Tomas Bata University in Zlín
Faculty of Applied Informatics

Doctoral thesis

Modernization of alarm detector
used for the protection of glass panels

Modernizace poplachového detektoru
určeného pro ochranu skleněných ploch

Author:	**Ing. Václav Mach**
Study program:	Engineering Informatics (P3902)
Study field:	Engineering Informatics (3902V023)
Supervisor:	doc. Mgr. Milan Adámek, Ph.D.

Zlin, April 2021

Keywords: *Alarm Detector, Intrusion and Hold-up Systems, Glass-break Detector, Window.*

Klíčová slova: *Poplachový detector, Poplachový Zabezpečovací a Tísňový Systém, Glass-break Detektor, Okno.*

The full version of the dissertation thesis is available in the Library of Tomas Bata University in Zlin

Acknowledgment

Abstract

The goal of this dissertation thesis is to design and manufacture a combined alarm detector, used for the protection of the glass planes. The main active elements of the detector are the accelerometer for the force calculation of the impact, and the air quality sensor used for the detection of the glass integrity. The concept of the detector meets the current standardization which also reaches the highest security grade. The prototype of the detector is divided into two parts each implemented into the window frame. The outcome of this thesis is the prototype with the technical documentation which can be used for the certified testing and the following placing on the market. The detector has a common communication interface for communication with the Control and Indicating Equipment via the RS-485.

Abstrakt

Cílem disertační práce je navrhnout a vytvořit kombinovaný poplachový detektor určený pro ochranu skleněných ploch. Aktivními prvky daného detektoru jsou akcelerometr pro vyhodnocování působící síly na sklo a sensor kvality vzduchu pro indikaci změny celistvosti skla. Navržený detektor splňuje platnou standardizaci pro poplachové Glass-break detektory, která vyhovuje nejvyššímu stupni zabezpečení. Model poplachového detektoru je rozdělen na dvě části, které jsou umístěny přímo v okenním rámu. Výsledek disertační práce je funkční prototyp společně s technickou dokumentací, které mohou být použity jako podklad pro certifikaci a následné uvedení daného produktu na trh. Detektor je vybaven standartním rozhraním pro spolehlivou komunikaci s běžnými poplachovými ústřednami pomocí sběrnice RS-485.

Table of Content

1. Introduction

The Intruder Alarm System (IAS) became very popular in modern households, and companies, where people want to protect their lives, health, and possession effectively. This system can be classified as technical security which replaces the less efficient physical security. Physical security is very often used in large buildings or areas where the person can control several systems at once. However, this manner is very inefficient and expensive in small facilities. The author [1] mentioned that a person stares at a screen for more than 20 minutes, his attention drops by 30%, and for periods over an hour, this drop can reach up to 70%. That is why the IAS is much more suitable and also more cost-effective for the small facilities. The standard IAS consists of several devices that can detect the intruder in the protected area without any person involved. [2]

The main component of the system is called the Control and Indicating Equipment (CIE) which controls the whole security system, and it also controls all connected devices called alarm detectors. [3] It also provides external communication with the Alarm Receiving Center (ARC) which can dispatch security forces immediately when the alarm is triggered. [4] The modern systems are usually extended by the non-alarm applications which are controlled by the CIE. The author in [5] claimed that the IAS which is extended by the other application is called the Integrated Alarm System.

The most critical layer between the intruder and the protected possession is the casing done by the walls, windows, and doors. [6] The walls themselves are unbeatable by the normal force, and the intruder has only two ways to get into the protected house or area. These options are the doors and the windows. Nowadays, the doors are the most secure part of the entrance to the house. On the other hand, the most vulnerable opening is the window.

The goal of this research is to improve the technical protection of the windows against potential intruders by using the glass-break detector embedded into the window. The final detector should be able to evaluate vibration which can be created by the intruder during the breaking through. According to the author [7], every glass-break detector must be designed according to the standardization called the CSN EN 50131-2-7-2 Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive).

Every alarm system also must have assigned a Security Grade which specifies the equipment of the expected intruder. The final grade for the whole system depends on the element which has the lowest grade. [8] This responsibility is given by the CSN EN 50131-1 ed. 2 Alarm systems - Intrusion and hold-up alarm systems Part 1: System requirements. [9]

The Security Grade must be expressed as a number from I. to IV. where the lowest level is the I. and the highest level is the IV. Common rules for the application of IAS allow to optimize the security for specific risks or to evaluate the level of the specific security. It can be used also as the establishment of security requirements for the building or area. The explanation of each level is the following:

- Level I: Low risk: It is assumed that the intruder or burglar has little knowledge of the system and has a limited range of available tools.
- Level II: Low to Medium Risk: It is assumed that the intruder or burglar has limited knowledge of the system and the use of common tools and portable devices.
- Level III: Medium to High Risk: It is assumed that the intruder or burglar is familiar with the system and has an extensive range of tools and portable electronic devices.
- Level IV: High Risk: Used when security has priority over all other aspects. It is assumed that the intruder or burglar is capable or able to prepare a detailed intrusion plan and have a complete range of equipment, which can replace the critical components of the system. [9]

Every detector available on the market also needs to have assigned the Environmental Class where the devices can operate normally in given conditions. It is necessary to determine the environment in which the detector or other equipment of technical security is located. Environmental Classes can be divided into four levels and the detailed description are following:

- Level I: Indoor: Usually indoor spaces with a constant temperature (in residential or commercial buildings), (+ 5 °C to + 40°C).
- Level II: Indoor general: Mostly indoor spaces without constant temperature (in corridors, halls, or staircases and where condensation can occur on windows and in unheated warehouses, or warehouses where heating is not permanent), (-10 °C to + 40°C).
- Level III: Outdoor protected: Mostly outside buildings, where devices are not fully exposed to the weather, (-25 °C to + 50°C).
- Level IV: Outdoor general: Usually outside buildings, with devices fully exposed to the weather, (-25 °C to + 60°C). [9]

As mentioned before, the IAS should protect the life, health, and possession of the owner. The main and the most critical layer between the potential intruder and the possession of the owner is the casing of the building. This layer is created by three main parts. The first is the wall which is the main component of the typical casing of the building, and it is made almost of bricks and concrete. It means that the wall is destructible only with a lot of force and noise. The second part of the casing of the building is the front door. Nowadays, the front door is the most secured part of the

whole technical protection, and the front door is not used to breaking into the building by the intruder. The last part of the typical casing layer is the glass panels, which are very easy to breakthrough. Despite this fact, the protection of the glass panels is done only by the one type of detector called the glass-break detector. The company iMateriály provides the study of the breaking into the buildings via the casing layer. [10] This study proved that the glass panels are the most commonly used part to break into the building. All parts used by the intruders are the following:

- breaking through glass panel 80% (52% balcony door; 28% windows)
- breaking through cellar 7%
- breaking through the front door 13%

It means that most of the intrusion into the building is done by breaking through the glass panels. The same company iMaterály also provides all types of breaking into the object via the casing layer. This information helps with the identification of the most vulnerable part of the glass panels of the building.
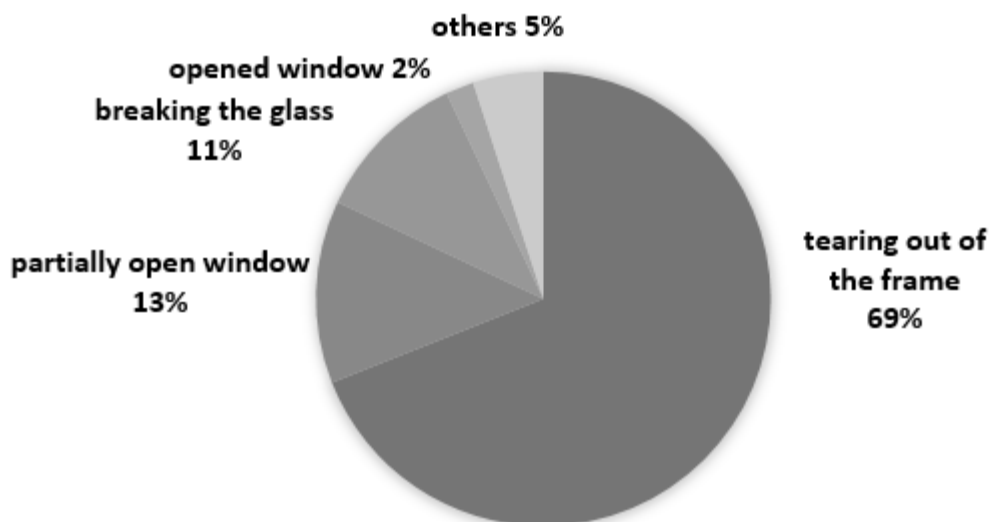
Fig. 1 Types of the breaking via the window of the building [10]

It is more than clear that intruders are using glass panels in most cases. The study also showed that the glass panels can be divided into glass doors and the normal windows where the glass-break detector can be used for both types. All glass-break detectors are very sensitive to false alarms, and it is the biggest problem of the glass-break detectors. The main goal of this research is to design a new concept of the detector which can reduce the number of false alarms.

The previous figure also showed that the breaking of the glass is not the main type of intrusion. The biggest and for the glass-break detector mostly undetectable is tearing out the frame of the window. According to this research, the new prototype should be able to detect even the tearing out of the frame by the intruder.

1.1 Alarm Detectors

There are many alarm detectors on the market that can be divided according to their application into many categories. Each category has a different usage in the alarm systems, and each detector must be connected to the CIE. There are several ways how the detector can be connected to the CIE. These ways are a wireless connection, a wired connection, an analog connection, and a digital connection.

In general, every detector must be connected to the CIE which periodically evaluates the incoming signal from all connected devices. Detectors can be connected in several ways depending on the situation and the environment. This connection can be divided into analog, and digital. According to [7], the analog connection has the maximum amount of connected devices based on the used mode. These modes are Normal Closed (NC), End of Line (EOL), and Advanced Technology Zone (ATZ). When the detector is activated, the resistance of the loop is changed, and the CIE can evaluate this event. However, this concept is outdated, and the digital connection is widely used in the alarm application. The digital connection uses one common bus for all connected detectors and it uses the address system. Every detector has a unique address and direct access to the system. Digital communication can be further divided into metallic and wireless. However, the wireless connection has several disadvantages, and it cannot be used in a high-risk situation of intrusion. Detectors using wireless connection must have their power source, and the communication can be disturbed or misused by the potential intruder.

The detectors have several states which must be evaluated by the CIE. These states are Idle, Alarm, Sabotage, and Failure. According to the author [5], the sub-category of Sabotage and Alarm is the anti-masking function which is the ability to detect the intruder who attempted to defeat the detector by blocking it with a material that blocks its main function, such as paper, tape, film, or spray. When the detector is triggered, it automatically sent the Alarm and Sabotage message to the CIE.

As mentioned before, detectors can be divided into several groups according to their application. The most common aspect is the environment, where detectors can be placed. Detectors can also be divided into the outdoor and indoor according to the environment. This group provides the temperature limit given by the Environmental Class for each category. The other partition can be focused on the type of used sensor. There are detectors which have sensor focused on the light (Passive Infra-Red), sound (Microwave) contact (Magnetic contact) or vibration (Glass-break). Each category is suitable for different purposes and locations. [11] The following chapters are focused on the glass-break detectors which are the main subject of this thesis.

2. State of the Art of Glass-break Detectors

The majority of the market is covered only by acoustic detectors. The main reason for this phenomenon is the fact that it can be mounted everywhere in the room and it can cover several glass panels at once.

Publications

The authors [12], [13], and [14], stated that the present state of development of security systems is at a point of stagnation. It means that the manufacturers are copying the old and outdated model of glass-break detectors without any innovative approaches and user feedback, this attitude will lead to a blind alley.

The author [15] improved the acoustic type of the glass-break detector to distinguish the onset of glass breaking from speech, music, and noise in a 20 ms loop. This demonstration proved that glass-break could be integrated into a microphone and function as an excellent processing-triggering smart threshold for existing DSP-based glass break detectors.

Another author [16] tested the glass-break detectors under extreme conditions like using special foil to reduce the impact to the glass or using different types of tools to breakthrough. This paper proved that all tested devices are not reliable under presented conditions; However, like in the previous papers, the author points to the stagnation.

The last interesting publication [17] is focused on the investigation of the Wavelet Packet Decomposition (WPD) method of glass-break acoustic signal detection in comparison with the conventional method. The method improves also the resistance to false signals, which is important from the point of view of the standard of requirements. For example, the WPD method with the application of a 32 element-time signature improves the resistance to false signals by 10-15%.

