Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Distributed Perimeter Monitoring System for Industrial Facilities Using Artificial Intelligence

Tofig Mansurov

tofiq.mansurov@aztu.edu.az

Sergey Zhdanovich
Elnur Mansurov
Tatiana Kovalenko

Article

Keywords:

Posted Date: November 24th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11562707/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Distributed Perimeter Monitoring System for Industrial Facilities Using Artificial Intelligence

Tofig Mansurov[1*], Sergey Zhdanovich[2], Elnur Mansurov[1], Tatiana Kovalenko[2]

[1*]Azerbaijan Technical University, Baku, Azerbaijan Republic.
[2]Belarusian State Academy of Telecommunications, Minsk, Republic of Belarus.

*Corresponding author(s). E-mail(s): tofiq.mansurov@aztu.edu.az;
Contributing authors: zsvzsv@tut.by; mansurovelnur@mail.ru;
tgkov@yandex.by;

Abstract

Industrial facility security is ensured by the creation of a dynamic distributed monitoring system that can quickly adapt to rapidly changing perimeter security monitoring conditions. This analysis of the subject area identified the deficiencies of existing systems, and developed a distributed perimeter monitoring system for industrial facilities using telecommunication fiber as a sensing element. The system enables continuous monitoring of the perimeter of industrial facilities using telecommunication fiber as a sensor. It detects unauthorized intrusion when optical radiation levels change, ensures reliable operation of industrial facilities when external influences occur, and automates the diagnostic and security monitoring process for industrial facilities. This work aims to improve operational efficiency, monitor the perimeter of industrial facilities in hazardous conditions, and promptly identify and localize emerging threats. This work aims to expand capabilities, thereby creating a unified platform for monitoring and managing industrial facility security.

Keywords: industrial facility, perimeter, telecommunication fiber, sensor, artificial intelligence, neural network, distributed monitoring system

1 Introduction

Fiber-optic cables, typically used for transmitting data, can also serve as sensors in distributed perimeter monitoring systems for industrial facilities. They are capable of detecting unauthorized intrusions and mechanical disturbances—such as impacts, deformations, vibrations, and other external influences—affecting the optical fiber. Such solutions are widely employed in modern security systems, particularly for establishing security perimeters around industrial sites. The advantages of contemporary fiber-optic technologies stem from their immunity to electromagnetic interference and their high level of electrical safety. Furthermore, standard telecommunication fibers can often function as sensing elements; they are readily available and more cost-effective than specialized sensing cables. External mechanical disturbances alter the properties of a telecommunication fiber, which in turn affects the characteristics of the optical signal propagating through it. Currently, the development of distributed perimeter monitoring systems for industrial facilities—leveraging machine learning and artificial intelligence (AI)—is a highly relevant and pressing objective.

A distributed perimeter monitoring system for industrial facilities that incorporates artificial intelligence represents a next-generation, end-to-end high-tech solution designed to ensure comprehensive physical security and minimize the risk of unauthorized access to strategically important sites. For large-scale operations—such as oil and gas infrastructure, ports, and energy or industrial complexes—traditional security approaches are becoming increasingly less effective. The integration of artificial intelligence algorithms fundamentally shifts the paradigm of physical security.

Research exists on the development of distributed monitoring systems for industrial facilities, with each system performing specific control functions [1–3]. The operation of various industrial sites necessitates the creation of a distributed perimeter monitoring system, which requires a comprehensive approach. In such a system, a telecommunication fiber—laid along the perimeter of the protected site—is used as a sensing element (sensor). It has been established that any unauthorized interference with the telecommunication fiber causes a change in the attenuation of the optical signal propagating through it [4, 5].

Traditional technical security systems, which rely on simple sensors and manual video analysis, suffer from several critical drawbacks, including a high rate of false alarms, challenges posed by complex topographical conditions, and the "human factor." Continuous monitoring of dozens or even hundreds of video feeds leads to rapid human fatigue, which in turn increases the risk of failing to detect actual threats.

The objective of this work is to develop a distributed perimeter monitoring system for industrial facilities that incorporates artificial intelligence methods. This approach facilitates security planning and ensures the safety, reliability, and operational efficiency of various industrial sites, representing a significant and timely research task with both theoretical and practical implications.

2 Distributed industrial facility perimeter monitoring system using artificial intelligence

When developing a distributed industrial facility perimeter monitoring system, the use of artificial intelligence allows for the creation of systems capable of solving intelligent problems using a variety of approaches, while a neural network performs data-based learning using applied mathematical tools.

