximum number of sections.

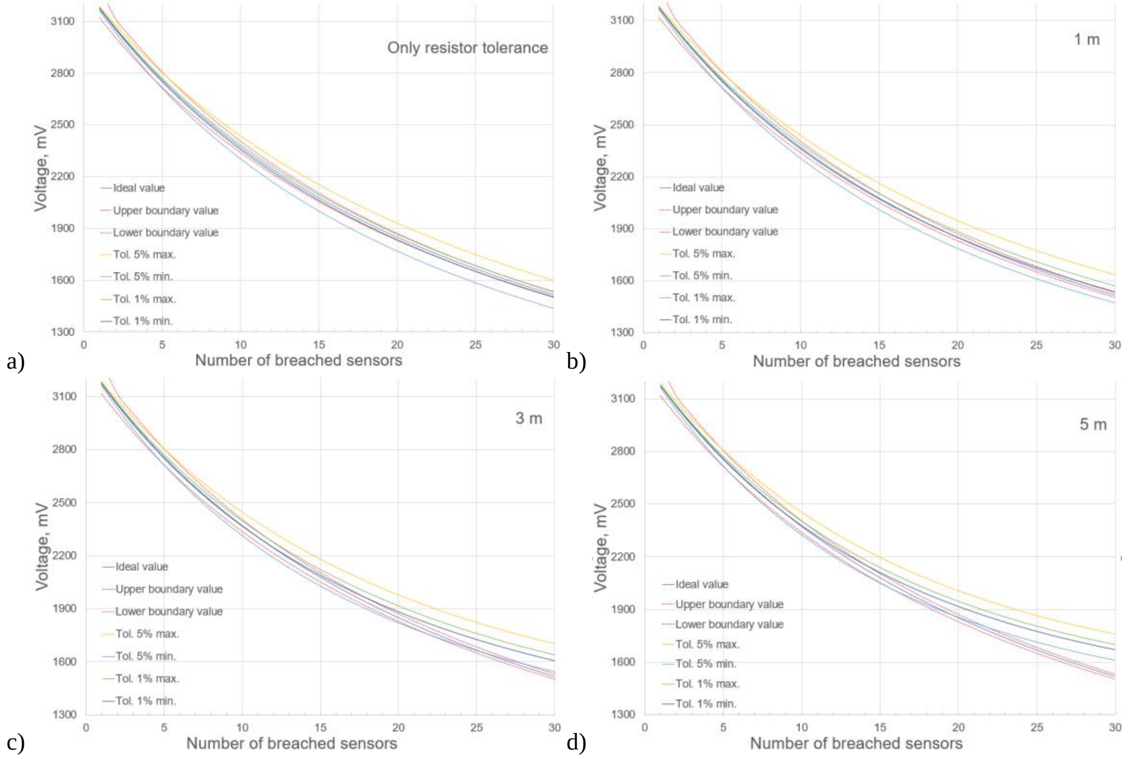

Fig. 8. Voltage variation graph depending on the active sensor; red dashed line – curves indicating boundaries within which the voltage can vary: a) case without accounting for resistance of wires; b) case for wires with length of 1 m between sensors; c) case for wires with length of 3 m between sensors; d) case for wires with length of 5 m between sensors

Table 2. Points of intersection with the boundary curves

Wire length Tolerance	Without wire resistance	1 m	3 m	5 m
	Theoretical number of sections			
max. @ tol. 5%	6	5	5	5
min. @ tol. 5%	5	5	5	6
max. @ tol. 1%	26	15	12	10
min. @ tol. 1%	25	28	17	15

The wire resistance and resistor tolerance significantly limit the proper operating of the perimeter alarm system. Using resistors with a lower tolerance improves the system's performance, but it does not eliminate the negative impact of the wire resistance. The length of the wires depends on the size of the alarm installation: the size of the building, the layout of the rooms, the placement of windows and doors, and the wires routing method. The complexity of the installation is a disadvantage because, for sensors closer to the end, the wire resistance has a dominant effect on the difference between the ideal and actual values. This is clearly seen when comparing the graphs without accounting for wire resistance to those for a 5 m length. The characteristic bending of the ideal calculated curves for the end sensors is evident.