Low-Security Grade level

The next problem is the fact that not a single glass-break detector currently on the market does not meet the requirements for Security Grade number IV. This is caused by the requirements for the Security Grade IV which are very strict. The mentioned standardization CSN EN 50131-2-7-2 requires alarm triggering by changing the integrity of the glass panel. This change is not based on the impact force. However, the change can be done by the fire torch, glass cutter, or etching of the glass. This event is impossible to detect by the detectors which are based on the vibrations or based on the sound. It means that the glass-break detector meeting the requirements of Security Grade IV. must be able to detect mentioned glass integrity.

Window protection

The glass-break detectors are mainly designed for detecting breaking through the protected window by breaking the glass panel. However, previous ***Fig. 1 Types of the breaking via the window of the building [10] (pp. 9)*** shows that almost 70 % of intrusion are aimed at tearing out the window frame without breaking the glass panel inside of the window. This requirement is not mentioned in the standardization CSN EN 50131-2-7-2. However, this type of intrusion should be also implemented into the new model.

From the research and current situation on the market, it is more than clear that glass-break detectors need to be rapidly improved. The biggest disadvantage of these detectors is the high number of false alarms. The companies who designing and installing the alarm system usually avoiding the glass-break detectors at all due to the huge amount of false alarms and low reliability. As mentioned before, the main layer between the potential intruder and protected possession is the casing of the building which is formed by the glass-panels without any active protection. This thesis is focused on the innovation and improvement of the contact glass-break detectors.

3. Goals of the Dissertation

This chapter shows the main goals of this thesis that should be fulfilled. These goals are forming a logical sequence for designing and verifying the new model of the glass-break detector. The main goal of this thesis is to design and manufacture the new concept of the contact glass-break detector, which is ready for certified testing according to the standardization CSN EN 50131-2-7-2.

1. Research in the state of the art of glass-break detectors.

The first part of the thesis should summarize the present situation and design of glass-break detectors available on the market. Each category should be described in detail with physical properties. One part of this goal is to find the causes of the false alarms which are very common. The problem causing the false alarm must be strictly defined and also it must be solved by a reasonable and reliable solution.

2. Designing and the fabrication of the glass-break detector

The second part should be focused on the fabrication of the designed detector. This part should consist of all schematics documentation of all used components and the real design of the fabricated detector. The main program should cover all possible scenarios which are mentioned in the standardization CSN CLC/TS 50131-2-7-2, and the program should be able to communicate with the common CIEs via the serial interface.

3. Verification of the functionality by testing and measuring according to the standardization.

The designed glass-break detectors should be tested according to the standard CSN CLC/TS 50131-2-7-2 in the created testing room. These experiments should prove, that the designed prototype achieved all needed obligations according to the standardization and that the prototype is ready for certified testing. All testing and experiments should be recorded and explained in detail for repeatability.

4. Create the technical documentation for the final prototype.

The final prototype must have the technical documentation which can be used for further certified testing in the laboratory, and it also can be used as a guide for the upcoming application for the patent. The documentation should consist of all expected information and illustration as common alarm detectors currently at the market.

4. Glass-break Detectors

The glass-break detector is used to detect breaking through the protected glass panel. It can be constructed in two different forms. The first one is based on vibration and the second on sound. The vibration-based glass-break detector usually has a shock sensor that can detect the vibration. This part can act as a switch during the vibration. According to the author [12], the vibration-based glass-break detectors employed aluminum foil conductors mounted on the inner surface of glass enclosures and triggers the alarm when the physical event broke the conducting path. In this case, the detector must be mounted right on the glass to obtain sufficient transmission of the vibration.

The second manner uses the sound created by the impact on the glass panel. The standard microphone is used to capture the sound. The authors [13] and [14] also stated that the breaking sound of the glass is in the higher frequencies above 14 kHz. However, these frequencies above 14 kHz can be also produced by many other devices in the house. According to this problem, two-phased detection was developed. The destruction itself produces the first sound wave of breaking glass, and after that, another sound is created by the glass hitting the floor. This combination improved the reliability of glass-break detectors, and the following chapters describe mentioned manners in detail.

4.1 Acoustic Glass-break Detectors

The acoustic glass-break detector is a contactless device that can be mounted anywhere in the protected room or area. It searching for frequencies that are characteristic for the breaking glass of any dimensions and materials. It uses the piezo-electrical microphone to register sound signals and pressure waves typical for breaking the glass. Advanced types also use the time domain to reduce false alarms by the two-phase detection. In the first one, the glass is break in the frame of the window and after several seconds the shards fall on the ground making another sound effect. [15] [18]

The biggest advantage of these glass-break detectors is the range that can be covered. In this case, the detector must have direct visual contact to all protected glass panels and the place between the detector and the glass panel must be empty. The disadvantage of this type is a huge amount of false alarms which can be caused by negative influences like loud sounds, glass containers, technical equipment, or animals. The acoustic detector will not trigger the alarm when the protective foil is installed on the glass panel. [19] [20]

Acoustic detectors are designed for indoor use only and they can be used for several types of glass panels. The typical input voltage for the detectors is 12 V DC and it contains the potentiometer which can be used for the gentle adjustment of the

sensitivity of the alarm triggering. When the alarm is triggered the detector actives the output relay for 2 seconds and the time for analyzing the incoming signal is maximal 4 seconds. Some of the glass-break detectors have a dual function. It can be used in scenarios where security is the most important aspect of the application. The detector can separate the glass-break and the PIR function and these functions can be used independently. On the other hand, the combination can be used to reduce the number of false alarms.

4.2 Contact Glass-break Detectors

The passive contact glass-break detector is firmly placed on the window where it is detecting the energy produced by the impact on the glass panel. These detectors can be divided into passive and active.

The passive contact glass-break detectors have the piezoelectric sensor tuned to resonance frequency from 40 kHz up to 120 kHz. The sensor ignores the environmental noises in the protected area. The detector must be installed physically on the window which means that it is always visible to the residents. However, it is also visible for the potential intruder and it can act as prevention. The disadvantage is the fact that the detector must be connected by a metallic cable and every glass panel must have its detector. The passive contact glass-break detector can detect intrusion even with the alarm foil installed on the glass panel. [21] [22] The detector can recognize the environmental influences due to the advanced properties of the piezoelectric sensor.

The active contact glass-break detector consists of the transmitting and receiving parts that are placed on the glass panel and periodically checking the signal. The signal can be based on a physical medium like wire or it can be based on the optical beam. The alarm is triggered when the medium is distorted. This type of glass-break detector is used only in the most secured buildings because it is the most reliable type of detector. It is not used in residential areas due to its cost and difficult mounting. [23]

The last type of contact glass-break detector is called the alarm foil which is very rare due to the difficult mounting and high price. These detectors are not normally available for residential systems. The detector is based on the breaking of a conductive medium, which is a conductive wire or a specially vaporized meandering conductive path located on a protected surface.

4.1 Sources of False Alarms

A false alarm is an event when the alarm is triggered by the detector but there is no context with the real threat. The false alarm is very often caused by the wrong installation in the area by the technical ignorance of the alarm designer. The most common mistake is the ignorance of the installation manual, and it can be also caused by the user. However, all these variants should not cause a false alarm when the installation instructions are fulfilled. The biggest disadvantages of the glass-break detector are the huge amount the false alarms usually caused by two sources. The first one is the influence of the weather like strong rain, hail storms, or thunderstorm. The second is the influence created by the traffic like passing car, truck, train or tram.

The main assumption for flawless and reliable detection is the choice of the device which usually uses the two-phase detection mentioned before. A great example is the combination of the contact glass-break detector with the PIR detector. This type of detectors can trigger the alarm only when both parts of the detector triggers the alarm at the same time. However, in this case, the influence outside of the protected area can be caused by the weather and the traffic which is almost impossible to cover. It means that there is not any possible way how to use two-phase detection for outside influences like weather or traffic. The resistance of the mentioned false alarms can be solved only by the better and more advanced software solution.

The last part of the false alarm is the acoustic waves which can transmit a pressure wave from the source to the glass panel and it can cause the false alarm. These waves can be generated inside or outside of the protected area. The outside influence is done usually by the thunderstorm, passing or horning train, passing truck and by the trashcan for the glass. On the other hand, there are also many sources of sound inside of the house like a barking dog, loud door ring, or music.

In general, there are a lot of influences that can cause false alarms and the main goal of this thesis is to develop a new model to reduce the huge amount of false alarms.

5. Accelerometers

Accelerometers are used to measure static gravitational acceleration, which makes it possible to determine the angle of deflection of the measured object, and also to measure the dynamic acceleration due to shock, motion, or vibration with low amplitude and low frequency, which reaches several tens of Hz. [24]. The accelerometer measures the acceleration force in g and it can measure in one, two, or three directions. Currently, the most commonly used are tri-axial accelerometers, which consist of a system of three accelerometers, each measuring the acceleration in a different direction - in the X, Y, and Z directions. There are the basic types of accelerometers: capacitive accelerometers Micro Electro Mechanical System (MEMS), and piezo-resistive accelerometers. [25]

5.1 Capacitive Accelerometers

Capacitive accelerometers using MEMS technology are the cheapest, most common, and smallest sensors of this type. The principle of its function is to place the weight mounted on the springs. One end of the springs is attached to the plates of the comb capacitor and the other end to the installed weight. Under the influence of the force acting on the sensor, the weight moves on the springs, which causes a change in the distance between the condensing element and the mass, and thus affects the change in capacity. [26]

Capacitive accelerometers made with MEMS technology are mainly used in wearables, mobile devices, and widely understood consumer electronics. One of the biggest advantages of MEMS accelerometers is the possibility of their implementation directly on the printed circuit board. The shortcomings of MEMS circuits include low measurement accuracy, especially in the case of measuring higher amplitudes and frequencies, and as a result, are not suitable for special industrial applications.

5.2 Piezo-sensitive Accelerometers

Another type of accelerometer is a sensor using the piezo-resistive effect. The principle of its function resembles the function of a strain gauge or sensor of measuring stress. Accelerometers of this type are equipped with a piezo-resistive material that deforms under the action of an external force by changing the resistance. The change in resistance is then converted into an electrical signal taken by a receiver integrated with the accelerometer. Piezo-resistive accelerometers are characterized by a large measuring band, thanks to which they can register vibrations with high amplitudes and frequencies, which is useful, among other things, in various impact tests. [27]

Another advantage of piezo-resistive accelerometers is the ability to measure slowly changing signals, which allows their use in inertial navigation systems to calculate the speed and change the position of circuit elements.

5.3 Accelerometer MPU-6050

The accelerometer MPU-6050 is a very sensitive sensor that can be used for differing output even with the slightest change in orientation or placement in the space. The accelerometer MPU-6050 was chosen for this research due to its low cost, easy-to-mount, and digital connection with less power consumption, taking up to 5V. The chip has a 6-axis device that combines a 3-axis gyroscope, 3-axis accelerometer, and a Digital Motion Processor (DMP) which process the data inside and helps lower system power consumption by allowing the system processor to read the sensor data in bursts and then enter a low-power mode as the MPU collects more data. The output of the accelerometer has 6-bit Analog to Digital Converters (ADC) for digitizing the gyroscope and accelerometer outputs. [28] It also has pinheads which are necessary for the connection with the Arduino UNO. Communication with all registers of the device is performed using either TWI at 400 kHz. [29]

The MPU-6050 features three 16-bit ADCs for digitizing the accelerometer outputs. For precision tracking of both fast and slow motions, the program features a user-interface for programming of the accelerometer full-scale range of ±2g, ±4g, ±8g, and ±16g. Typically, the lowest the range, the more sensitive the readings will be from the accelerometer. For example, measuring small vibrations using a small-range accelerometer will provide more detailed data than using a 16g range. [30]

For this research, the smallest possible range is applied. The DPM periodically evaluates the actual state of the accelerometer, and it can send this data to the main microcontroller. These data are already converted to a suitable format of the decimal number which is suitable for further evaluation. Accelerometers can measure acceleration on one, two, or three axes. The DMP produces current acceleration in a given direction.
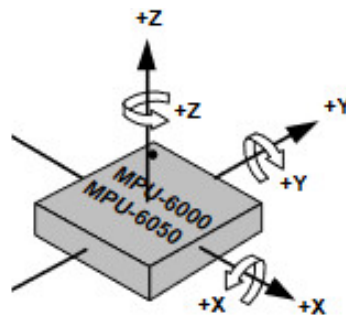

Fig. 2 Representation of the acceleration and rotation of the MPU-6050 [31]

6. Air Quality Sensors

The air quality sensors are used for monitoring the air pollution in the surrounded room or specific area. There are many various types of these devices specialized for different applications and most of them are used for measuring the concentration of gases like ozone, carbon monoxide, sulfur dioxide, carbon dioxide (CO_2), and many others. Nowadays, these sensors are very cheap for massive implementation in different systems and households. Based on this thesis, the most important gas for detection and measuring is carbon dioxide. Currently, there are several methods and principles used for measuring the concentration of carbon dioxide in the air. [32]

The first one is called the Nondispersive Infra-Red which is based on emitting an IR beam through the air which consists of carbon dioxide. The sensor measures the amount of the absorbed IR light. The signal from the infrared detector is further amplified and then evaluated by other electronics which can determine the concentration of carbon dioxide.