The operating algorithm for the distributed industrial facility perimeter monitoring system is used to detect mechanical impacts on telecommunications fiber optics and consists of the following steps [3, 5]:

- collecting data from various sensors during unauthorized intrusions on telecommunications fiber optics;
- data preparation, i.e., processing and adapting information for further use in detecting unauthorized intrusions;
- model training, i.e., studying data to perform specific applied tasks, such as detecting unauthorized intrusions; the program analyzes the data and finds patterns;
- testing and optimization—after training, the model is tested on new data to evaluate incoming information about unauthorized intrusions from various sensors, and, if necessary, the algorithms are further tuned and improved;
- real-time operation, i.e., after successful testing and optimization, the model is ready for use in real-world conditions, for example, for classification or decision-making based on sensor data.

Artificial intelligence consists of three components: an executive system, a knowledge base, and an intelligent interface.

The first component is the executive system, which executes programs designed to effectively detect unauthorized intrusions.

The second component is the intelligent interface, which enables adaptation to a wide range of end-user needs.

The third component is the knowledge base, which facilitates interaction between the first two components.

Figure 1 shows a model of a distributed system for monitoring the perimeter of industrial facilities using artificial intelligence.

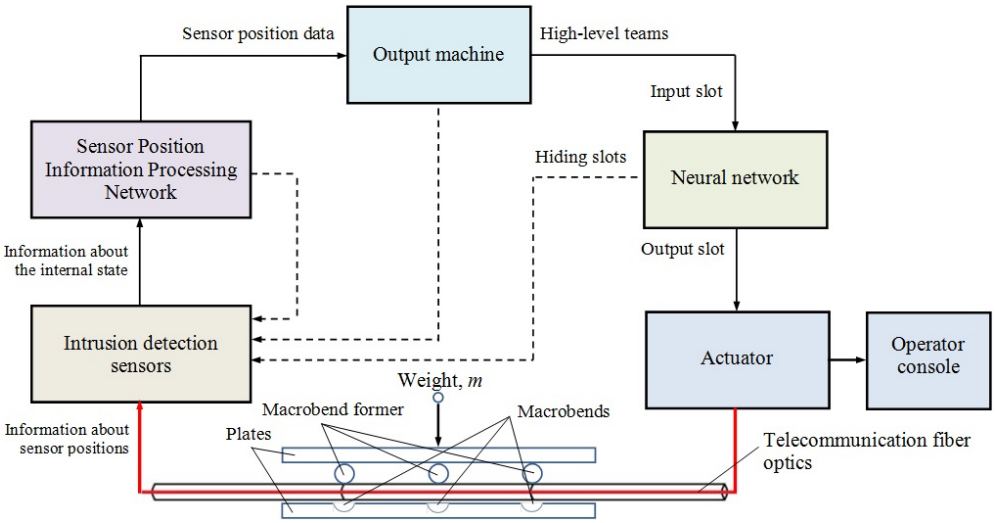


Fig. 1 Model of a distributed perimeter monitoring system for industrial facilities using artificial intelligence

The model of a distributed industrial perimeter monitoring system using artificial intelligence is a multi-layered architecture capable of detecting unauthorized intrusion into a telecommunications fiber optic cable, processing data from sensors, making decisions using a neural network, and controlling an actuator. Each system node performs a specific function.

As shown in Figure 1, the distributed industrial perimeter monitoring system consists of an inference engine, a neural network, an actuator, an operator console, an intrusion detection sensor, a sensor position processing network, and a telecommunications fiber optic cable used as a sensor.

3 The operating principle of a distributed perimeter monitoring system for industrial facilities

In the initial state of a distributed industrial facility perimeter monitoring system, all sensors in the system are also in their initial state. When an unauthorized intrusion with a certain mass m occurs on a telecommunications fiber, it undergoes macrobending, and some of the optical radiation intensity through the fiber's core and cladding escapes beyond the fiber, thereby reducing the primary optical radiation level in accordance with the location and mass m of the unauthorized intrusion.

The primary (raw) signals received from the sensors are converted into a stable macrosignal suitable for further analysis. Physical parameters, such as the location of the unauthorized intrusion and the mass m, are also generated here. The network processing information on the positions of the telecommunications fiber optic sensors analyzes the sensor status, verifies the signals, pre-filters, and prepares the data. The processed information is transmitted to the "Inference Engine" module. This module

is the logical control center, generating high-level commands based on processed data on the positions of telecommunication fiber-optic sensors and sending decisions to the neural network, actuator, and operator console.

