ACTA PHYSICA POLONICA A No. 4 Vol. **146** (2024)

Proceedings of the 21st International Conference on Global Research and Education (Inter-Academia 2024)

Experimental Tests on the Fire Resistance of Wooden Fire Doors

M. Bartyś*

Institute of Automatic Control and Robotics, Warsaw University of Technology, św. A. Boboli 8, 02-525 Warsaw, Poland

Doi: 10.12693/APhysPolA.146.361

*e-mail: `michal.bartys@pw.edu.pl`

This paper presents the selected results of experimental tests on the fire resistance of wooden fire doors. It focuses on answering two questions. The first, of a technical nature, is an attempt to answer whether wood, due to its combustible properties, can be used in the construction of fire doors. The second, methodological, is an attempt to indicate the advisability of carrying out experimental research to identify the complexity of physicochemical phenomena. The paper structurally consists of two main parts, namely technical and research. The first part presents the architecture of a prototype wireless distributed network system for fire hazard research and monitoring. The second part of the paper presents selected results of experimental tests performed in the fire testing laboratory using the developed system. The analysis of the obtained experimental results allowed conclusions of a practical nature to be drawn regarding the applicability of the developed system in commercial fire doors. The final section of the paper presents conclusions and directions for further development.

topics: experimental studies, fire resistance test, fire doors, wireless measurement and data acquisition systems

1. Introduction

For obvious reasons, the typical materials used for fireproof doors are steel or aluminium alloys and mineral wool [1, 2]. The use of wood for this purpose may be considered rather surprising due to its flammability and physicochemical properties [3, 4]. Nevertheless, under certain circumstances, the use of wood for fire-resistant doors is desirable due to the special architectural requirements placed especially on renovated and/or modernised museums, palaces, theatres, cinemas, or buildings with a high standard of interior design. The question, therefore, arises as to whether the use of wooden fire doors is at all possible and, if so, under what conditions and whether such doors can be given technical approval.

The modelling of the fire resistance is the subject of numerous analytical and simulation studies [5]. Nevertheless, the technical approval of the fire resistance still requires a series of experimental tests in accredited test laboratories.

In the event of a fire, fire doors should not allow an excessive rise in the average temperature measured on the surface of the door on the side opposite to this exposed to the fire. The allowable temperature rise should not exceed 140°C. The thermal separation capability is assessed in standard fire resistance tests and determined by the parameter EI xx, where xx is the number of minutes for which the tested door meets the conditions of tightness and thermal insulation and does not allow the spread of flames in the event of a fire. Standardised values for the parameter xx are 30, 60, 90, 120. The question arises: can wooden doors be designed to achieve at least EI 30 resistance? This question will be answered in this paper.

In this paper, we will not be concerned with the design of the doors themselves, but will focus our attention on how the doors can be equipped to reduce the risk of harm to property, human health and life, and the environment in the event of a fire emergency.

The paper, therefore, asks whether, in addition to mandatory passive fire protection, the doors should be able to monitor the ambient temperature in combination with predicting and signalling fire hazards. Equipping fire doors with such devices would make it possible to locate the source of the fire and provide rapid and early warnings. Among other things, this would enable a rapid response by the relevant fire protection services.

In recent years, the *internet of things* (IoT) concept has gained particular importance in industry [6–9]. This is because it has enabled the intensive exchange of information between smart devices. This has resulted in the development of many new applications, fostering increased production efficiency and contributing to improved functional safety. When referring to real-time industrial applications, the terminology *industrial internet of things* (IIoT) is used instead of IoT.

In this paper, we will present the concept of a fire risk monitoring system based on the application of original IIoT devices concerning fire doors and intended for experimental and commercial use. The paper contributes both to system design and experimental investigations. In particular, the design of IIoT devices that meet the conditions for applicability in fire doors and are robust enough to withstand high operating temperatures will be presented.