The second approach is focused on the Electrochemical sensors which consist of an electrochemical cell filled by the electrolyte. The sensor is measuring the electromotive force using special electronics and this value is used for the determination of the concentration of CO_2 in the air.

The last method for measuring CO_2 is based on the Electroacoustic sensors which operate on the frequency ultrasound evaluation of changes in the mechanical resonator. The change in the frequency of the ultrasonic waves is used for the determination of the concentration of CO_2.

6.1 Air Quality Sensor CCS811

This sensor is used for measuring air pollution and air quality. It is a digital gas sensor that has integrated a metal oxide (MOX) gas sensor to detect Volatile Organic Compounds (VOCs) for indoor air quality monitoring with a microcontroller. Internal logic can further process raw sensor measurements to output an equivalent to CO_2. The CCS811 supports multiple drive modes to take a measurement every 1 second, every 10 seconds, every 60 seconds, or every 250 milliseconds. The chip can communicate with the microcontroller via the analog or digital interface depending on the application. The most suitable solution with the microcontroller is communication via the I2C interface, where several chips can be connected to just one bus line. The chip has a very small dimension of 2,7 x 4 mm according to the LGA Package for Surface Mount Device.

7. Multi-chamber Windows

Nowadays, almost all windows in private or industry areas are multi-chamber due to the thermal insulation properties and durability. Due to the standardization, the contact glass break detector must be placed on the inner side of the protected window which is the first glass panel. The simple window with just one glass panel is very easy to put the detector on the first inner glass panel. However, the multi-chamber window has at least two independent glass panels [33] and it is impossible to install the glass-break detector into the finished window. The main disadvantage which causes false alarms is the multi-chamber window. Current standardization for contact glass-break detectors does not deal with the multi-chamber windows. The current combination of the contact glass-break detector with the multi-chamber window is illustrated in the following figure.
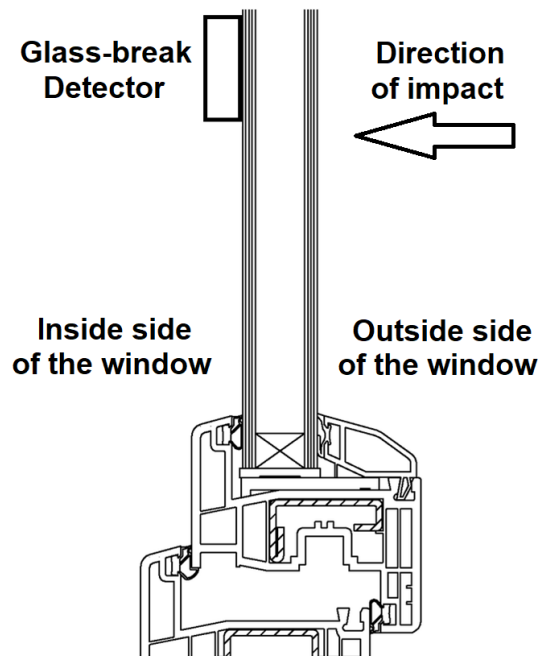

Fig. 3 Current situation of the glass-break detector and the window

The construction of the multi-chamber window can be divided into two main parts. The first one is the glass panels joined together by the spacer and the special glue. The gap between the glass panels is filled by the special gas which reduces the thermal conductivity of the space between two or more window panes. [34] The argon gas insulates better than ordinary air and the thermal insulation function of plastic windows is better. As a result, the argon gas has less energy and transfer less heat than diatomic molecules and it is heavier than oxygen. The second is the plastic frame where the glass panel is placed. The frame is usually divided into several chambers which provides more insulation.

7.1 Energy Losses of Multi-chamber Windows

As mentioned before, the current position of the contact glass-break detector is on the inner side of the window and the impact is situated on the opposite side. It means that the energy needs to travel through whole glass panels and the plastic frame. Some energy created by the impact is absorbed by the transitions between several components in the complex window before it gets to the outer glass panel. According to this information, the first test was created to prove the energy losses between several components in a multi-chamber window.

This test is done by the two independent accelerometers MPU-6050 which are active parts for the final concept of the glass break detector. Each of the MPU-6050 is placed on the inner and the outer side of the multi-chamber window. Both devices are connected to the microcontroller called ATtiny328P using the I2C interface. [35]. For better illustration and minimal distortion, the program uses the I2C interface which can communicate with both devices with minimal time delay. The concept should show the bending differences between the inner and the outer glass panels in the multi-chamber window. The schematic part of the connection between the microcontroller and the accelerometers is shown in the following figure.
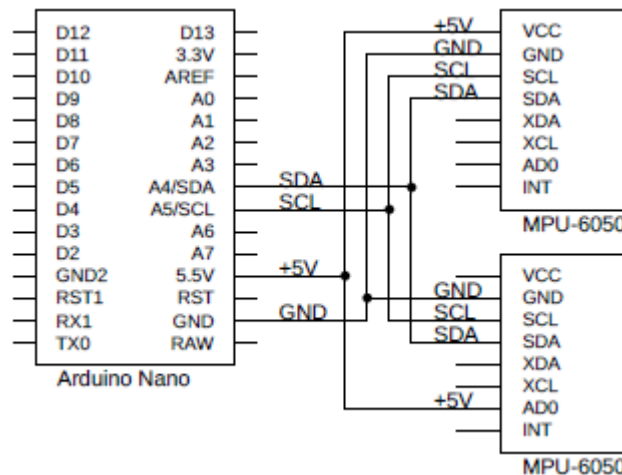

Fig. 4 Schematic part of the energy lost in the multi-chamber window

For consistent evaluation and illustration for the energy lost in the multi-chamber window, the setup for the Impact resistance of hard object on glass was chosen which is listed further in the chapter named *8.3.3 Impact Resistance of Hard Object on the Glass (pp. 37)*. The vibration from the accelerometers is measured and transmitted to the microcontroller which displays the outcome on the screen used by the Arduino IDE. [36] This experiment should prove and record the possible energy lost in a multi-chamber window at least in one standard glass type listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. The outcome of the experiment can be found in the following figure.
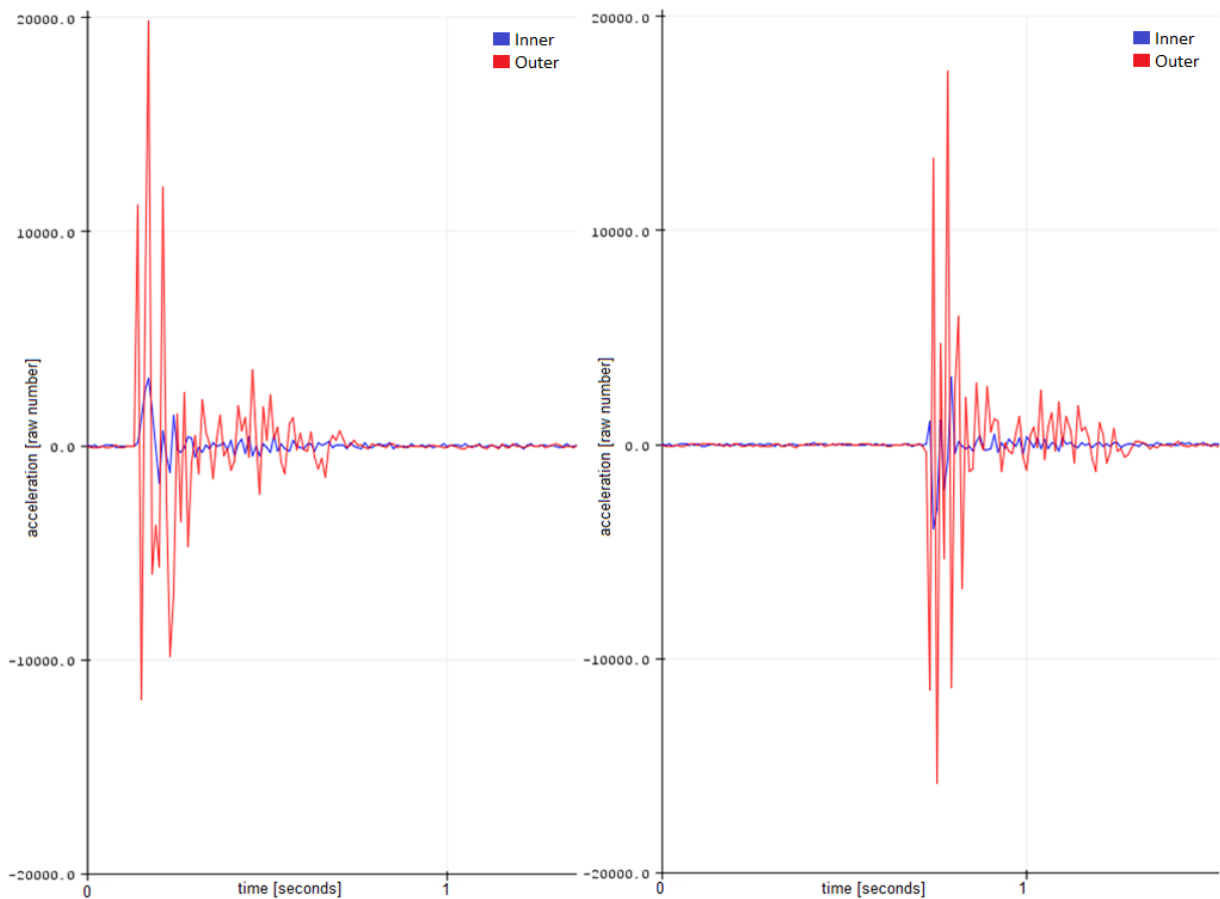
Fig. 5 The energy differences between the inner and outer side of the glass panel

The previous figure shows the illustration of vibrations created by the impact on the glass panel by the rubber ball from the experiment Impact resistance of hard object on the glass. The output of the accelerometer in form of the raw number is detailed explained in further chapter *9.7 Signal Processing and Evaluation (pp. 56)*. This experiment was done 20-times in the same conditions to achieve a sufficient amount of measurements. The outcome is listed below.
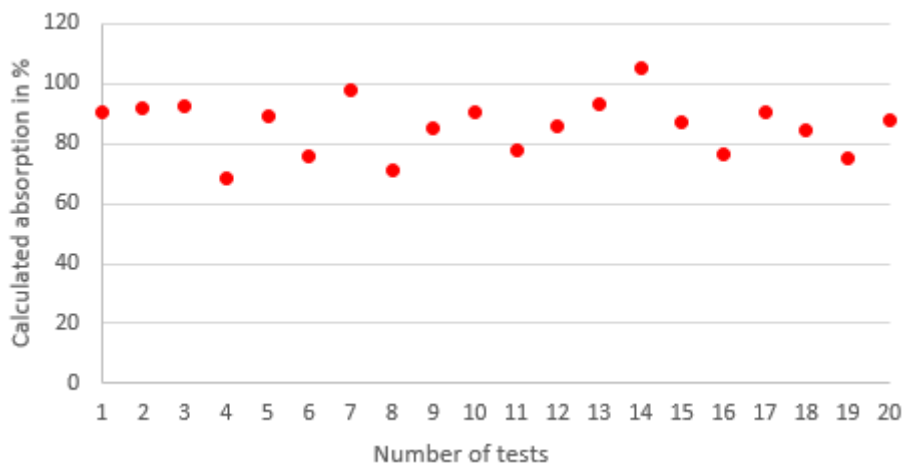

Fig. 6 The outcome of the energy absorption experiment

The experiment shows that the absorption of the energy by the frame is 85.05 % for a normal glass panel. According to this problem, the approach of the glass-break detector is designed and described in the following chapter.

7.2 Glass-break Detector Inside of the Multi-chamber Window

According to the previous chapter, the new concept of the contact glass-break detector is installed inside of the chamber of the glass panel. This design should bring major advantages. The biggest advantage of the new concept is the placement of the detector inside of the glass panel which can measure the energy of the impact without any losses or distortion by the frame. The second advantage is the dimension and the placement which make the detector almost invisible in the glass panel and technically unreachable for the potential intruder.