An inference engine, based on the received information, performs a logical inference from a pre-constructed fact base [5–7]. In this case, a fact is a statement that is true when an event occurs, for example: "There is an unauthorized entry." A rule in this case is a parameterized statement consisting of two parts: a condition and a result, for example: "If there is an unauthorized entry, then the unauthorized entry is a violation of the perimeter of industrial facilities." If the condition is true for unauthorized entry, then the rule is converted into a fact: "An unauthorized entry is a violation of the perimeter of industrial facilities." An inference engine can typically perform one or both of the following operations:

- fact verification—a fact is considered true if it can be deduced according to the laws of formal logic from the existing fact and rule base;
- finding the set of parameter values for a given rule that converts the given rule into a true fact.

In most cases, the inference engine concludes that a fact is false if its truth is not deducible from the fact and rule base. However, this can lead to misinterpretation of knowledge, since the results "Unauthorized entry is false" and "Unauthorized entry is unprovable" are indistinguishable. An inference engine is a generalized problem-solving procedure that, based on the knowledge base and in accordance with the user's information needs, constructs a chain of reasoning (logically connected units of knowledge) leading to a specific result.

The inference engine formulates high-level commands based on the received data on the positions of telecommunication fiber optic sensors and transmits them as source data through input slots to the neural network.

The neural network provides intelligent information processing, receiving data from the inference engine and signal processors through input and hidden slots, and generating low-level commands for actuators through output slots. The neural network also identifies anomalies, predicts complex situations, and filters out false positives and borderline events. After determining the truth of the fact, the neural network generates low-level commands about unauthorized access and transmits them to the actuator via the neural network's output slots. From the actuator's output, information about unauthorized access to the telecommunications fiber is transmitted to the operator console to alert technical personnel and initiate the necessary measures to resolve the situation.

4 Experimental setup and research methodology

In the experimental studies, a single-mode telecommunication optical fiber—with parameters conforming to the ITU-T G.655 recommendation—was selected as the sensing element. This fiber exhibits higher microbending sensitivity than other types of single-mode telecommunication optical fiber used in optical data transmission systems [4, 8].

Figure 2 shows the experimental setup for the studies and includes an optical radiation source with wavelengths of 650, 1310, 1490, 1550, and 1625 nm, an optical radiation power meter, telecommunication optical fiber, textolite plates 1 and 2, and microbending formers, which are metal wires of varying diameters.

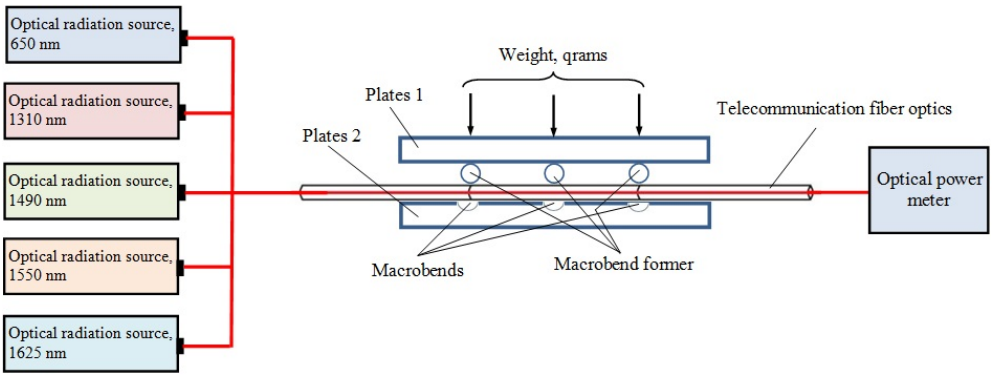


Fig. 2 Scheme of the experimental setup for conducting research

During the studies, an optical tester (OT 3-1) was used as a source of optical radiation and an optical power meter. From the source's output, optical radiation enters the input of a telecommunications optical fiber in the studied wavelength range of 650, 1310, 1490, 1550, and 1625 nm, which corresponds to the "transparency windows" of single-mode telecommunications optical fiber [8, 9]. The power of optical radiation entering the input of the telecommunications optical fiber was 1.0 mW for all wavelengths.

The telecommunications optical fiber is connected to a source and optical power meter. During the experiments, the length of the telecommunications optical fiber did not exceed 5 m, so optical power losses in the studied telecommunications fibers can be neglected.