The structure of the paper is as follows. After the short introduction and motivation of the paper presented in Sect. 1, the concept of a cloud-based distributed fire risk monitoring system will be presented in Sect. 2. Section 3 will be devoted to the design of IIoT devices. Experimental tests and a discussion of the obtained results with a view to assessing their practical applicability are presented in Sect. 4. Conclusions, comments, and recommendations, as well as an announcement of further work, are presented in Sect. 5.

2. Cloud-based fire door monitoring system

This paper introduces, among others, smart IIoT devices specifically designed for use in fire doors. Essentially, they are just components of a complex, distributed, cloud-based data acquisition, monitoring, and warning system. Due to the scope of this paper, we will not discuss the entire system in detail. Nevertheless, the fire risk cloud-based monitoring and warning system will be characterized synthetically to give an idea of the place and role of IIoT devices. Figure 1 depicts a general block diagram of this system.

The distributed, cloud-based fire door monitoring system is a wireless IT communication system designed to collect and analyse data from IIoT devices. Three channels of communication are used for this purpose:

(i) Bluetooth 5.0,
(ii) GSM,
(iii) Ethernet.

The entire system includes both hardware and software components. The hardware components of the system are IIoT and access devices. The IIoT devices operate in the local broadcasting mode. The data packets spread by the IIoT devices are transmitted via the GSM infrastructure to the cloud server system via local access devices acting as network hubs.

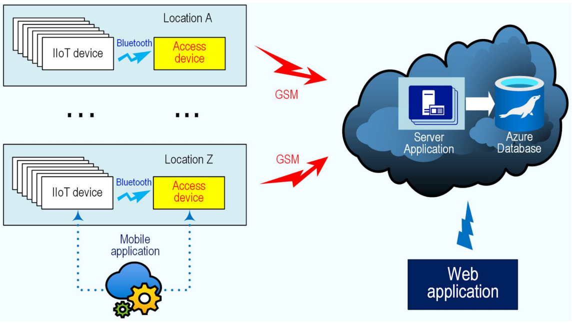

Fig. 1. Block diagram of a distributed, cloud-based fire door data acquisition, monitoring, and warning system.

A server application is implemented in the cloud computing system, co-operating with a database. Access to the cloud computing system is realised via a web application. It enables both the system administrator's tasks and the processing and visualization of the acquired data. In addition, a mobile application enables the configuration and commissioning of the hardware components of the network system (both IIoT and access devices).

3. IIoT smart device

Several critical functional requirements have been formulated for the IIoT smart devices. Among the most important are:

- temperature monitoring,
- thermal robustness,
- encrypted remote and local access,
- ultra-low power consumption,
- embedded supply,
- small dimensions,
- economics.

3.1. Mechanical design

For ease assembly and disassembly, the housing of the IIoT device has been designed in the form of a two-part thin-walled tube made of amorphous *acrylonitrile-butadiene-styrene terpolymer* (ABS). ABS is characterised by its hardness and impact resistance. ABS also has good insulating properties. It does not absorb electromagnetic waves. It changes to a plastic liquid state at temperatures between 190 and 240°C.

The housing of the IIoT device consists of two pieces, i.e., a cylindrical body and a lid. The body is made as a thin-walled cylinder with an outer diameter of 29.5 mm and a height of 42.5 mm. The

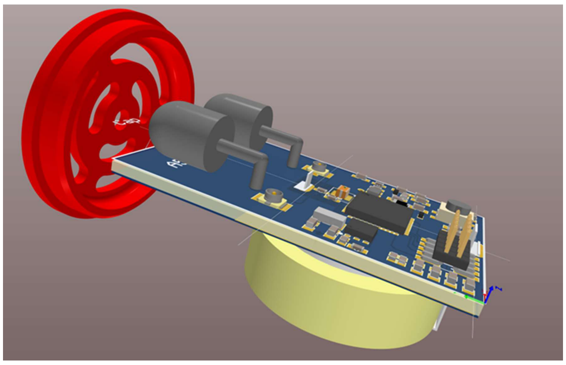

Fig. 2. Isometric view of the interior of the IIoT device. Two helical antennas, two UFL connectors for connecting external antennas, the central unit, and the electrochemical cell (yellow) are visible.

thickness of the walls and bottom of the cylinder is 1 mm. The lid is cylindrical with an outer diameter of 29.5 mm and a height of 4.5 mm. The face of the lid is perforated for good contact with the surrounding atmosphere.