The placement inside the glass panel of the window is a very difficult task and it has a lot of problems. The main issue is the dimensions of the detector which must be placed inside of the glass panel of the window which is less than 1 cm high. Moreover, the detector itself should not be big and obscure the view of the window. According to the mentioned problems, the design is divided into two parts, one for the active part for the measurements and the second for the evaluation and accessories. The new concept can be found in the following figure.
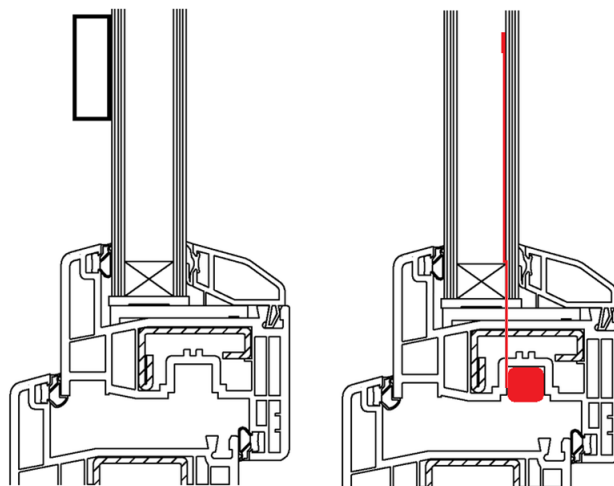

Fig. 7 The new concept of the Glass-break detector in the multi-chamber window

The visible active part of the glass-break detector which is installed inside of the glass panel consists only of the accelerometer MPU-6050 and the air sensor CCS811 placed on the flexible PCB strip. The flexible strip is very adaptive for passing the energy from the impact to the MPU-6050 without any distortion. Moreover, the flexible part is almost see-through and it is suitable for embedding into the glass panel of the window. The biggest problem of the design is fact that the flexible strip with the MPU-6050 and the CCS811 must be inserted into the glass panel in the manufacturing

process. This problem was consulted with the manufacturer of the multi-chamber windows called STIMOS-OKNA. The technical person responsible for the technological part of the manufactural process stated that the concept is possible. The critical parameter for embedding the strip into the chamber is the thickness of the strip which is 0.12 mm [37] which is acceptable for the final gluing and pressing two parts of glass panels together.

The second part is focused only on the technical part and final evaluating of the data from the MPU-6050 and the CCS811. The main part is the microcontroller ATmega8 which is fast enough and it also has the proper interface for communication with the MPU-6050 and CCS811. The problem comes with the placement in the window which was also consulted with another company VD Glass focused only on merging the multi-chamber glass panels with the plastic window frame. Placing the detector inside of the frame was chosen as the most convenient and easy way after several experiments. The detector inside of the frame is suitable for the connection with the strip, hidden and protected against the potential intruder. The concept of the technical connection between the strip with the MPU-6050, CCS811, and the technical part of the detector can be found in the following figure.

Fig. 8 Concept of the physical connection of the prototype

The final prototype of the detector composed of two independent parts can be found in *Appendix 3: Photo of the Detector together (pp. 80)*. The detector should be constructed according to CSN CLC/TS 50131-2-7-2: Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive). This standard guarantees reliable functionality in different environments. These requirements are discussed in the following chapter.

7.3 The Technical Part of the New Glass-break Detector

As mentioned before, the final design consists of two parts. The first one is the main part which is responsible for the evaluation and communication with the CIE. The main component of this part is the main microcontroller ATmega8 which receives the

data from the accelerometer, air sensor and also provides communication with the CIE. The microcontroller is equipped with 23 Programmable I/O lines, where some of the pins support PWM and analog inputs. [38] The 8 MHz crystal is used for the lower power voltage 3.3 V. The connection between the ATmega8, MPU-6050, and the CCS811 using mentioned I2C which uses two wires SDA and SCL. Both wires must be pulled up by the additional resistors to the operating voltage. [39] The main schematic components are listed in the following figure.
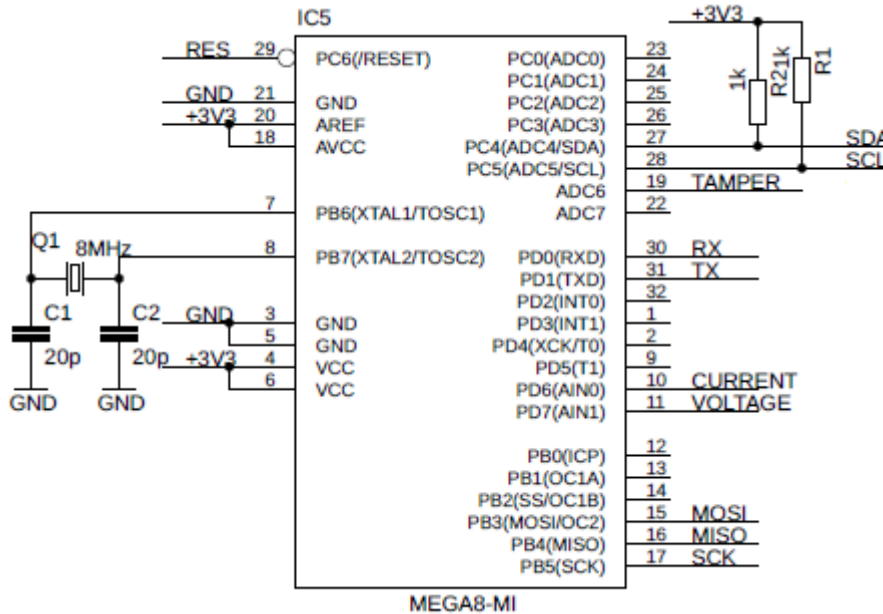

Fig. 9 Schematic part of the main part of the detector

Many of the commercially made detectors has usually external communication interface based on the RS-485 with specialized software. This design should be followed for easy integration in existing applications for technical security. However, the microcontroller ATmega8 does not have an RS-485 interface. This interface must be added to the schematic using the chip LTC485S which is a converter between the UART and RS-485. This chip is bidirectional and does not need any software. The connection between the LTC485S and the ATmega8 is listed in the following figure.
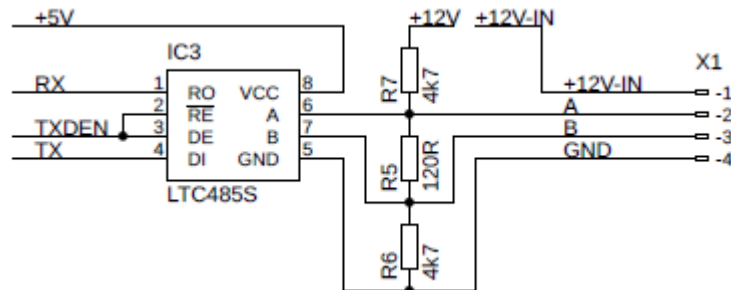

Fig. 10 Schematic part of the communication via the RS-485

The board itself needs to have voltage regulators for different voltages. Usually, the main voltage which is distributed by the CIE is 12 V DC. This voltage is also used by the communication interface RS-485. However, this voltage must be regulated to 5 V

for the current measuring and the 3.3 V for the ATmega8, LTS485S, MPU-6050, and CCS811. The increasing and the step increasing of the power voltage is protected by the first fixed voltage stabilizer TS1117BCW50 for 5 V which has the operating range from 7 V up to 15 V. The ripple of the power voltage is protected by the input and output set of the capacitors which can smooth the output voltage in case of the sinus input. Another function is the current consumption measured by the chip ACS712 and the input voltage measured by the simple voltage divider. All schematic part focused of the power part is listed in the following figure.
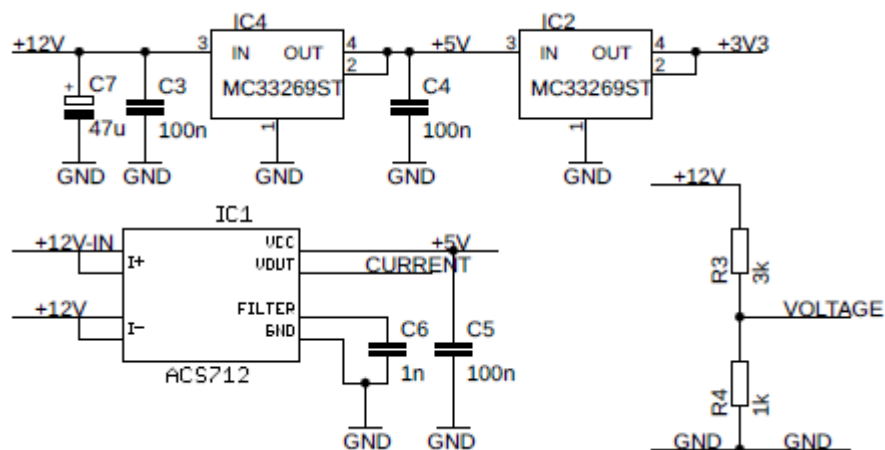

Fig. 11 Schematic part focused on the power voltage distribution and measuring

The final physical PCB should be as small as possible due to the limited space inside of the gap between the window frame and the panel. At the edge of the mainboard is placed the terminal where a flexible PCB strip can be soldered at 90 degrees. The bottom side also has the tamper button. Both sides of the PCB can be found in the following figure with the labels.
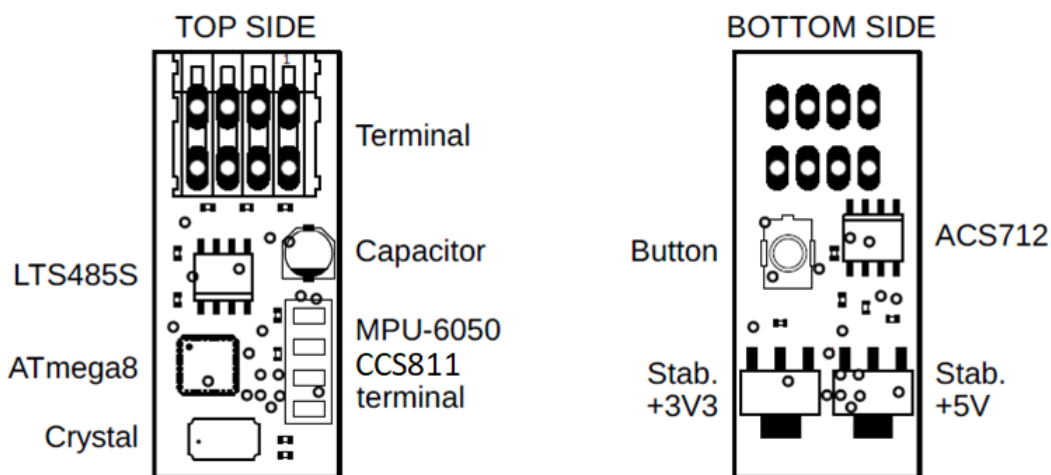

Fig. 12 Physical design of the Glass-break detector prototype

The real photography of the physical design of the evaluating part of the detector can be found in ***Appendix 1: Photo of the Evaluating part of the Detector (pp. 78)***.

The second part of the glass-break detector is focused on the vibration capturing by using the accelerometer MPU-6050. This part is manufactured by the flexible PCB which is bendable, light-weight, and very slim. The second component on the flexible PCB is the sensor CCS811 which can measure the concentration of carbon dioxide in the surrounding air. The schematic part consists of the accelerometer MPU-6050 and CCS811 which can be seen in the following figure.
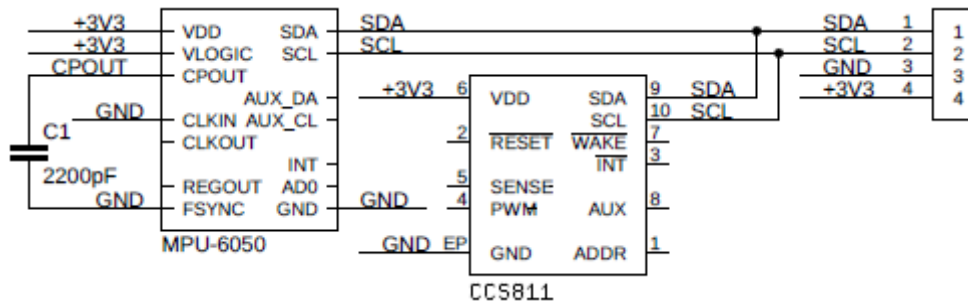

Fig. 13 Schematic design of the flexible strip

The physical design of the flexible PCB is done in form of a long strip that can have up to 1 m in length. The concept of the physical design can be found in the following figure.

Fig. 14 Physical design of the flexible strip

The real photography of the physical design of the active part of the detector can be found in *Appendix 2: Photo of the Active part of the Detector (pp. 79)*.

The company STIMOS-OKNA also stated that the multi-chamber glass panels are usually filled with 90-95% inert gas at normal atmospheric pressure, typically the argon gas is used for its good thermal insulation. The glass panels are very well encapsulated and the company reports a maximum gas leakage of up to 5% per year. The service life of the glasses is calculated at 20 - 25 years. According to this information, the mentioned sensor CCS811 was also placed on the flexible PCB to periodically measure the concentration of the carbon dioxide that should not be presented inside of the multi-chamber glass panel.