In the simulations conducted, an equal wire length between successive intrusion sensors was assumed. In a real perimeter alarm system, the distribution of sensors in the protected zone is uneven, resulting in varying wire lengths between them. A possible way to improve the system's performance is through a calibration method. This involves measuring the actual voltage values for all activation states and using them to calculate the operating ranges. This approach allows for the elimination of the impact of wire resistance and the tolerance of resistors used in the alarm loop. Based on the obtained values, the operating ranges can be calculated as shown in Figure 7-a.

To implement the calibration method practically, for a finished installation with any number of sensors, it is necessary to measure the voltage for each activation state. Most of this procedure can be performed by the alarm control panel. The role of the installer is merely to activate the specified access point and communicate this to the control system of the panel. The measurement procedure must be carried out for all sensors in the perimeter loop. In the subsequent steps of the calibration procedure, the following actions should be performed:

- approaching the access point indicated by the alarm control panel and activating it;
- return to the alarm control panel and confirm the activation of the specified sensor;
- the alarm control panel indicates the next sensor to activate;
- deactivate the sensor that was previously activated;
- repeat the entire procedure for all sensors in the alarm circuit.

However, remote access to the control panel significantly reduces the time required for this process. Moreover, the calibration procedure is performed only once at the beginning, during the installation. The measured voltage values can be recorded and then used for monitoring the status of the alarm circuit. This approach allows installers to eliminate the effects of wire resistance and resistor tolerance, enabling the handling of a greater number of sensors.

3.3. Measurement Stand

To practically test the developed system, a special alarm control panel and manipulator with an alphanumeric display and keyboard were designed. The separation of functions into two devices allows the installer to place manipulator in any visible location and easily accessible location for the user, such as near the building's entrance doors. Meanwhile, the control panel should be located in the secured part of the monitored zone to make it more difficult for potential intruders to locate and disable the entire alarm system.

Both devices operate under the control of an ARM Cortex-M4 STM32F303CBT6 microcontrollers, which can operate at frequencies up to 72 MHz and features four 12-bit ADCs with support for up to 39 channels. Communication between the modules is carried out via a CAN 2.0a bus. The use of the CAN serial link allows for the connection of a larger number of devices and provides high resistance to interferences. This enables the system to be expanded in the future with additional modules, e.g., GSM wireless communication. The designed system also includes emergency operation capability on battery power, since it has to be resistant to power supply interruptions. The block diagrams of the main PCB boards are shown in Figure 9 and their visualisation in figure 10.

The control software was written in C language using high-level HAL (Hardware Abstraction Layer) libraries. Through the user interface, it is possible to change the settings of the alarm control panel and communicate the system's status to the user. When the alarm system is activated, the access panel retrieves the saved configuration settings from FLASH memory. After synchronization is complete, the main menu appears on LCD with information on the status of:

- alarm zones – the system has two independent zones;
- inputs – which input data is activated and calibrated;
- power supply – operating on battery or mains power, battery charge level.

A settings menu was also developed, allowing the following options:

- display configuration – adjustment of the brightness and contrast level;
- input configuration – selection of the input type NC, NO, EOL, 2EOL, 3EOL, custom connection system; selection of the number of sensors for the custom system;
- output configuration – selection of the default output state;
- zone configuration – assignment which inputs trigger a specific zone and which outputs are controlled by that zone.

If the settings are not configured correctly, the system will not allow access to the arming menu. If the custom connection system is selected, the calibration process is begun upon entering the arming menu (Fig. 11). This process involves measuring the voltages for all sensor activation states and using them to calculate the correct detection ranges.