The diameter and height of the body and lid have been selected so that the housing fits into the door frame and its installation requires only a hole of ⌀30 mm and a depth of 43 mm.

The IIoT device (Fig. 2):

- is made in the form of a 24.5 × 41.5 mm glass-epoxy,
- has laminated printed circuit board,
- is designed to operate in environmental conditions specified by an ambient temperature ranging from −40 to 85°C and a relative humidity of up to 100%,
- contains autonomous temperature and humidity sensor,
- is equipped with two pre-installed helical antennas selected for 868 MHz and 2.4 GHz bands,
- has two plugs for optional connection of external flexible antennas,
- enables bidirectional serial communication with both access devices and IIoT devices,
- is powered exclusively from an electrochemical lithium cell soldered directly to the printed circuit board.

The IIoT device uses the CC1352R1 microcontroller from Texas Instruments. It features an Arm Cortex-M4 core, clocked at 48 MHz. The microcontroller has 80 KB of RAM, 8 KB of cache memory, and a built-in RF processor operating in the bands 2.4 GHz and 433 MHz or 868 MHz or 915 MHz. A TI-RTOS real-time system was installed in the IIoT along with a Bluetooth 5.0 stack.

3.2. Modes of operation

The IIoT device operates in two basic modes:

(i) initialisation mode

and

(ii) normal operation mode.

Initialisation mode is triggered automatically for a brand new device. Initialisation involves storing relevant data in the non-volatile memory of the IIoT device's processor, including:

- the device unique identifier,
- the private key for the digital signature,
- the public key for verifying the digital signature.

The initialisation process is carried out from a dedicated mobile application. Once this process is completed, the device automatically enters normal operation mode. In this mode, the IIoT periodically measures the ambient temperature and relative humidity. For most of the time in normal mode, the microcontroller remains in deep sleep mode. Then, temperature and humidity measurements are taken every 5 s by the integrated sensor of environmental parameters. Once an hour, the microcontroller is woken up to transmit the result of the last measurement. The information is sent to an access device and then from the access device to a cloud-based application.

When temperature exceeds 50°C, the sensor immediately awakens the microcontroller of the IIoT device. The microcontroller then verifies the likelihood of a fire hazard based on trend analysis of the temperature. If the fire hazard is confirmed, the microcontroller increases the frequency of transmission of the measurements to the access device. The device then broadcasts measurements once every 30 s until destruction or when the temperature value falls below 50°C.

In normal operation mode, the IIoT communicates with the access device using the advertising function of the Bluetooth 5.0 standard. This function enables the transmission of a data frames in broadcast mode. Communication is carried out using the LE Coded S8 physical layer. This layer uses the *forward error correction* (FEC) algorithm [10, 11], allowing communication errors to be corrected.

In order to verify both the source of the data and its integrity, the IIoT device signs the communication frame using the *Elliptic Curve Digital Signature Algorithm* (ECDSA) [11–13]. It uses an asymmetric encryption algorithm based on elliptic curves, which encrypts the hash function determined from the data frame. The encryption is implemented using hardware support from IIoT embedded microcontroller.

3.3. Access device

Due to the limited transmission power, the communication range of IIoT devices does not exceed 100 m in open space. In enclosed spaces, the range is much shorter and, in extreme cases, may not exceed 10 m. Therefore, a system architecture concept was adopted in which the communication of the IIoT devices with the cloud server takes place via an access device.

The task of the access device is to receive packets transmitted locally by IIoT devices and then forward them via the HTTP mechanism of the cloud server. The access device, like an IIoT, operates in two modes:

(i) initialisation mode

and

(ii) normal operation mode.

The initialisation mode is activated when the device has not yet been initialised. During initialization via the dedicated mobile application, the relevant configuration parameters of the fire monitoring system are stored, including:

- the unique access device identifier,
- the PIN number of the SIM card used in the device,
- the APN access point identifier,
- the private key for the digital signature,
- the public key for verifying the digital signature.