7.4 Embedding Detector Inside of the Multi-chamber Window

The biggest challenge comes with the whole idea of embedding the glass-break detector inside of the multi-chamber window. As mentioned before, the design is divided into two parts. The first part in form of the flexible strip with the accelerometer and the air sensor must be placed inside of the glass panel called window filling. The second part is a standard PCB with all needed components for the signal processing and evaluation placed inside of the plastic window frame.

The first problem is that these two parts of the plastic window are manufactured separately in different locations by different manufacturers. However, both manufacturers must communicate and share the information of the order from the customer. The whole process of ordering by the customer begins at the manufacturer which installs the final window at the customer. This manufacturer is focused only on the manufacturing of the plastic framing of the window. Usually, this manufacturer measures or gets the dimensions of the hole for the window. The dimensions are used for the framing and this dimension also specifies the dimensions of the window filling which are sent to the company for the glass panel processing. Then that glass panel is sent back to the framing company which embeds the glass panel into the plastic frame.

The whole process is very common and the final embedding of the glass-break detector inside of the multi-chamber must follow this process. It means that the flexible strip with the accelerometer and air sensor must be placed into the multi-chamber glass panel by the window filling company. The evaluating part of the glass-break detector must be embedded into the window frame by the company focused on the plastic framing.

The minimal and the maximal dimensions of the window must be strictly given for the proper function and detection of the glass-break detector. The company STIMOS-OKNA which is focused on the plastic framing stated, that the up to 90% of the customer demands the height of the window of 120 cm. The width of the window can differ. However, the common width according to the STIMOS-OKNA is from 60 cm to 120 cm. The main information from the dimension is that the height is mostly 120 cm. This number is very important for the placing of the flexible strip which should be placed always in the middle of the window.

For wide manufacturing of the glass-break detector based on this design is very important to have only one design that fits most of the offers of the customers. It means that the flexible strip should be 60 cm long and it should be installed into the window filling vertically. This installation guarantees that the accelerometer and air sensor on the flexible strip 60 cm long placed vertically will be almost always horizontally centered. The vertical placement should be always in the middle of the width of the window filling. The situation can be found in the following figure.
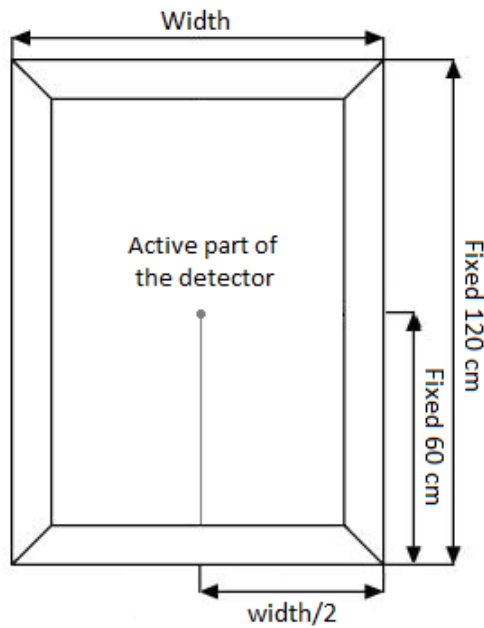
Fig. 15 Physical design of the Glass-break detector prototype

The photography of the embedded detector into the Multi-chamber window can be found in ***Appendix 4: Photo of the Detector embedded inside of the multi-chamber windows (pp. 81)***. The embedding part of the flexible strip into the window filling can be done according to the previous figure by a person who is not educated or certified for installing the IAS. The person only glues the flexible strip with the accelerometer and air sensor on the inner side of the most outer glass panel while merging multi-chamber glass panels. The strip must stick out 4 cm to ensure connection to the evaluating part of the glass-break detector placed in the frame. After this stage when the flexible strip is embedded into the window filling, the multi-chamber glass panel can be exported to the plastic framing company.

The plastic company can very easily put the multi-chamber glass panel into the plastic frame. The tiny gap in the bottom part of the frame must be milled to ensure a flexible strip passing through the frame to its outer place. This gap has a very small dimension of 1 mm x 10 mm only for the passing through the one end of the flexible strip where the evaluating part of the detector will be connected. To ensure the unchanged insulating properties, the gap with the flexible strip is sealed by the assembly sealant.

The profile of the plastic frame for the windows is the same for all types of windows. Every plastic profile has a gap that is used for the security fitting and the gap is created around the whole frame. The fitting is also used for the locking mechanism which allows the opening of the window. Usually, the fitting is placed around the whole casing based on the manufacturer. However, the mechanism has several places on the window where it is placed and not all of them must be used in the assembly. It means that the bottom part of the fitting can be removed and the gap can be used for the evaluating part of the detector.

This approach was consulted with the STIMOS-OKNA company and also by the standardization of the security fitting some parts can be ignored based on the installing difficulty. Every mentioned part of the embedding process was consulted with the STIMOS-OKNA company and with the company focused on making windows filling. Both companies were introduced with the final concept and both companies stated, that it is possible without any additional equipment or knowledge. It means that this concept and procedure can be accepted by other companies in the future.

8. Technical Requirements for the GB Detector

This chapter is focused on the technical requirements for the testing of the glass-break detectors using the standardization CSN CLC/TS 50131-2-7-2: Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive). This standardization states the requirements for glass-break detectors installed inside of the protected buildings with the application of all Security Grades from I: up to IV.

The main function of the detector is detecting the force generated by the mechanical impact of the object on the glass panel which leads to the protected area. Moreover, the detector must provide a specified range of the messages and signals for further applications in the IAS. The more unspecified function can be added to the software of the detector without the influence of the main function.

8.1 Functional Requirements

This chapter is focused on the functional requirements which are given by the standardization and every detector must meet given demands. All requirements can be reached by the software solution according to needed Security Grades.

8.1.1 Event Processing

Every detector must process and evaluates the events which are given by the standardization. The main event is the alarm triggering by the intruder which must be done for all Security Grades. These events are listed in the following table.

Tab. 1 Signal processing according to Security Grade

Event	Security Grade			
	1	2	3	4
Triggered by the intruder	M	M	M	M
Idle state	M	M	M	M
Masking	O	O	M	M
Sabotage	O	M	M	M
Low power voltage	O	O	M	M
Power loss	O	M	M	M
Local self-test	O	O	M	M
Remote self-test	O	O	O	M
O = Optional; M = Mandatory				

8.1.2 Signal and Message Generating

Every alarm detector must be able to generate a specific signal or message according to the mentioned events. This signal must be transmitted wirelessly or via the metallic cable to the CIE in a given form and time. All needed signals according to the event type are listed in the following table.

Tab. 2 Signal or message generating based on the event

Event	Signal Type		
	Alarm	Sabotage	Failure
Triggered by the intruder	M	NA	NA
Idle state	NA	NA	NA
Masking	M	O	M
Sabotage	NA	M	NA
Low power voltage	O	O	M
Power loss	M	O	O
Local self-test - satisfactory	NA	NA	NA
Local self-test - unsatisfactory	NA	NA	O
Remote self-test - satisfactory	M	NA	NA
Remote self-test - unsatisfactory	NA	NA	M
M = Mandatory; NA = Not Allowed; O = Optional			

Despite these main signals, there are also additional signals mostly for the Integrated Alarm Systems which are very often supplemented to a classic alarm system. These additional signals must meet the requirements for the Integrated Alarm Systems and the evaluation of additional signals must not affect the main function of the IAS.

8.1.3 Time Requirements

The detectors using the metallic wiring must trigger the alarm signal under the 15 second after the previous signal or message and the wireless has much more complicated requirements. However, this research is focused only on metallic wiring. The detector must be operating normally after 180 seconds after switching on and it must be able to process the local or remote self-test every 24 hours without the negative impact of the main function. These time requirements are valid for all alarm detectors despite the Security Grade.

8.2 Detection

The detection is the most important part of the standardization which must trigger the alarm signal if the glass panel is destroyed. The detector must trigger the alarm signal even during the testing with requirements listed in the following table.

Tab. 3 Requirements for the detection testing

Requirement	Security Grade			
	1	2	3	4
Main detection test	M	M	M	M
Drilling by the diamond drill	O	O	O	M
Cutting the glass	O	O	O	M
O = Optional; M = Mandatory				

The detection testing is divided into three independent categories depending on the Security Grade. Each category is focused on the different intrusion approach.

8.2.1 Main Detection Test

The main test is based on the falling steel ball with a diameter of 100 mm through a plastic tube with a diameter of 110 mm. The angle of the tube and the glass panel is 45 °. The end of the tube is modified and the tube must be placed 50 mm in front of the glass panel. The setup of testing equipment is shown in the following figure.
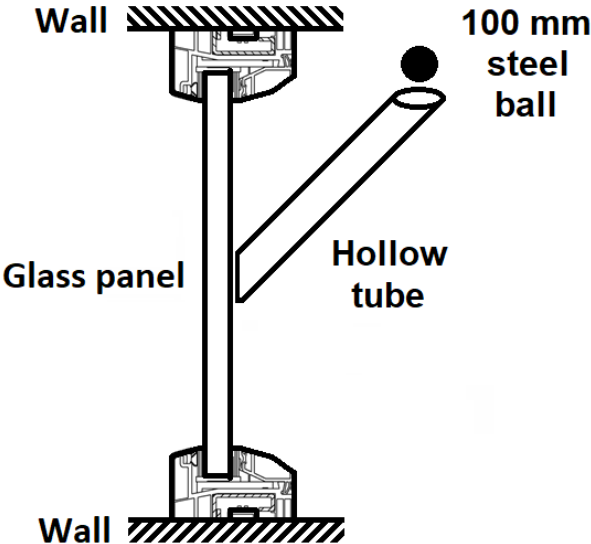

Fig. 16 Settings for the verification of the Main detection test

The main test must be done by using all recommended types of glass which are listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. The minimal number of the test is set at 8 samples. 7 of 8 attempts must be detected for each type of the glass panel. Moreover, the features of the testing glass panels are a little bit different from

the standard type of glass panels, and also the height of the fall is varying for a different type of glass panel. All mentioned limitations and requirements are listed in the following table.

Tab. 4 Additional information for the Main detection test

Glass type	Maximal thickness	Maximal height of the fall
Normal	8 mm	1,1 m
Coated	9 mm	12,0 m
Hardened	8 mm	1,8 m
Insulated	20 mm	1,8 m
Wired	8 mm	1,8 m

8.2.2 Drilling by the Diamond Drill

The main aim of this test is to ensure that the detector can identify the change of the glass panel entirety. The detectors are mounted on the glass panel according to the manual and the testing is done by drilling a hole with a diameter of 20 mm with the diamond drill bit from the outside side of the glass panel. The drilling is done four-time in different locations. The first hole is drilled at the furthest point away from the detector on the panel and three-times in the random points on the glass panel.

The detector must detect the change of the entirety of the glass panel at least three times in a random location. The drilling is very often used to drill a hole and the detector can be deactivated or destroyed through the drilled hole. This type of testing must be applied to all types of glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. This test must be replayed for each type of glass panel.

8.2.3 Cutting the Glass

This test is done using three detectors which are mounted on the inner side of the glass panel according to the user manual. The cutting is done by the common glass cutter, and the glass panel is carefully scratched in form of a circle that is 100 mm in diameter. The detector must trigger the alarm after removing the loose part of the glass panel. This test must be replayed for each of the types of glass panels listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. However, the standard glass cutter is not specified further in the standardization, and the testing person can choose between several types currently on the market.

8.3 False Alarm

This part aims to test if the influences of the surrounding environment can negatively act on the detector. The detector must not trigger the alarm signal during the testing procedure which is divided into several independent categories each focused on a different type of the influence. Before and after each test the main test must proceed to ensure the detector is working properly.

8.3.1 Impact Resistance of Small Object on the Glass

This testing aims to ensure that random influences that have no physical impact on the glass panel do not trigger the alarm. The typical non-alarm influence is the hail storm. In this case, the 6 detectors are mounted on the inner part of the glass panel and 3 kg of the poly-oxy-methylene ball are launched by the plastic tube on the glass panel. The plastic tube is 180 cm long and placed 50 mm in front of the glass plane. The settings of this testing are following.
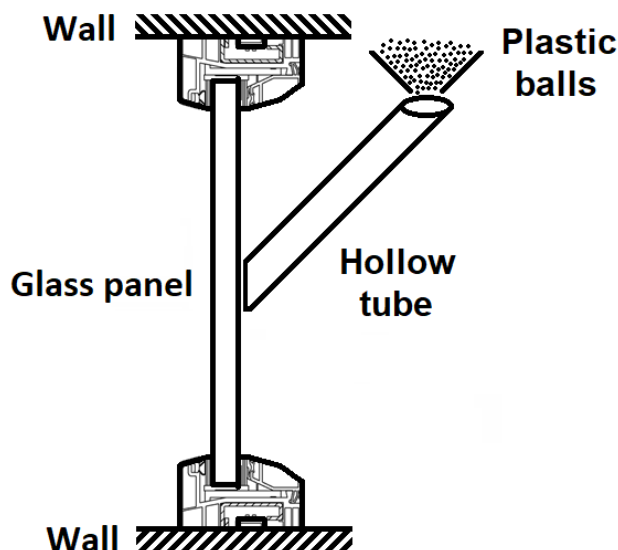

Fig. 17 Settings for the Impact resistance of small object on the glass

The features of the poly-oxy-methylene balls have very specific properties and specifications. It can be purchased as plastic ball bearings, and the specification is listed in the following table.