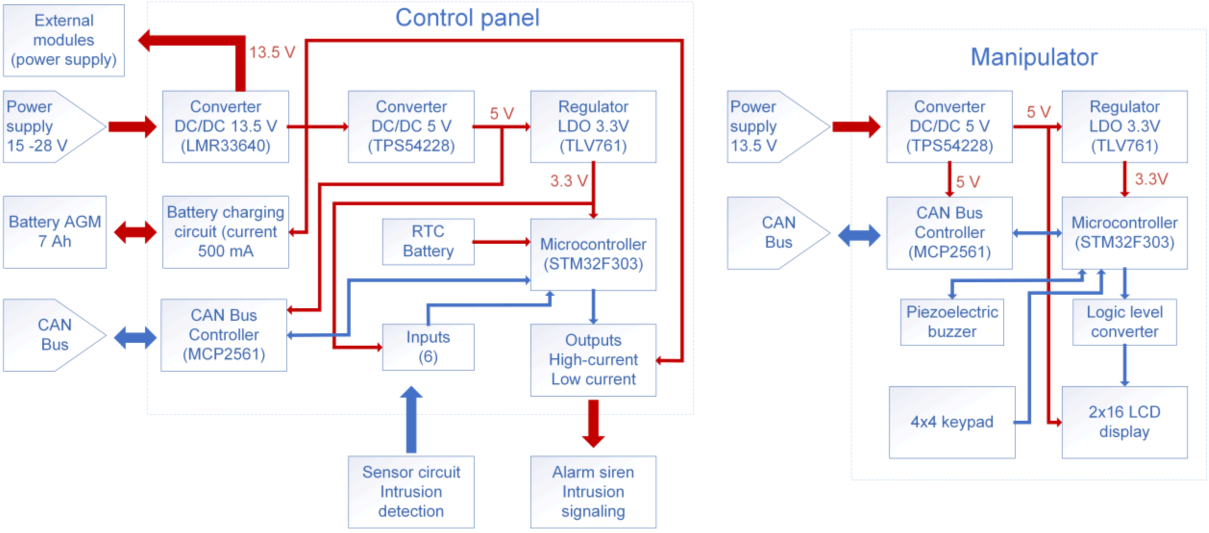
Control panel
External modules (power supply)
13.5 V
Power supply 15 -28 V
Converter DC/DC 13.5 V (LMR33640)
Converter DC/DC 5 V (TPS54228)
5 V
Regulator LDO 3.3V (TLV761)
3.3 V
Battery AGM 7 Ah
Battery charging circuit (current 500 mA
RTC Battery
Microcontroller (STM32F303)
CAN Bus
CAN Bus Controller (MCP2561)
Inputs (6)
Outputs High-current Low current
Sensor circuit Intrusion detection
Alarm siren Intrusion signaling
Manipulator
Power supply 13.5 V
Converter DC/DC 5 V (TPS54228)
5 V
Regulator LDO 3.3V (TLV761)
5 V
3.3V
CAN Bus
CAN Bus Controller (MCP2561)
Microcontroller (STM32F303)
Piezoelectric buzzer
Logic level converter
4x4 keypad
2x16 LCD display

Fig. 9. Block diagram of alarm control panel and manipulator: power supply connections are indicated in red; signal and control connections are in blue