In initialisation mode, the access device uses the Bluetooth 5.0 physical layer to establish a connection with a dedicated mobile application. Once initialisation is complete, the access device automatically enters normal operation mode. In this mode, the device performs passive scanning of data packets broadcasted by IIoT devices. The scanning consists of cyclic listening to successive advertising channels.

4. Experimental studies

Experimental studies were carried out at the Fire Research Laboratory at the Ship Technology Centre in Gdańsk, Poland. Their aim was both to verify the functionality of the prototype wireless data acquisition system, the idea of which is outlined in this paper, and to conduct real-world fire resistance tests. In particular, the following tests were carried out:

(i) correctness of logging experimental data,
(ii) correctness of detection of fire hazard,
(iii) reliability of fire alarm notifications,
(iv) correctness of communication with the cloud,
(v) charge loss degree of electrochemical cell,
(vi) life time of IIoT devices under fire conditions,
(vii) fire resistance tests for both single- and double-leaf wooden doors.

4.1. Fire resistance test for single-leaf doors

To implement the test plan, four IIoT devices were installed in the door frames of two pairs of single-leaf solid wooden fire doors. The first two IIoT devices (numbered #1 and #2) were mounted on the fire-affected side of the door and the other two (numbered #3 and #4) on the exterior side. The devices were mounted in the top beam of the door frame in such a way that the faces of the IIoT devices were covered when the door was closed.

A snap shot of the door prepared for testing is shown in Fig. 3. The location of the two IIoT devices in the door frames outside the fire-affected side is indicated in by the yellow circles marked 1. The location of the IIoT devices on the side affected by fire is similar. Number 2 indicates K-type thermocouples (chromel–alumel) for measuring the temperature distribution on the door surface. The total number of used thermocouples in this experiment was 26. The thermocouples are attached to the stationary temperature measuring system marked with number 3. The duration of the experiment is measured using a timer (marked with number 4). However, it is worth noting that the measurement and data acquisition system referred to in this paper does not apply to temperature measurements made using thermocouples.

The achieved results of the tests are shown in Table I.

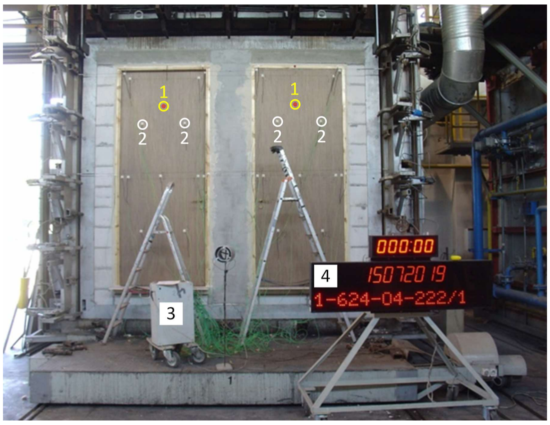

Fig. 3. View of single-leaf solid fire doors prepared for fire resistance testing.

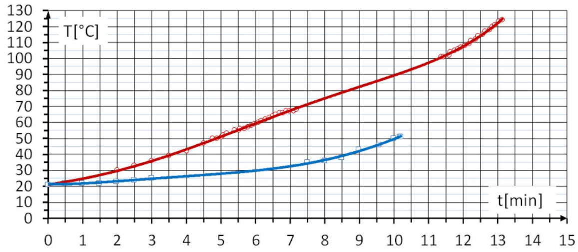

Fig. 4. Temperature rise recorded in the cloud during the fire resistance test of single-leaf doors. The red line indicates the temperature recorded on the fire side and the blue line the temperature on the opposite side of the door.

TABLE I

Test results for single-leaf solid doors.