Microbends $1, \ldots, n$ are formed on the telecommunications optical fiber using metal wires with a diameter of 200 μm, positioned perpendicular to the telecommunications optical fiber [9]. Wire diameters greater than 200 μm cause the telecommunications optical fiber to fracture, while wire diameters less than 100 μm cause virtually no attenuation of optical radiation at the microbend.

The microbend is formed by compressing the wire and the telecommunications optical fiber between textolite plates 1 and 2 using a force generated by a load of mass m, which is positioned on plate 1 and plate 2 on a horizontal, hard surface. The textolite plate 1 and the load have a mass m, which is sufficient to form microbends in telecommunication optical fiber. As the mass m increases, the attenuation of optical radiation power due to microbends increases. Experimental studies determined the

attenuation of optical radiation power introduced by microbends:

$$P_{rp} = 10 \lg \left(\frac{P_{inp}}{P_{out}} \right), \tag{1}$$

where P_{inp} is the power of the optical radiation source at the input of the telecommunication optical fiber; P_{out} is the power of the optical radiation at the output of the telecommunication optical fiber, entering the input of the power meter.

The sensitivity of sensors on microbends of telecommunication optical fiber formed under the influence of a certain mass m is characterized by the value α, determined by the formula:

$$\alpha = \frac{\Delta D_m}{\Delta m} = \frac{D_{1m} - D_{2m}}{m_1 - m_2} \text{ dB/gram}, \tag{2}$$

where ΔD_m is the change in the attenuation of the optical radiation power; Δm is the change in the acting mass; D_{1m} is the attenuation of the optical radiation power in a telecommunications optical fiber when exposed to a force created by the mass m_1; D_{2m} is the attenuation of the optical radiation power in a telecommunications optical fiber when exposed to a force created by the mass m_2.

The stability of optical radiation sources and the properties of single-mode telecommunication fiber, as well as the parameters of the optical power meter, were achieved by adhering to measurement conditions in accordance with the requirements of ISO/IEC 17025-2019. The studies were conducted at an ambient temperature of 20–25 °C, humidity up to 70%, and atmospheric pressure of 975–1025 GPa.

5 Results and discussion

This section of the article on the implementation of artificial intelligence (AI) in distributed perimeter monitoring systems for industrial facilities presents key performance metrics, comparative analysis data, and an assessment of practical significance.

In [3, 4], studies were carried out in the course of which it was established that an increase in the diameter of the wire microbending former leads to an increase in the attenuation of the optical radiation power at the microbending of the telecommunication optical fiber at a constant value of the mass acting on it, and it was also determined that the highest value of sensitivity to the mass of action is observed for the G.655 telecommunication optical fiber, and the maximum sensitivity is achieved at an optical radiation wavelength of 1625 nm. In the course of this study, several microbends located at different distances from each other were used to create the telecommunication optical fiber sensor, and a wire with a diameter of 200 μm was used as a microbending former.

During the study, the dependences of optical radiation power attenuation for wavelengths of 1310, 1490, 1550, and 1625 nm were determined for telecommunication fiber optic sensors created by forming two, three, and five microbends in G.655 telecommunication fiber. Typical dependences of optical radiation power attenuation D_m on the mass m of the load forming the microbends are shown in Figure 3 for one, three, and five microbends spaced at 0.7 cm intervals at a wavelength of 1625 nm.