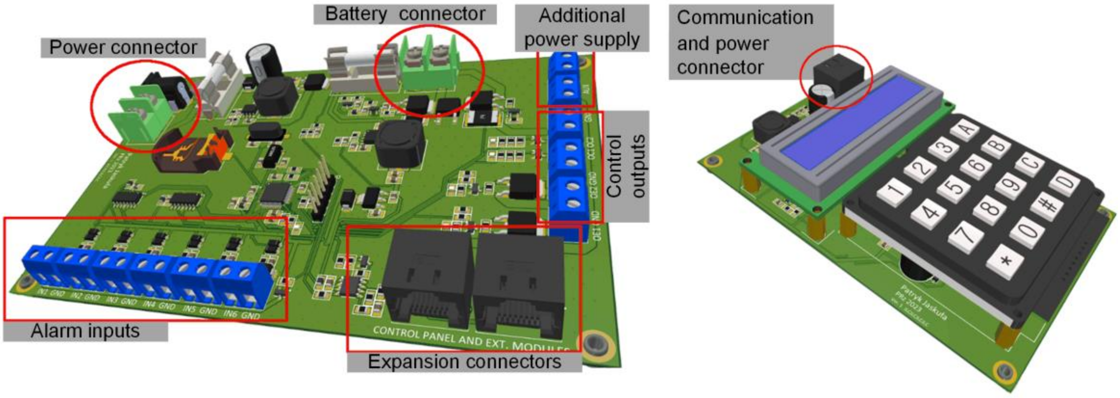

Fig. 10. 3D model of printed circuit boards

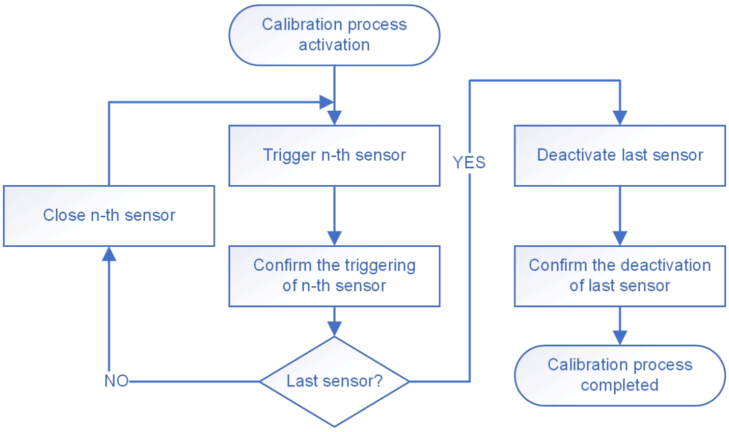
Calibration process activation
Trigger n-th sensor
Close n-th sensor
Confirm the triggering of n-th sensor
Last sensor?
NO
YES
Deactivate last sensor
Confirm the deactivation of last sensor
Calibration process completed

Fig. 11. Block diagram of calibration process

After the calibration process is completed, the measured voltage values are saved in FLASH memory to avoid the need for re-calibration in the event of a power loss. Then, the user can select the zone to be armed or disarmed. The system has two independent zones, which are armed with an 8-digit code consisting only of numbers. If an incorrect code is entered during disarming, an alarm is triggered. If any sensor on a line is triggered for a given input, a message appears showing the input number and sensor number.

3.4. System Tests

To evaluate the performance of the developed perimeter configuration, a test circuit was created. It consists of 20 sensors, each spaced 1 meter apart. The circuit loop in assembled using 2x0.5 mm YDY cable as well as parametrizing resistors with a value of 470 Ω and a tolerance of 1%. On the control panel side, a 47 Ω resistor is used as a pull-up resistor to the 3.3 V power supply in the voltage divider. The test circuit, along with the alarm system, is shown in Figure 12.

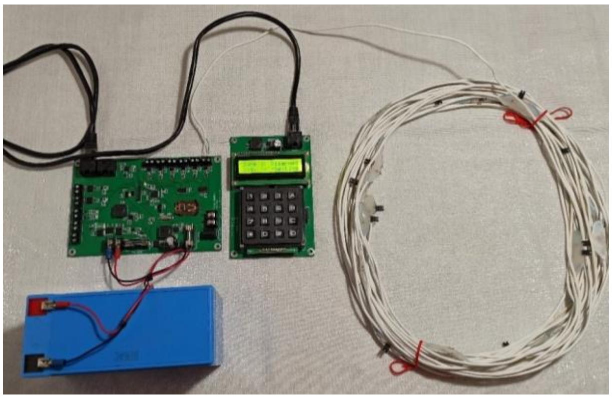

Fig. 12. Test perimeter loop, along with the alarm system

The obtained results of voltage measurement are presented in Figure 13, where they are plotted alongside the ideal values calculated for a resistor tolerance of 1%, taking into account the resistance of the cables.

The point where the curve based on the measurement intersects with the dashed lines determines the detection limits in relation to the ideal case (Fig. 13). Therefore, the maximum number of sensors that can be handled without errors for the designed circuit is 15. The intersection points for the curve calculated at the tolerance limit values are listed in Table 3. As can be observed, the intersection points for the measured values occurred for sensors located farther than the calculations for the worst-case scenario indicated. The measured voltage curve is situated between the curves calculated for extreme tolerances, confirming that the theoretical considerations closely approximate the system's behaviour. This allows the detection limits to be determined for installations with any number of sensors and cable lengths if a calibration method is not applied.