Parameter	Unit	#1	#2	#3	#4
fire detection time	min	5	5	–	–
max. registered temp.	°C	124	100	61	51
IIoT device lifetime	min	13.1	11.3	5.3	10.2

The overall evaluation of the test results is positive. The door met the 30-minute fire resistance test requirements. The fire detection time occurred 5 min after the start of the fire test. This is considered a valid fire response time. The IIoT devices, depending on the location, were destroyed at different time instants. The critical factor for the destruction of an IIoT device is a temperature rise above 100°C. The temperature of the device which is fixed on the opposite side of the fire (blue line in Fig. 4) indicates good thermal insulation of the door. When the temperature rises above 50°C, both IIoT devices installed on the side of the fire identified the state of a fire. One device generated a fire warning after 5 minutes, while the other generated a fire warning after 10 min. The temperature rise during the fire tests is shown in Fig. 4. The condition for completing the fire test is shown in Fig. 5.

4.2. Fire resistance test for double-leaf glazed doors

The aim of this study was to experimentally determine the functionality and durability of the IIoT device under standardised fire test conditions. The test involved double-glazed doors, for which a 30-min fire resistance was expected. For this purpose, two IIoT devices numbered #5 and #6 were installed in the pine frames of two pairs of double-glazed wooden fire doors. Device number #5 was installed on the side subjected to direct fire, and device number #6 was installed on the opposite side. Both devices were mounted in the upper door frame in such a way that their faces were covered and sealed by the door seal when the door was closed.

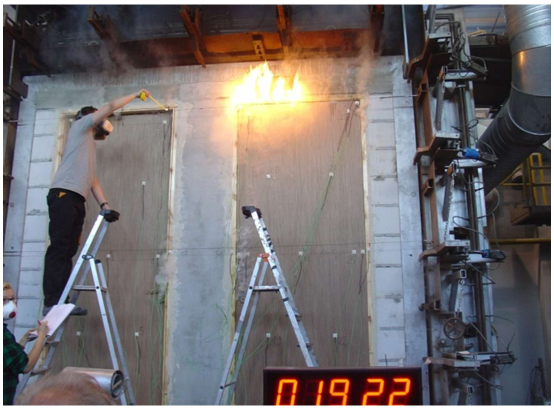

Fig. 5. The moment the fire resistance test is stopped.

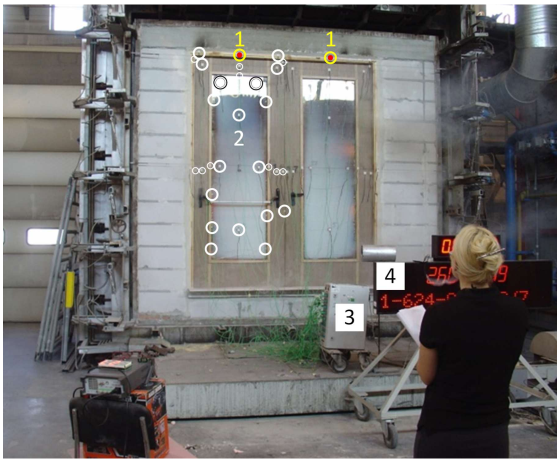

Fig. 6. View of the double-glazed fire door installed in the furnace during the 30-minute fire resistance test. The fire-induced tarnishing of the glazing is already visible. The distribution of thermocouples in one wing only is shown for better visibility. The designations are the same as in the description of Fig. 3.

For research purposes, 27 K-type thermocouples were installed on the surface of each door leaf. The analysis of the obtained spatiotemporal temperature distribution allows for the experimental identification of unknown parameters of simulation models of thermal energy transmission. However, it should be noted that a simulation model of this process is not the subject of this publication. A snap shot of the door prepared for fire test is shown in Fig. 6. The results of the test are shown in Table II.

The evaluation of the test results is positive. The door met the 30-min fire resistance test requirements. The fire test was carried out according to the appropriate test procedure until the 31st minute was completed. The maximum temperature in the furnace reached 500°C in the 5th minute and 960°C in the 10th minute of the test.