Tab. 5 Specification of the poly-oxy-methylene balls

Material	Delrin 500 or 100
Density	1 390 kg.m^{-3}
Diameter	12 mm ± 1 mm
Amount	790 to 800 pieces
Hardness	115 HRR to 122 HRR

8.3.2 Impact Resistance of Soft Object on the Glass

This testing simulates the soft object which can hit the glass panel like a punch with a human fist. In this case, 6 detectors are placed on the glass panel and the hitting force is created by the pendulum with the rubber ball on its end. The proper testing must be done without any bouncing of the rubber ball and the setting of this test is showed in the following figure.
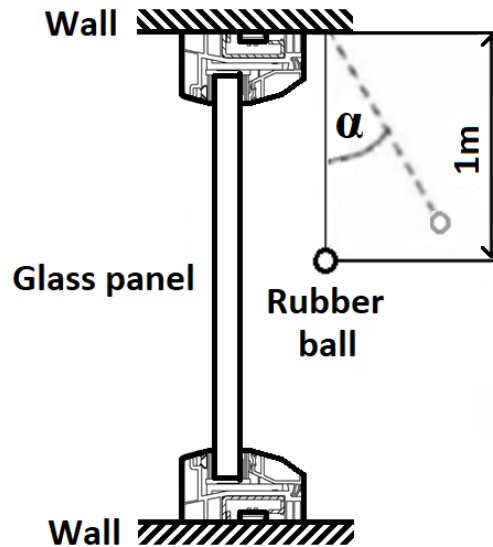

Fig. 18 Settings for the Impact resistance of soft object on the glass

The features of the rubber ball are also very specified and the ball must be solid. The mounting mechanism must not change the center of the mass for the whole ball. The specification given by the standardization is listed in the following table.

Tab. 6 Specification of the pendulum for soft object testing

Pendulum	rubber ball
Diameter	80 mm ± 5 mm
Weight	0,38 kg ± 0,05 kg
Angle α	60 ° ± 5 °
Number Of Tests	5
Time Between Tests	5 s

8.3.3 Impact Resistance of Hard Object on the Glass

This part of the testing is focused on the impact of the hard object which is falling to the glass panel like hitting by the bicycle handlebars. In this case, 6 detectors are placed on the glass panel and the hitting force is created by the pendulum with the steel ball on its end. The proper testing must be done without any bouncing of the steel ball and the setting of this test is showed in the following figure.
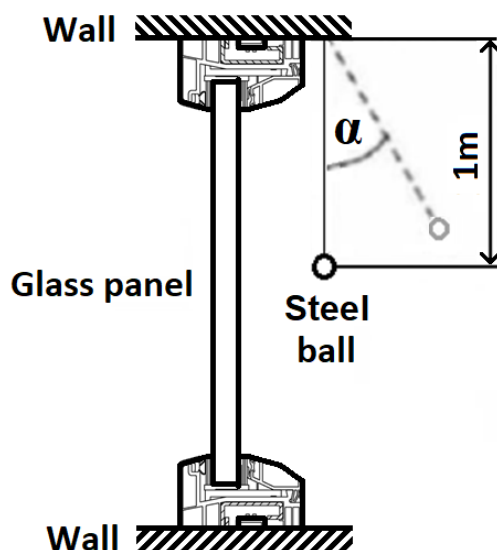

Fig. 19 Settings for the Impact resistance of hard object on the glass

Due to the steel material which is much denser the rubber ball has only 40 mm in diameter. The standardization also mentioned that the surface of the steel ball must be polished and other features of the steel ball are listed in the following table.

Tab. 7 Specification of the pendulum for hard object testing

Pendulum	steel ball
Diameter	40 mm ± 3 mm
Weight	0,26 kg ± 0,03 kg
Angle α	60 ° ± 5 °
Number Of Tests	5
Time Between Tests	5 s

8.3.4　Static Pressure Resistance

This test simulates the permanent pressure which can be created on the glass panel. This can be caused by the tension of the glass panel or by the force of the leaning object of the glass panel. The 6 detectors are placed on the glass panel on the inner side and the pressure is created by the pneumatic cylinder or another type of force with the following experiment.
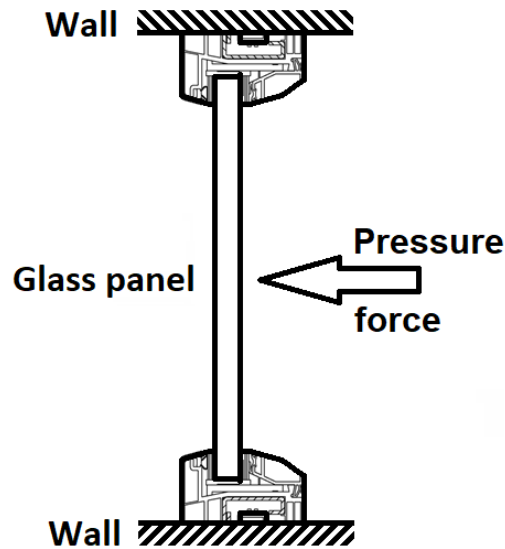

Fig. 20 Settings for the Static pressure resistance

The standardization gives only information about the diameter of the cylinder and the force. The actual setting of the experiment is only a preview, and the settings of this experiment can differ from the preview. Further instruction for the experiment is listed in the following table.

Tab. 8 Specification of the cylinder for the static testing

Force of the pressure	$100\,N \pm 5\,N$
Duration of the force	5 s - 6 s
Number of tests	5
Time between tests	5s
The diameter of the cylinder	5 cm

8.3.5 Dynamic Pressure Resistance

This test is done due to the dynamic pressure differences which are forced at the middle of the glass panel like atmospheric pressure, strong wind. In total, six detectors must be placed on the glass panel on the inner side. The pressure is created by the pneumatic cylinder whit the following features.
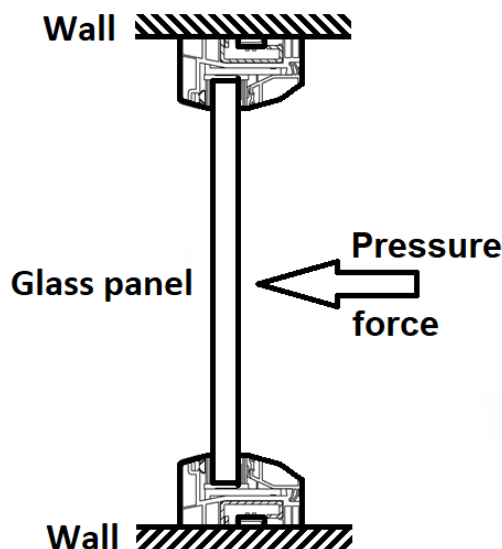

Fig. 21 Settings for the Dynamic pressure resistance

The experiment is very similar to the previous one with a slight difference in the force and time duration. The specification for further testing is also listed in the following table.

Tab. 9 Specification of the cylinder for the dynamic testing

Force of the pressure	50 N ± 2,5 N
Duration of the force	1 s - 2 s
Number of tests	5
Time between tests	1 s
The diameter of the cylinder	5 cm

8.3.6 Broadband Noise Resistance

This test is simulating the noises which can be outside or inside of the protected glass panel. The frequency is very close to the real frequency of the breaking glass and it must be ignored by the detector. The active part of this test is the integrated circuit with the hard leads. Using the integrated circuit are created vibrations on the glass panel by pushing and moving the integrated circuit. The maximal duration of this test is set at 5 minutes. This test does not include any further information or instruction.

8.4 Sabotage

All components and adjusting elements that could affect the function of the detector must be located inside the detector cover. Access to these components must require the use of appropriate tools and must generate a sabotage signal before gaining access to the inside of the detector. The access must not be possible without triggering the sabotage signal or causing visible damage. A sabotage signal should be generated even the detector is removed from the mounting surface. The detector must have the function to detect the blocking of the main function, and the sabotage protection requirements for each Security Grade are given in the following table.

Tab. 10 The sabotage protection requirements for each Security Grade

Requirement	Security Grade			
	1	2	3	4
Casing durability	M	M	M	M
Removing from the glass	O	M	M	M
Masking detection	O	O	M	M
Resistance against mag. field	O	M	M	M
O = Optional; M = Mandatory				

The maximum response time to cover the detection device must be 180 seconds. The masking detection should be signaling by the requirements given in *Tab. 1 Signal processing according to Security Grade (pp. 31)*. The signals shall remain active for at least the duration of the masking. During the coverage period, the coverage messages must not be canceled and after the coverage is canceled, the signaling itself must be canceled.

All requirements listed in the standardization are a combination of hardware and software approaches which should be evaluated by the main program installed inside of the glass-break detector.

8.5 Electrical Requirements

The idle and maximum current consumption of the detector at the rated input voltage must not exceed the values specified by the manufacturer. The detector must also meet all functional requirements in the range of input voltage +/- 25%. When the voltage rises slowly in a given range, the detector must operate normally without any message, signal, or failure. The detector must meet all functional requirements with a sinusoidal change of the input voltage +/- 10% from the nominal value with a frequency of 100 Hz. Step changes of the input voltage between the maximum and minimum value must not activate any signals. All mentioned requirements are

connected to the Security Grade where some of them are not required. This part of the testing is not focused on the main purpose of the glass-break detector, it is focused mainly on the technical part of the design. The following table applies to detectors that use external power supplies.

Tab. 11 The requirements for the electrical part

Test	Security Grade			
	1	**2**	**3**	**4**
Current consumption	R	R	R	R
Range of the power voltage	R	R	R	R
Increasing the voltage	NR	R	R	R
The ripple of the voltage	NR	R	R	R
Step increasing of the voltage	NR	R	R	R
R = Required; NR = Not required				

9. Threshold Measuring and Testing

All detectors which are coming to the market must be tested by the certificate authority to ensure flawless and reliable function. This authority guarantees that the equipment fulfills all declared information given by the standardization. The test itself takes place in a special room with very strict conditions. This chapter is focused on the testing of the glass-break detectors which are used in alarm applications.

The main idea of the pre-testing in the not-certified room is for the development and the debugging of the design for flawless and reliable function in the real operation. When the prototype of the glass-break detector will pass through all possible scenarios of the standardization in the non-certified room, then it can be sent to the certified laboratory for authorized testing. This approach saves a lot of money and time because all certified procedures are taking a lot of time and also money.

The constructed glass-break detector must be tested to prove flawless and reliable functionality. As mentioned before, the test can be done in the standardized testing facility. However, due to the testing techniques, unofficial testing can be done in the special room if the conditions are fulfilled. According to the standardization testing scenarios are following:

- Functional requirements
- Detection
- False Alarm
- Sabotage
- Electrical requirements

To prove flawless function all scenarios must be tested on the designed glass-break detector. Special laboratory in Tomas Bata University in Zlín at Faculty of Applied Informatics was created according to the standard CSN CLC/TS 50131-2-7-2: Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive). The main goal of this testing is to prove that the detector can pass through all scenarios listed in mentioned standardization. The room must have specific properties which are listed in the following table.

Tab. 12 Conditions of the testing room

Temperature	15 °C to 35 °C
Relative Humidity	25 % to 75 %,
Air Pressure	86 kPa to 106 kPa

During the testing is critical to complete all operating instruction given by the standardization. The detectors must be connected to the nominal power voltage and it

must be connected to the monitoring device which can indicate the signal from the detector. The connection must be stabilized for 180 seconds before the main test. All equipment must be situated in the testing room and the room must be empty.

The main element of the testing is the empty room where the testing window in the firm frame is placed. The frame is placed 1 meter above the ground and it has flexible holdings for different dimensions of the tested glass panels. The frame is fixed very firmly in place and there no chance for the moving of the glass panel in the frame.

The whole testing scenario is based on the one mounting setup which is the same for all scenarios of the testing. It means, that one mounting setup is suitable for all parts and it does not have to change through the scenarios. The critical part of the testing is the evaluation and triggering of the alarm signal in specific conditions given by the standardization. Every scenario of the testing has the specified amount of the glass-break detectors on the glass panel, the triggering element, and the number of repetitions. All this information is listed in the standardization.

9.1 Dimensions and Types of the Glass Panels for Testing

The standardization strictly defines the standard types of glass panels for the testing. These types can be divided into 5 main categories: normal, coated, hardened, insulated, and wired. Further information about standard types of glass panels can be found in the following table.