Table 3. Intersection points for curve calculated at tolerance limit values

	Calculations for 1 m and 1% tolerance		**Measurement**
	Max.	**Min.**	
Intersection points	13	19	15

To examine the noise level in the test perimeter loop, voltage fluctuations were measured by the A/D converter for the test circuit with 20 sensors. A total of 12,500 samples were collected at a sampling frequency of 12,500 Hz for three sensor activation cases in the circuit. The collected data is presented in four histograms in Figure 14.

For all cases, the read value varies by four quantization levels. The ADC voltage resolution is approximately 0.805 mV, which corresponds to a peak-to-peak value of the measured signal of 3.22 mV. This value represents the smallest signal change that the ADC can accurately distinguish. Anything below this is considered as the ADC's own noise and disturbances induced on the cable.

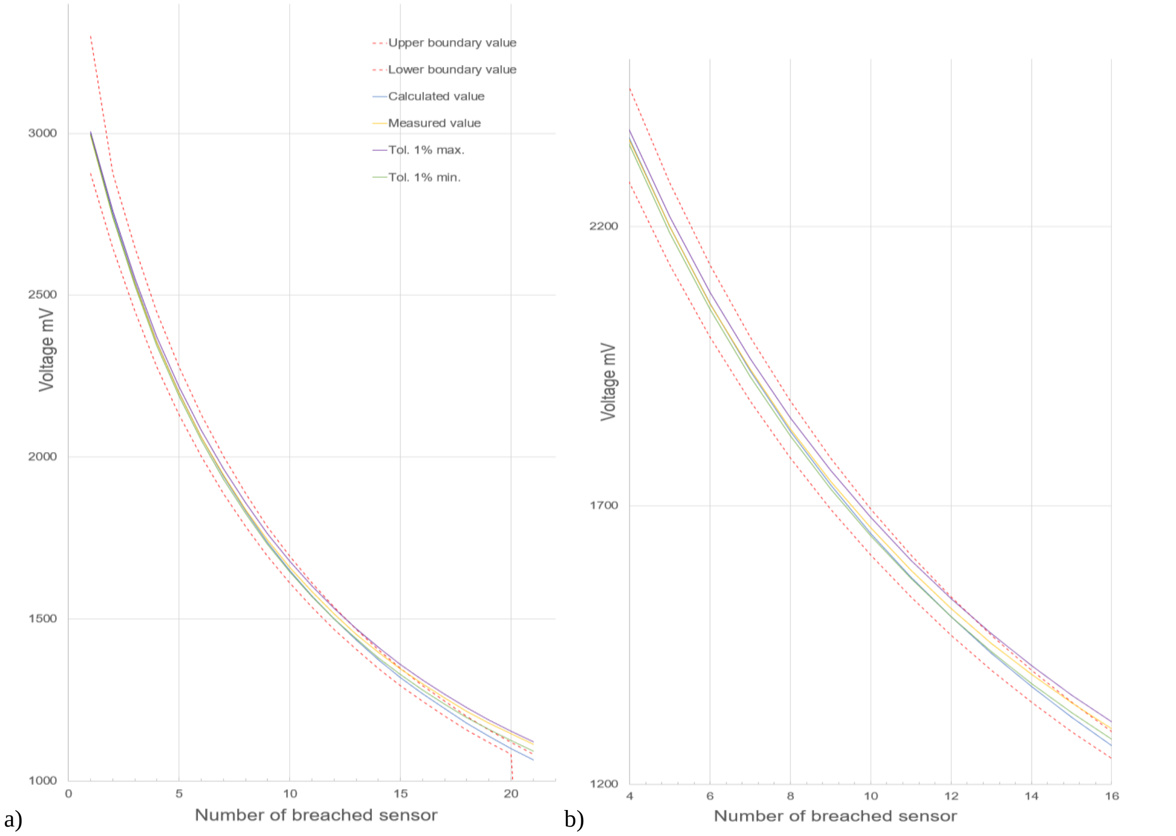

Fig. 13. Voltage at output of perimeter loop as a function of activated sensor; dashed curves indicate voltage variation limits for each activation state: a) Main graph; b) Enlarged section of graph