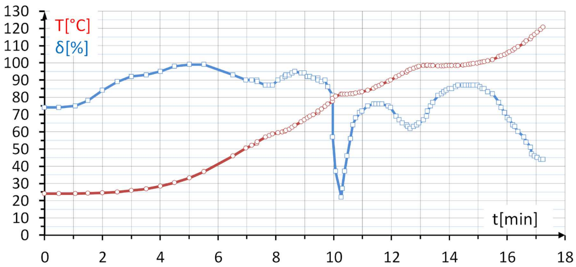

Fig. 7. Temperature (red line) and humidity (blue line) recorded in cloud on the side of the fire exposure.

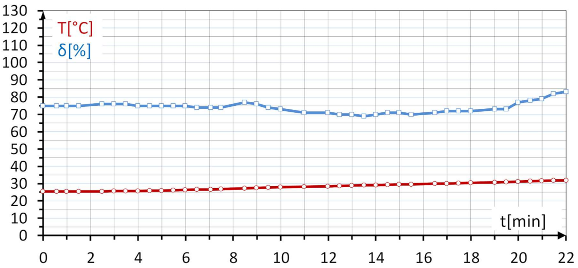

Fig. 8. Temperature (red line) and humidity (blue line) recorded in cloud on the opposite side of the fire.

TABLE II

Test results for double-leaf glass doors.

Parameter	Unit	#5	#6
fire detection time	min	7	–
maximum temperature	°C	121	32
max. relative humidity	%	100	89
min. relative humidity	%	22	69
IIoT device lifetime	min	17.3	22.0

The fire alarm was reported by the IIoT device approximately 7 min after the start of the experiment. This is still an acceptable, albeit maximum, fire response time. The dynamics of the temperature and humidity changes recorded by the IIoT devices mounted on the fire side and exterior are shown in Figs. 7 and 8, respectively.

Case 1: Temperature and humidity measured on the fire exposure side

The recorded temperature measured by the IIoT number #5 on the fire side (Fig. 7) gradually increased until the IIoT was physically destroyed. The damage occurred in the 17th minute of the experiment. The IIoT device correctly generated a fire alarm message in the 7th minute of the experiment. Much more interesting are changes in the relative humidity (Fig. 7). In the first phase of the study, up to about the 5th minute, the humidity increases up to 100% despite the expected decrease. This surprising effect can be explained in such a way that water stored in the wall into which the door frame is embedded has started to be released as a result of the fire action. At this point, it should be noted that the door frame was put in just only few days before the experiment was carried out. Next, around 10th minute, the humidity dropped sharply for a while.

The interpretation of this decrease might be as follows. IIoT devices are installed in door frames in such a way that, under normal operating conditions, they have access to the atmosphere surrounding the door through gaps between the door frame and the edges of the door. In fire doors, expanding seals are fitted to prevent the ingress of smoke, gases, and open flames when the temperature of the atmosphere exceeds a certain limit value. The seal, which expands as the temperature increases, cuts off the possibility of direct ambient air access to the IIoT device for a period of time. In the small enclosed volume of the IIoT device, there is then a drop in relative humidity caused by the rise in temperature and isolation from the moisture transfer released from the walls and doors. However, the effect of the rapid drop in relative humidity shown in Fig. 7 is mainly due to another cause related to the conditions of the experiment. It is due to the effect of the sudden opening of the furnace vents by the automatic temperature control system. Around the 10th minute of the experiment, the temperature in the furnace reached the permissible limit. Further relative humidity fluctuations are also caused by the temperature control system. A similar effect of a sudden drop in relative humidity, similar to that in Fig. 6, is also observed in industrial wood dryers.

This observation leads to the conclusion, that the information value of a relative humidity measurement is marginal with regard to the detection of a fire risk. Hence, we will not refer to this physical quantity in the remainder of this paper.

It should be noted that expansion seals quickly lose their insulating properties when they themselves are exposed to direct fire.

This case shows the specificity and randomness of the physical phenomena occurring in laboratory fire tests. It also indicates how many factors have to be taken into account when modelling the combustion and heat transfer processes.