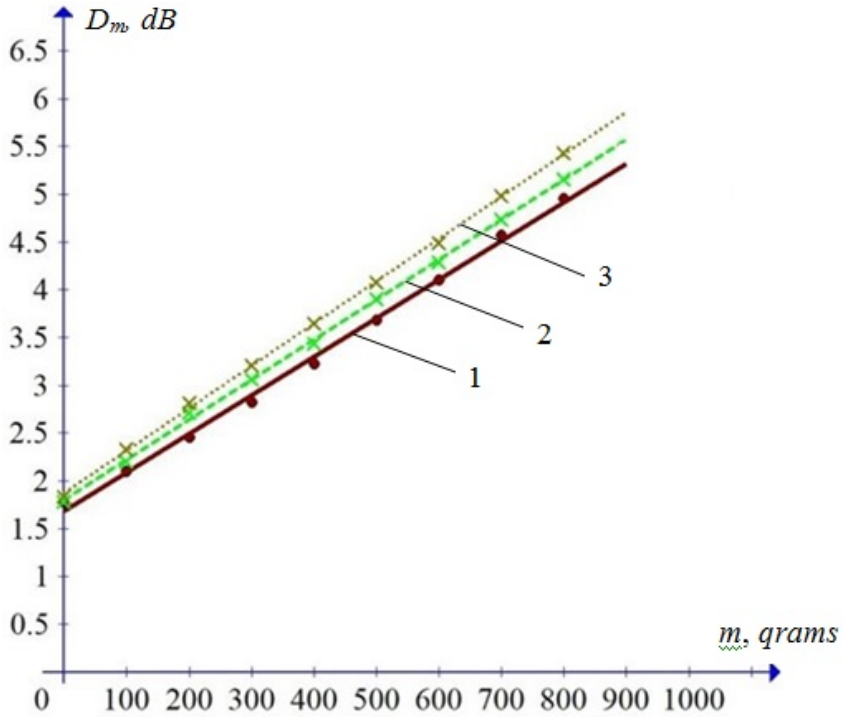


Fig. 3 Optical power attenuation versus mass for a wavelength of 1625 nm: 1—one microbend; 2—three microbends; 3—five microbends, 0.7 cm pitch

Figure 4 shows the dependences of optical radiation power attenuation D_m on the number of microbends formed at 0.7 cm intervals for different masses m at a wavelength of 1625 nm.

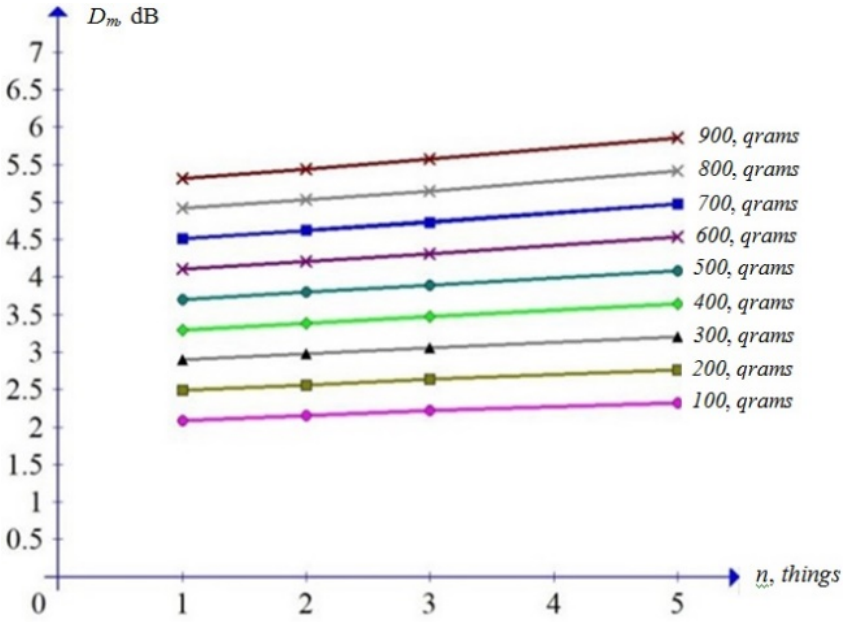


Fig. 4 Dependences of optical radiation power attenuation on the number of microbends formed in 0.7 cm increments for different masses (100–900 grams) at a wavelength of 1625 nm

Figure 5 shows the dependences of the attenuation of the optical radiation power D_m on the mass m of the load, which forms three microbends located at a step of 0.7 cm using optical radiation with a wavelength of 1550 nm and 1625 nm.