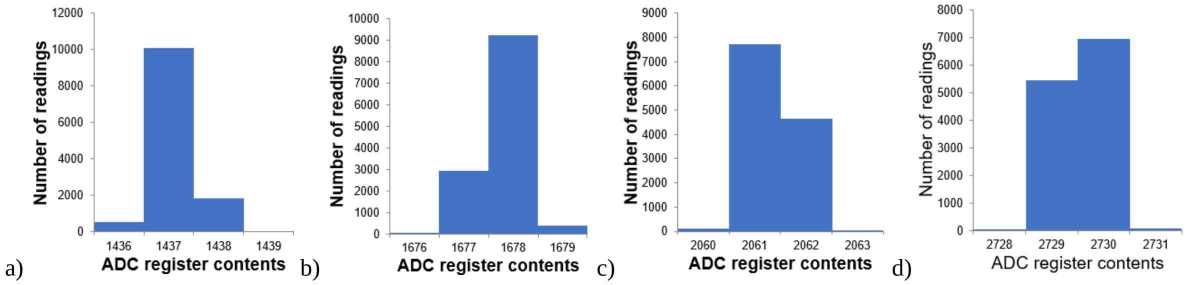

Fig. 14. Variation in values read from ADC: a) For 20th breached sensor; b) For 15th breached sensor; c) For 10th breached sensor; d) For 5th breached sensor

The level of noise depends on the electromagnetic environment in which the alarm system operates and cannot be estimated without specialized measurement equipment. However, during the calibration process, it is possible to determine the minimum voltage value below which the voltage on the perimeter line should not be reduced. This approach provides a margin for potential disturbances. Measurements from the test circuit allowed the determination of the minimum voltage value at which the system operates correctly. The smallest voltage change occurs with the activation of the last sensor and is 41 mV relative to the penultimate sensor. The maximum voltage change from the midpoint of the range for the last sensor's activation state is calculated as shown in Figure 7-a. This value is 20.5 mV and represents the threshold for the designed system using the calibration method. This confirms the proper operating of the system for a circuit with 20 sensors under real conditions. The chosen value is greater than the measured voltage changes to ensure a margin for additional disturbances.

4. Summary

In this work, an attempt was made to develop a proprietary configuration for a perimeter alarm system, which addresses the limitations of commercially systems available on the market. A parametrized configuration line was proposed that allows for the handling of a large number of sensors within a single monitoring loop. The developed perimeter loop ensures the ability to distinguish the activation of each detector using only two connecting wires. The developed system is compatible with any NC (normally closed) type sensors, such as reed switches. Additionally, the proposed connection method is straightforward to install, thanks to the standardization of the parametrizing resistors used in the circuit.

Furthermore, a calibration method was proposed to enhance the capabilities of the developed alarm system. The limit on the number of sensors depends on the accurate detection of individual states. Any disturbances in the circuit can lead to incorrect identification of which sensor has been triggered. Sensors near the end are most susceptible to this issue due to the small voltage change between consecutive activation states. Nevertheless, the calibration procedure significantly increases the number of access points in the perimeter loop.

To test the performance of the developed configuration for perimeter line, a demonstrator was built, consisting of an alarm control panel and an access manipulator. The effectiveness of the proposed connection configuration was tested in an alarm circuit with 20 sensors. Measurements showed that the most significant factor affecting the system's performance is the resistance of the connecting wires.

Thus, the Custom EOL configuration, utilizing the calibration method, can handle 20 access sensors in a single monitoring loop and allows for detecting where a breach has occurred. The system can successfully be used in facilities where multiple control points are required to be supervised and they are located close to each other. Moreover, the alarm system was designed with the possibility of expanding it with additional modules, such as a GSM wireless communication panel. An additional feature was the ability to operate even in case of a power failure, through the use of an emergency battery.