Case 2: Temperature and humidity measured on the side opposite to the side exposed to fire

The temperature measured at the fixing point of the IIoT device on the side opposite the fire side (Fig. 8) gradually increased from 25.5 to 32°C in the 22nd minute. Such a slow rise in temperature demonstrates the very good insulation performance of the door. As the temperature did not exceed 50°C, the device did not set a fire alarm. Since, in reality, a fire can occur on either side of the door, it follows that IIoT devices should always be installed on both sides of the door.

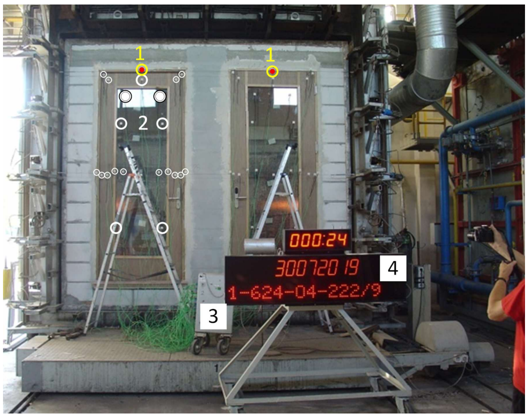

Fig. 9. View of the single-leaf glazed fire door installed in the furnace during the 60-min fire resistance test. The distribution of thermocouples in one wing only is shown for better visibility. The designations are the same as in the description of Fig. 3.

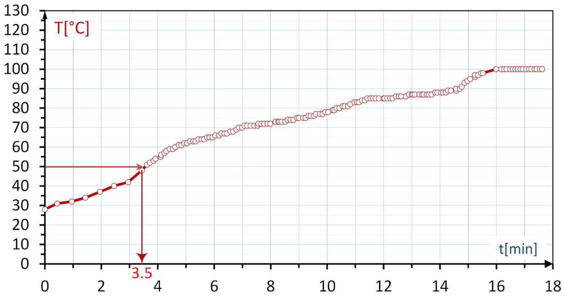

Fig. 10. Changes in temperature recorded by IIoT #7 during the fire resistance test (fire side).

The relative humidity recorded showed little change and reflected the relative humidity of the air in the laboratory. The relative humidity showed almost no sensitivity to fire, unlike on the fire side.

4.3. Fire resistance test for single-leaf glazed doors

This study aimed to experimentally determine the functionality of the cloud-based monitoring and data acquisition system as well as the durability of the IIoT devices when performed under fire test conditions. Single-leaf glazed doors, for which a 60-min fire resistance was expected, were tested.

For this purpose, four IIoT devices were installed in the oak frames of two pairs of single-leaf glazed wooden fire doors. The devices numbered #7 and #8 were placed on the fire side in the upper beam of the door frame. The devices numbered #9 and #10 were mounted in the upper jamb outside the fire side. All devices were mounted so that their fronts were covered by the top edge of the door and sealed with the door seal.

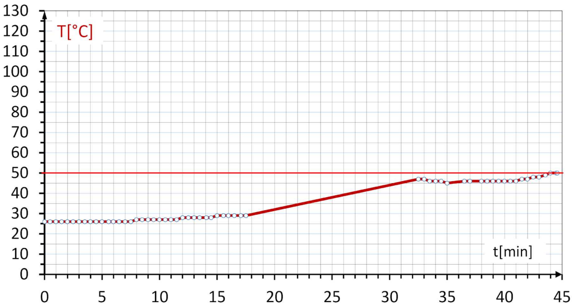

Fig. 11. Changes in temperature recorded by the IIoT #9 during the fire resistance test (fire-free side).

TABLE III

Test results for single-leaf solid door.

Parameter	Unit	#7	#8	#9	#10
fire detection time	min	3.5	5	–	–
max. registered temp.	°C	100	103	36	50
Maximum humidity	%	90	54	87	69
IIoT device lifetime	min	17.6	17.9	7.0	44.6

In addition, 21 K-type thermocouples were installed on the surface of each door leaf with the research goal identical with that stated in Sect. 4.2. A snap shot of the door at the 24th second of the fire test is shown in Fig. 9.

The results of the test are given in Table III.

The result of the fire resistance test according to EI 60 requirements is negative. The test was interrupted in the 45th minute due to an open fire outside the door. However, by the time the test was interrupted, the IIoT devices mounted in the upper jamb outside the fire side had not been damaged.