Tab. 13 Standard types of glass for testing

Type of the Glass	Thickness	Deviation
Normal	6 mm	± 2 mm
Coated	6 mm	± 3 mm
Hardened	6 mm	± 2 mm
Insulated	4 mm	± 2 mm
Wired	6 mm	± 2 mm

The most important feature of the glass panel is also the dimension of the window which is also strictly given by the standardization by minimum and standard size.

- Minimum size: 400 mm to 400 mm
- Standard size: 800 mm to 1000 mm

43

9.2 Functional Requirements

The first and the most important part of the certified testing is the functional requirements which are divided into three main categories: event processing, signal generating, and time requirements. Each category is driven by different criteria for accomplishing and also based on the Security Grade.

Event Processing is focused on the signalization of all possible events given in *Tab. 1 Signal processing according to Security Grade (pp. 31)*. It means that the detector must react to all situations in form of the message transmitted to the CIE. The possible events are following:

- Triggered by the intruder
- Idle state
- Masking
- Sabotage
- Low power voltage
- Power loss
- Local self-test
- Remote self-test

The functional requirements are driven only by the software which periodically updates all possible variables which can change during the operation. This information is then transmitted via the interface to the CIE. There comes the first problem of the complete communication via the CIE which is the software protocol for the communication using the RS-485. The software and command part of the connected CIE is the private information of the company which produces the alarm application. The code is not available even for the researchers. However, the final code can be very easily modified by the company which can use the glass-break detector in the system.

Triggered by the intruder is an event when the main detection is triggered. These cases are very strictly given by the detection described in the following chapter. Other influences and causes must not trigger the main alarm. This event has the main priority over others and the message must be immediately transmitted via the interface to the CIE.

The idle state is the default condition when the detector is not influenced by any negative effect and this condition must be transmitted via the interface on request.

The masking state is must be triggered when the main detecting element is somehow distorted unexpectedly. This event can be caused by the intruder or it can be caused by the failure of the accelerometer MPU-6050 or CCS811. The accelerometer and air quality sensor are placed inside of the multi-chamber glass panel and it cannot

be physically distorted by the intruder. However, both devices can fail and this event must be able to register by the microcontroller. According to this problem, the microcontroller is periodically sending a request for the report. The microcontroller triggers the Masking event when one of the devices does not answer the request. In this case, the Sabotage is not triggered immediately. However, the program set the request for the new initialization of the not responding device and after unsuccessful initialization, the detector follows the program.

Sabotage is triggered when the detector is removed from its original position by the intruder. This function is focused only on the evaluating part of the detector which is placed inside of the window frame by the micro-button. When the detector is removed from the frame, the micro-button is triggered and the Sabotage is also triggered.

The low power voltage function is triggered when the power voltage drops under the given threshold. The schematic and the threshold value is listed in detail further in chapter *9.6 Electrical Requirements (pp. 55)*.

Power loss is a very serious and difficult event to process because the message must be sent to the CIE even the main power supply is unplugged. It means that the detector must have some energy stored when the power is disconnected. This is solved by using the capacitor which can power the detectors for a time that is needed for transmitting the message. More information is listed further in chapter *9.6 Electrical Requirements (pp. 55)*.

Local self-test must be done periodically at least once in 24 h according to *Tab. 1 Signal processing according to Security Grade (pp. 31)* and *Tab. 2 Signal or message generating based on the event (pp. 32)*. That means that the detector must be able to simulate the alarm without transmitting the alarm message to the CIE.

Remote self-test must be done in the same way as the Local self-test. However, it is requested by the CIE and it also must follow the requirements listed in *Tab. 1 Signal processing according to Security Grade (pp. 31)* and *Tab. 2 Signal or message generating based on the event (pp. 32)*.

All mentioned function is conditioned by the Security Grade and the Type of the Signal which is mandatory or forbidden. All functions must be managed according to *Tab. 1 Signal processing according to Security Grade (pp. 31)* and *Tab. 2 Signal or message generating based on the event (pp. 32)*. The last important feature for the Functional requirements is the time requirements that must be implemented into the final program.

As mentioned before, triggering and processing the functional requirements are controlled by the program with several inputs. Some of the inputs have a place in the program itself, and other inputs have the physical trigger like the sabotage function

with the mechanical micro-button. The idea of the Functional requirements is listed in the following part in form of the simplified diagram. This graphical representation is also used from the final structure of the main program for the glass-break detector prototype.
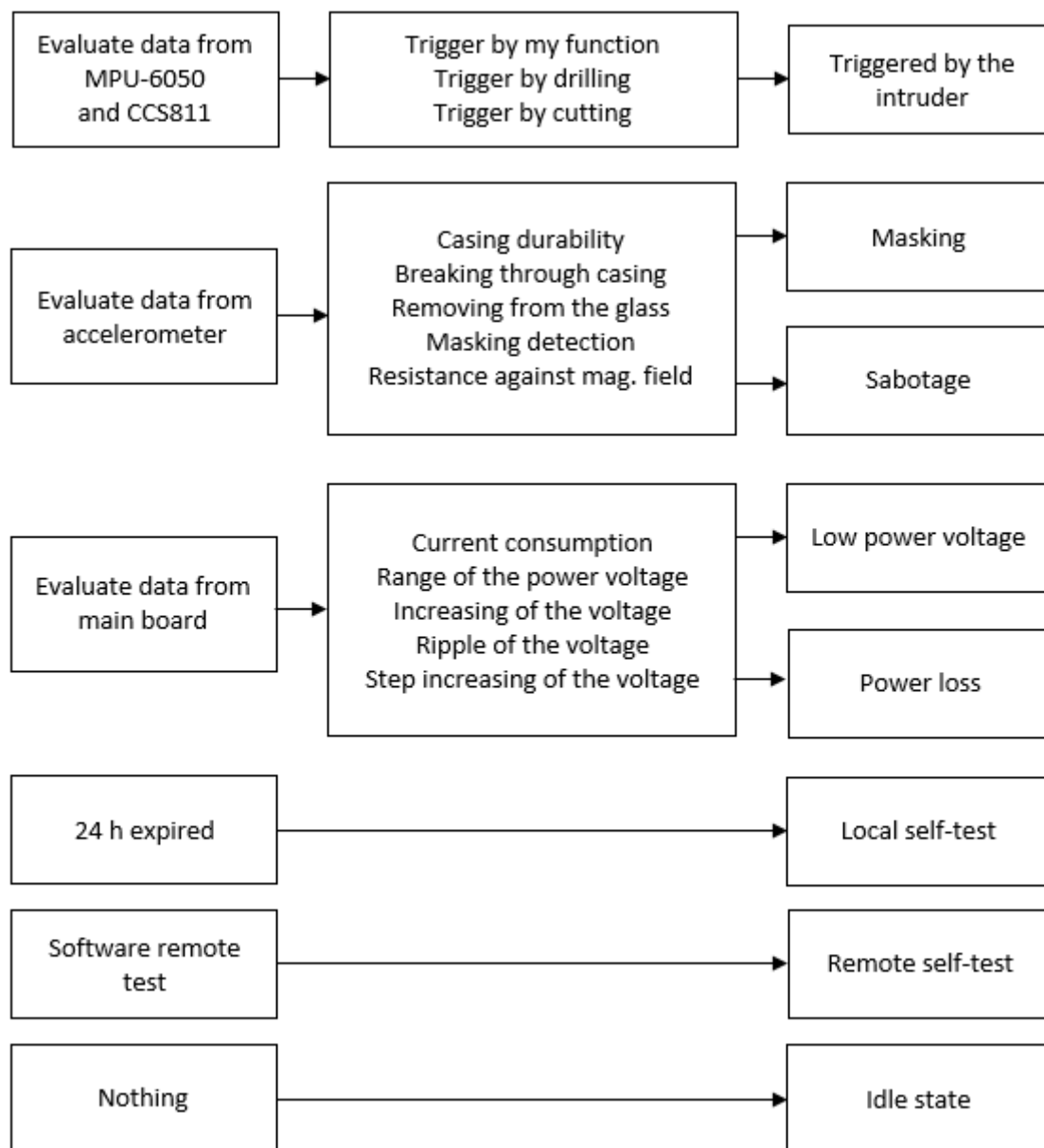

Fig. 22 Graphical representation of the sequence for the functional requirements

9.3 Detection

The first and the most important function of the whole glass-break detector is the main detection test. This function has the highest priority of the program and it must be executed and processed on top of all functions. According to the standardization, additional tests are Drilling by the diamond drill and Cutting the glass for the highest Security Grade.

The following chapters follow standardization. However, according to the destructive and non-destructive testing, the first non-destructive testing focused on the False alarms was tested. The Detection was tested after successful False alarm testing.

The main detection test

The main detection test is done in the room with the specification listed in *Tab. 12 Conditions of the testing room (pp. 42)* and the testing scenario is listed in *Fig. 16 Settings for the verification of the Main detection test (pp. 33)*. According to the standardization, the test must be done for all types of glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. However, this type of testing is destructive which means that each test consumes one window and the test must be done 8-times for each type of glass type. The total number of consumed/destroyed windows just for the main detection test is 40. This number is totally out of the financial range of this thesis.

According to this problem, the detection test was done for all glass types only once. The standardization requires testing of all glass types regardless of the price. The company VD Glass and the STIMOS-OKNA provided one window for each glass type with a discount for the experiment. Other measurements further in this thesis proved that the waveforms of one impact are quite the same.

Each glass type has different behavior according to its thickness, strength, and other properties. The first one was the normal glass where the steel ball broke through both glass panels in the multi-chamber window. The steel ball tear of the active strip of the detector and the program triggered the alarm function. The same happened to the coated glass. The wired and foiled glass type withstand the impact and the accelerometer was able to read the value of the impact. This value was out of the range of the accelerometer which means that the value exceeds the 32 767 raw which is equivalent of the 2 g (20 m/s). More information about this conversion can be found in *9.7 Signal Processing and Evaluation (pp. 56)*. This acceleration can be set as a threshold value for the final program. The main detection test is also supported by the CCS811 which can detect the CO_2 inside of the multi-chamber window after breaking the glass panel.

Drilling by the diamond drill

The second very important test for the main detection is the Drilling by the diamond drill which can be used by the intruder to get to the detector and disarm it. This test is also done in the room with the stable conditions listed in ***Tab. 12 Conditions of the testing room (pp. 42)***, and the test must be done for all types of glass listed in ***Tab. 13 Standard types of glass for testing (pp. 43)***. The diamond drill bit with a diameter of 20 mm is used for drilling a hole from the outside side of the glass panel. This process must be done four-time in different locations on the glass panel. The first hole is drilled at the furthest point away from the detector on the panel and three-times in the random points on the panel. The detector must detect the change of the integrity of the glass panel at least three times in a random location.

The drilling technique is not described in the standardization at all. There is not a single special diamond drill designed for the glass drilling currently on the market. One of the maintainer specialists from the Komponenty, a.s. comes with the idea of drilling technique based on the grinding, where the hollow tube with the diameter of 20 mm is used for the drilling. The abrasive paste consist of diamond particles is applied between the tube and the glass panel. This approach can quite well make a small hole through the glass panel without any compilation.

However, the drilling should create specific types of the vibration which are spreading through the glass panel in all direction. Here comes the biggest problem of this scenario. The vibrations produced by the drill are negligible compared to the measurement uncertainly of the idle state of the accelerometer. It means that the accelerometer is not able to detect this type of vibration. Avoiding this type of scenario is possible. However, the detector must be classified only for Security Grade III. which is unacceptable.

It means that the accelerometer is not able to detect vibration caused by the grinding. According to this problem, the idea of the inert gas in the multi-chamber glass panel was considered. When the glass panel breaks the argon gas inside of the multi-chamber rapidly changes its concentration. This is the reason why an active part of the glass-break detector also consists of the air quality sensor CCS811 which can periodically measure the concentration of the gas in the gap. However, the sensor which can detect the concentration of the argon is very big and expensive. According to this problem, the normal air sensor is used for the concentration of carbon dioxide. When the glass panel is intact, the sensor measures the concentration of the carbon dioxide inside of the multi-chamber glass panel less than 40 ppm. When the glass is broken, the sensor measures the concentration of the carbon dioxide which is approximately 400 ppm in normal air.

Cutting the glass

The last type of detection test is called the Cutting of the glass which is done by the common glass cutter. The cut circle must have a diameter of 100 mm and the detector must trigger the alarm at least on the removal of the loose part of the glass. This test is also done in the room with the stable conditions listed in *Tab. 12 Conditions of the testing room (pp. 42)*, and the test must be done for all types of glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)*.