Literature

[1] G. Vardakis, G. Hatzivasilis, E. Koutsaki, N. Papadakis “Review of Smart-Home Security Using the Internet of Things,” *Electronics* 2024, vol. 13, no. 3343. doi: 10.3390/electronics13163343.

[2] T. Shi, P. Guo, R. Wang, Z. Ma, W. Zhang, W. Li, H. Fu, H. Hu, “A Survey on Multi-Sensor Fusion Perimeter Intrusion Detection in High-Speed Railways,” *Sensors* 2024, vol. 24, no. 5463, doi: 10.3390/s24175463.

[3] Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, A. Wibisurya, “Door Security System for Home Monitoring Based on ESP32,” *Procedia Computer Science* 2019, vol. 157, pp. 673-682, doi: 10.1016/j.procs.2019.08.218.

[4] M. H. Assaf, R. Mootoo, S. R. Das, E. M. Petriu, V. Groza, S. Biswas, “Sensor based home automation and security system,” *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, Graz, Austria, 2012, pp. 722-727, doi: 10.1109/I2MTC.2012.6229153.

[5] M. Kijima, Y. Miyagaw, H. Oshita, N. Segawa, M. Yazawa, and M. Yamamoto, “Poster Abstract: Multiple Door Opening/Closing Detection System Using Infrasound Sensor,” *2018 17th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, IEEE, Apr. 2018, pp. 126-127, doi: 10.1109/IPSN.2018.00026.

[6] S. Smith, J. Ellis, R. Abrams, “Chapter 8 - Central Alarm Stations and Dispatch Operations”, Editor(s): IFPO, “The Professional Protection Officer”, Butterworth-Heinemann, 2010, Pages 89-103, ISBN 9781856177467, doi: 10.1016/B978-1-85617-746-7.00008-0.

[7] George Risk Industries, Inc., “Magnetic Contacts with Built-In E.O.L Resistors and Resistor Packs,” *www.grisk.com*, access on 2024-11-12.

[8] H. Ali, H. Medjadba, L. M. Simohamed and R. Chemali, “Intrusion detection and classification using optical fiber vibration sensor,” *2015 3rd International Conference on Control, Engineering & Information Technology (CEIT)*, Tlemcen, Algeria, 2015, pp. 1-6, doi: 10.1109/CEIT.2015.7233060.

[9] M. Verma, R. S. Kaler, and M. Singh, “Sensitivity enhancement of Passive Infrared (PIR) sensor for motion detection,” *Optik (Stuttg)*, Oct. 2021, vol. 244, p. 167503, doi: 10.1016/j.ijleo.2021.167503.

[10] M. E. Kalinkina, A. G. Korobeynikov, O. I. Pirozhnikova, N. A. Shmakov, and V. L. Tkalich, “Designing of reed switches for sensors and security alarm devices,” *IOP Conf Ser Mater Sci Eng*, Feb. 2021, vol. 1100, no. 1, p. 012009, doi: 10.1088/1757-899X/1100/1/012009.

[11] T. Li, D. Han, J. Li, A. Li, Y. Zhang, R. Zhang, Y. Zhang, “Your Home is Insecure: Practical Attacks on Wireless Home Alarm Systems,” IEEE INFOCOM 2021 – IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2021, pp. 1-10, doi: 10.1109/INFOCOM42981.2021.9488873.

[12] S. Ramadhani and D. P. Putri, “Design of a Home Door Security System Based on NodeMCU ESP32 Using a Magnetic Reed Switch Sensor and Telegram Bot Application,” S*inkron*, Oct. 2023, vol. 8, no. 4, pp. 2059-2068, doi: 10.33395/sinkron.v8i4.12688.

[13] M. Boroš, A. Vel’as, V. Šoltés, J. Dworzecki, “Influence of the Environment on the Reliability of Security Magnetic Contacts,” *Micromachines* 2021, vol. 12, no. 401, doi: 10.3390/mi12040401.