Examples of changes in temperature recorded on the exposed and unexposed side of the fire are presented in Figs. 10 and 11, respectively.

The fire detection alarm was set just before 4th minute after the start of the experiment, which can be seen in Fig. 10. The temperature measured at the location of the IIoT device mounted on the fire side gradually increased from the ambient temperature up to a value slightly exceeding 100°C, i.e., until the IIoT device was destroyed. The destruction of the IIoT device occurred in the 17th minute of the test, which is similar to the result of EI 30-min fire resistance test reported in Sect. 4.2.

In the final phase of the test, the temperature outside doors rose almost to 50°C (Fig. 11). Therefore, the IIoT devices mounted in this side of doors have not yet generated a fire alerts.

However, during the tests, occasional interruptions in data transmission were found, as can be seen in Fig. 11. These may have been the result of excessive attenuation of the radio signal resulting from the considerable distance of the IIoT devices from the access device.

5. Conclusions

The selected results of experimental tests on the fire resistance of wooden fire doors were presented in this paper. The results presented were obtained with the usage of a unique fire monitoring and data acquisition system based on IIoT smart devices.

The system has been primarily designed for use in wooden-framed fire doors. However, the system's architecture is so versatile that it can also be used for other commercial tasks, such as for example greenhouse gardening.

The system can be useful for scientific research aimed at the experimental identification of parameters and verification of physical phenomenological models of thermal energy transfer processes. In this respect, a preliminary analysis of the results of the experiments carried out indicates, among other things, the desirability of extending the models of flammability processes to include the effect of water migration and the influence of its phase transformations on their dynamics.

The functionality of the system and its suitability for fire risk monitoring was demonstrated. The experimental tests also showed that, contrary to popular belief, wood can be a material used in the construction of fire doors.

Further development is directed towards the design of IIoT devices that, using miniature integrated low-resolution thermal imaging cameras, can be used for early recognition of fire situations, as well as signalling the presence of people and living organisms in fire danger zones.

References

[1] T. Domański, W. Piekarska, M. Sága, M. Kubiak, Z. Sáternus, Z. Sagová, *Acta Phys. Pol. A* **144**, 300 (2023).

[2] R. Prieler, B. Ortner, T. Pfeifer, P. Kitzmüller, S. Thumser, G. Schwabegger, H. Hochenauer, *Fire Saf. J.* **141**, 103922 (2023).

[3] R.E. Lyon, N. Safronava, J.G. Quintiere, S.I. Stoliarov, R.N. Walters, S. Crowley, *Fire Mater.* **38**, 264 (2014).

[4] I. Ĉabalová, M. Zachar, B. Toman, in: *Fire Protection, Safety and Security*, 2017, p. 22.

[5] M. Tomaskova, J. Pokorny, P. Kucera, M. Balazikova, D. Marasova Jr., *Appl. Sci.* **12**, 2505 (2022).

[6] J. Singh, A. Gimekar, S. Venkatesan, *Int. J. Commun. Syst.* **36**, e4189 (2023).

[7] M. Ghobakhloo, *J. Clean. Prod.* **252**, 119869 (2020).

[8] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, D.O. Wu, *IEEE Commun. Surv. Tutor.* **22**, 2462 (2020).

[9] A. Sari, A. Lekidis, I. Butun, in: *Challenges, Design Principles, Applications, and Security*, 2020 p. 3.

[10] Z. Zonglin, W. Hu, *Comput. Commun.* **153**, 390 (2020).

[11] Q. Zhou, X. Chen, J. Wang, Y. Li, H. Li, T.Q.S. Quek, *IEEE Internet Things J.* **10**, 10893 (2023).

[12] J. Cui, F. Wang, Q. Zhang, C. Gu, H. Zhong, *IEEE Trans. Netw. Serv. Manag.* **20**, 357 (2022).

[13] D. Johnson, A. Menezes, S. Vanstone, *Int. J. Inf. Secur.* **1**, 36 (2001).