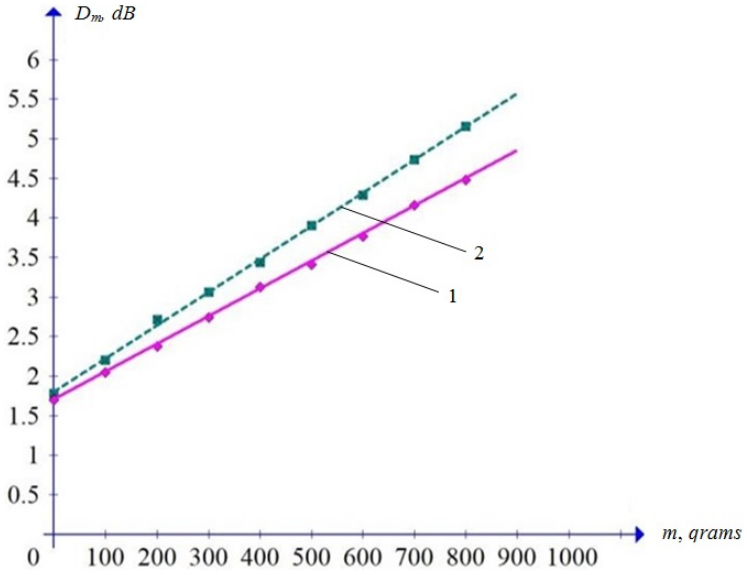


Fig. 5 Dependences of optical radiation power attenuation on mass for wavelengths of 1550 nm and 1625 nm for three microbends formed with a step of 0.7 cm: 1—wavelength 1550 nm; 2—wavelength 1625 nm

The sensitivity values of the G.655 optical fiber microbending sensor for the studied wavelengths of 1550 and 1625 nm and different numbers of optical fiber microbendings are presented in Table 1.

Table 1 G.655 optical fiber microbending sensor characteristics

Microbends		Wavelength,	D_{1m},	D_{2m},	α,
Quantity, pieces	Pitch, mm	nm	dB	dB	dB/gram
1	0.0	1625	2.11	4.95	0.0041
3	0.7	1550	2.05	4.47	0.0035
3	0.7	1625	2.20	5.16	0.0042
5	0.7	1625	2.33	5.43	0.0043

6 Conclusion

Thus, a dynamic distributed perimeter monitoring system for industrial facilities has been developed, enabling automated diagnostics and security monitoring of industrial facility perimeters. This system aims to improve operational efficiency, monitor the perimeter of industrial facilities in hazardous situations, and promptly identify and localize emerging threats. This system expands capabilities, thereby creating a unified platform for monitoring and managing industrial facility security.

The results of the experiment demonstrated that microbending of G.655 telecommunications fiber can be used to create a mass sensor formed by a 200-μm-diameter metal wire at an optical wavelength of 1625 nm. It was demonstrated that increasing the number of microbends increases the sensitivity of the telecommunications fiber optic sensor, but at the same time, the attenuation of the optical radiation increases. After the optical radiation passes through the telecommunications fiber optic sensor, the optical radiation received by the power meter is at a lower power. Since the lower power measurement range is limited, increasing the number of microbends to increase the sensitivity of the telecommunications fiber optic sensor requires increasing the power of the optical radiation source.

Acknowledgements. This work was supported by the Azerbaijan Science Foundation—Grant № AEF-BQM-BRFTF-4/2024-5(53)-06/02/1-M-02 and Belarusian Republican Foundation for Basic Research as part of the research project "Principles of creating combined sensors based on telecommunication optical fiber".

References

[1] Kovalenko, T.G., Zhdanovich, S.V.: Fiber-optic sensor based on microbending of optical fiber. Probl. Infocommun. **20**(2), 10–16 (2024)

[2] Vyalyshev, A.I.: Fiber-optic sensors for monitoring the state parameters of objects and the environment in monitoring tasks. Nat. Manag. (3), 32–37 (2014)

[3] Kovalenko, T.G., Zenevich, A.O., Zhdanovich, S.V., Novikov, E.V., Matkovskaya, T.A.: Study of microbending parameters of single-mode optical fiber for mass sensors. Izv. Univ. Instrum. Eng. **67**(1), 96–102 (2024)

[4] Vasilevsky, G.V.: Using optical fiber macrobending as a basis for creating a mass sensor. News Univ. Instrum. Eng. **63**(10), 930–937 (2020)

[5] Patterson, R.I., *et al.*: A fiber-optic current sensor for aerospace applications. IEEE AES Syst. Mag. **5**, 10–14 (1990)

[6] Yamagata, Y., *et al.*: Development of optical current transformer and application to fault location systems for substations. IEEE Trans. Power Del. **8**(3), 10–16 (1993)

[7] Gulakov, I.R., Zenevich, A.O.: Fiber-Optic Sensors of Physical Quantities: Monograph. Belarusian State Academy of Telecommunications, Minsk (2022)

[8] Gulakov, I.R., Zenevich, A.O., Mansurov, T.M.: Fiber-Optic Communication Lines. Belarusian State Academy of Telecommunications, Minsk (2020)

[9] Udd, E., Spillman Jr., W.B.: Fiber Optic Sensors: An Introduction for Engineers and Scientists. Wiley, Hoboken (2011)