[14] M. Boroš, A. Vel’as, Z. Zvaková, V. Šoltés, “New Possibilities for Testing the Service Life of Magnetic Contacts,” *Micromachines* 2021, vol. 12, no. 479, doi: 10.3390/mi12050479.

[15] A. S. Devi, A. K, B. C, A. Shali, D. Kavitha, and S. Hemavathi, “Smart Security System,” in *2022 1st International Conference on Computational Science and Technology (ICCST)*, IEEE, Nov. 2022, pp. 1–3, doi: 10.1109/ICCST55948.2022.10040301.

[16] K. Jakubowski, J. Paś, A. Rosiński, “The Issue of Operating Security Systems in Terms of the Impact of Electromagnetic Interference Generated,” *Energies* 2021, vol. 14, no. 8591, doi: 10.3390/en14248591.

[17] G. Uçtu, M. Alkan, İ. A. Doğru, M. Dörterler, “Perimeter Network Security Solutions: A Survey,” *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT),* Ankara, Turkey, 2019, pp. 1-6, doi: 10.1109/ISMSIT.2019.8932821.

[18] V Mach, A. Mizera, P. Stoklasek, M. Karhankova, M. Adamek, M. Bednarik, “Development of a Contact Glass-Break Detector for the Highest Security Level,” *Sensors* 2024, vol. 24, no. 97, doi: 10.3390/s24010097.

[19] P. Teixidó, J. A. Gómez-Galán, R. Caballero, F. J. Pérez-Grau, J. M. Hinojo-Montero, F. Muñoz-Chavero, J. Aponte, “Secured Perimeter with Electromagnetic Detection and Tracking with Drone Embedded and Static Cameras,” *Sensors* 2021, vol. 21, no. 7379, doi: 10.3390/s21217379.

[20] H. Xu, Y. Li, C. Ma, L. Liu, B. Wang, J. Li, “A Combined Sensing System for Intrusion Detection Using Anti-Jamming Random Code Signals,” *Sensors* 2022, vol. 22, no. 4307, doi: 10.3390/s22114307.

[21] Ropam Elektronik, “Porównanie central i terminali Ropam Elektronik”, (Product Catalogue), *ropam.com.pl*, access on 2024-11-12.

[22] Ropam Elektronik, “NeoLTE-IP-64, Neo-IP-64, NeoGSM-IP-64 Centrale alarmowe z komunikacją LTE/IP,” (Installation Instructions), Document version: 2.0, 2023-01-23, *ropam.com.pl*, access on 2024-11-12.

[23] A Tyco International Company DSC, “PowerSeries Neo HS2016/HS2016-4/HS3032/HS2064/HS2064 E/HS2128/HS2129 E Alarm Controller Reference Manual,” (Product Catalogue), *docs.johnsoncontrols.com/dsc*, access on 2024-11-12.

[24] A Tyco International Company DSC, “CENTRALE ALARMOWE HS2016/HS2032/HS2064/ HS2128,” (Installation and Programming Instructions), Document version 1.1, *www.montersi.pl*, access on 2024-11-12.

[25] Paradox, “SP Spectra. Control Panel Comparision Chart,” *paradox.ee*, access on 2024-11-12.

[26] Paradox, “Magellan/Spectra SP. Reference & Instalation” *paradox.ee*, access on 2024-11-12.

[27] Satel, “Made to Protect,” (Product Catalogue), 2024, *www.satel.pl*, access on 2024-11-12.

[28] Editorial Staff, “Why we use End of Line (EOL) Resistor in Fire and Gas System?”, Control and Instrumentation, *www.controlandinstrumentation.com*, access on 2024-11-12.

[29] System Automatycznej Kontroli Obiektu, “Parametryzacja NO/NC, EOL i 2EOL w systemach kontroli dostępu i alarmowych: Zalety parametryzacji wejść i stany konfiguracji” (NO/NC, EOL and 2EOL parameterization in access control and alarm systems: Advantages of input parameterization and configuration states), GMP Power, 21 November 2023, *sakokd.pl/blog*, access on 2024-11-12.