This scenario has the same problem as the previous one called the Drilling by the diamond drill. The glass cutter is not specified in the standardization and also the vibration caused by the cutting and by the removal of the loose part of the glass is very small. The vibrations and the impact are very similar to the scenario of the false alarm which must not be mixed. It means that also this scenario is not evaluable by the accelerometer and it must be evaluated by the concentration change of the argon inside of the multi-chamber glass panel by the sensor CCS811.

The final successful performing of the Drilling by the diamond drill and Cutting the glass scenario brings the final concept to the highest Security grade. This achievement is very special for glass-break detectors at all.

9.4 False Alarm

The false alarm section is focused on the false alarms caused mainly by the weather influences, and it must not trigger the main alarm function. All presented sub-section are prepared according to the standardization. However, these influences should not be evaluated as a false alarm, it should not be evaluated as the main alarm. It means that following testing procedures should not have any triggers, these procedures must not trigger the alarm.

Impact resistance of small object on the glass

The first type of the false alarm test is called the Impact resistance of a small object on the glass which should resistant against random influences that have no physical impact on the glass panel and do not trigger the alarm. The typical non-alarm influence is the hail storm. The settings for this test is illustrated in *Fig. 17 Settings for the Impact resistance of small object on the glass (pp. 35)*, and the test must be done for all types of the glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)* special balls specified in *Tab. 5 Specification of the poly-oxy-methylene balls (pp. 35)*.

As mentioned before, this influence is not evaluated as a false alarm, it should not trigger the main alarm. This testing should set the threshold limit of this influence and it must be avoided in the Detection program section. This test was done 20 times for each type of glass panel, and the threshold level is listed in the following figure.
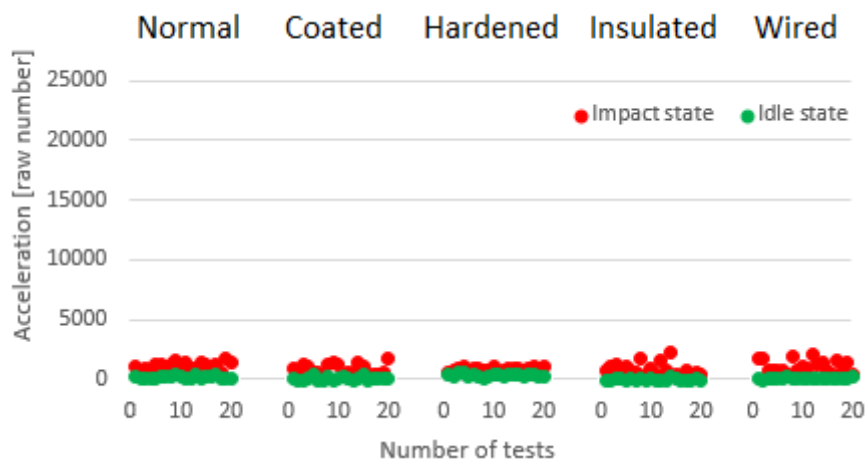

Fig. 23 Impact resistance of small object on glass with all glass panel

The previous figure showed that the impact of small balls hitting the glass has a negligible impact on the glass. The threshold limit can be set to the acceleration equivalent of 2500 and less. As mentioned before, this range must be ignored by the program.

Impact resistance of soft object on the glass

The following type of possible influence is the Impact resistance of soft object on the glass which simulates the soft object which can hit the glass panel like a punch with a human fist. The setting for this scenario is listed in *Fig. 18 Settings for the Impact resistance of soft object on the glass (pp. 36)*. The hitting force on the glass panel is created by the pendulum with the rubber ball on its end with specifications listed in *Tab. 6 Specification of the pendulum for soft object testing (pp. 36)*, and the test must be done for all types of glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)*.

The reason for this experiment is also for the waveform of the impact which must be deleted from the main detection. The total number of tests is also set to 20 times for each glass type and the outcome can be seen in the following figure.
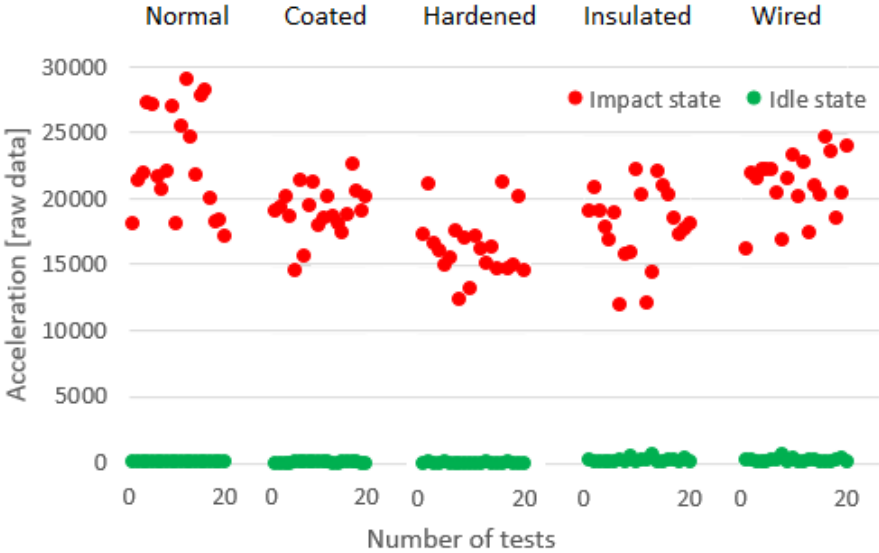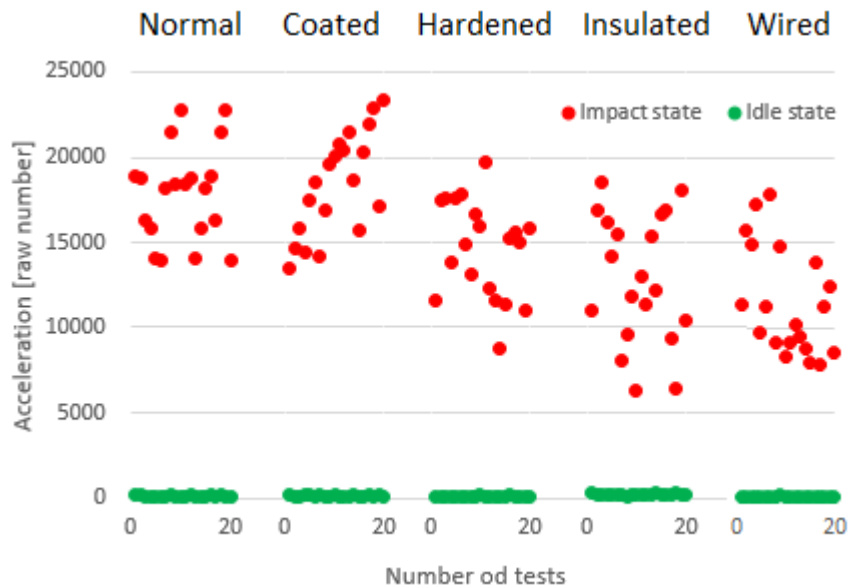

Fig. 24 Impact resistance of soft object on glass with all glass panel

The impact of the rubber ball with a diameter of 80 mm has a bigger impact on the glass panel than the previous one. The previous figure showed that the range of the impact of each type of glass panel is in the range of 10 000 and 30 000. This range must be also avoided by the final program and the total test was set to 20 times for each type of glass panel.

Impact resistance of hard object on the glass

This test is the same as the previous one except for the specification of the hitting ball which should simulate hitting the glass panel by the bicycle handlebars. The features of the steel ball are listed in *Tab. 7 Specification of the pendulum for hard object testing (pp. 37)*. The reason for this experiment is also for the waveform of the impact which must be avoided by the main detection. The total number of tests is also set to 20 times for each glass type and the threshold level can be seen in the following figure.

Fig. 25 Impact resistance of hard object on glass with all glass panel

The hit by the steel ball is very strong and it produces a lot of energy. The range of the measured values is between 25 000 and 5 000, and this range must be avoided by the final program.

Static pressure resistance

The fourth false alarm test is called the Static pressure resistance which simulates the permanent pressure which is created on the glass panel. This can be caused by the tension of the glass panel or by the force of the leaning object of the glass panel. The setup for this experiment can be found in *Fig. 20 Settings for the Static pressure resistance (pp. 38)* and it must be done for all types of the glass listed in *Tab. 13 Standard types of glass for testing (pp. 43)*. The pressure is should be done by a cylinder with features listed in *Tab. 8 Specification of the cylinder for the static testing (pp. 38)*.

As mentioned before, the set is done by the cylinder which creates the pressure on the glass panel. The pressure can be created by the press in a vertical position. However, this experiment can be done also horizontally by using only gravity. The 5 kg heavy cylinder placed horizontally on the glass panel creates the 50 N force horizontally. The acceleration was negligible and this scenario is overlapping with the ide state of the detector. However, this information is suitable because this is the scenario that should be ignored by the program.

Dynamic pressure resistance

The other false alarm resistance testing the pressure is called the Dynamic pressure resistance. This time the pressure is not only static but it is dynamic and it changes in time. The setting is the same as the previous one. The only change is the dynamic pressure created on the glass panel specified in *Tab. 9 Specification of the cylinder for the dynamic testing (pp. 39)*. The horizontal setup using gravity is also used in this scenario. The outcome of this test is the same as the previous one. The forces are negligible and the detector should ignore negligible forces.

Broadband noise resistance

The last false alarm resistance test is called the Broadband noise resistance, which is simulating the noises which can be outside or inside of the protected glass panel. The frequency is very close to the real frequency of the breaking glass and it must be ignored by the detector. The vibrations are created by the integrated circuit with the hard leads by pushing and moving the integrated circuit on the glass panel. The maximal duration of this test is set at 5 minutes.

This also should be the combination of the pressure and squeaking at the same time. However, even this type of impact is negligible and it is simply ignored by the whole program of the detector.

9.5 Sabotage

This chapter is focused on Sabotage which is purposely action aimed at the elimination of the main function of the glass-break detector by the intruder. Sabotage is one of the conditions that must be detected and transmitted to the CIE. This function must not be evaluated as an alarm. According to the standardization, the Sabotage of the glass-break detectors can be divided into 5 different parts. All mentioned parts must be included to fulfill the highest Security Grade.

Casing durability must be protected against the unauthorized intrusion into the detector main board, where the intruder can disarm or destroy the detector before the sabotage message. The construction of the detector is embedded into the window frame where it can be removed only by the opening of the window and the micro button is placed on the bottom part of the detector. It means that the intruder can get to the detector only by the opening of the window which can be detected. Moreover, when the detector is removed, the micro button is released and it can be detected.

Removing from the glass is intended for detectors which are usually placed visibly for the intruder. The removing or moving of the detector can cause a different reaction to the potential intrusion event. The prototype of this glass-break detector is completely closed and protected by the window and window frame. It means it is almost impossible for the intruder to remove the detectors from the inside of the window or window frame. However, to achieve maximal security and meet the standardization, the micro button is installed on the bottom side of the mainboard. When the detector is removed from the window, the micro button is released and the sabotage is triggered.

Masking detection is usually done for the detectors which need some incoming source of the signal which can be blocked or changed by the potential intruder. The active part of the detector is focused only on the acceleration of the glass panel and the gas inside of the chamber. The only way how the intruder can trick the accelerometer is through some kind of silencer of the muffler to absorb some vibration. However, the energy is absorbed by the silencer and does not damage the windows.

Resistance against magnetic field seems to have the reference to the Electromagnetic compatibly. However, this part is focused on the active component of the detector which cloud be sensitive to the magnetic field. The accelerometer and the air sensor are quite sensitive to the magnetic field, and this part is evaluated by the program. When the accelerometer or air sensor is affected by the magnetic field it produces an error message which is evaluated by the program and triggers the sabotage.

9.6 Electrical Requirements

The next chapter is dealing with the electrical requirements. Some of the topics must be monitored and the others must be considered during the design. In all cases, the design is a combination of components and the final program. The main part is focused on the protection against overvoltage and incorrect input voltage. According to the standardization, some of the values must be monitored, and in case of power failure, the detector must generate the Failure message.

Current consumption is a very critical and very important variable that must be monitored. This variable is measured by the chip called ACS712, and the schematic part of this circuit can be found in ***Fig. 11 Schematic part focused on the power voltage distribution and measuring (pp. 26)***. The measured power consumption is compared to the standard which is calculated by the all components on the board. When the power consumption differs a lot, the detector could have some failure, and the failure message must be generated.

The range of the power voltage must also be considered while designing the prototype of the glass-break detector. The recommended power voltage for the prototype is 12 V which is the standard level used in the alarm application. However, the input voltage can differ a little bit from the power supply, and the power management must be able to process voltages within a defined range. This range is given by the static power regulator on the input of the prototype called TS1117BCW50 for 5 V with a schematic which can be found in ***Fig. 11 Schematic part focused on the power voltage distribution and measuring (pp. 26)***. According to the technical documentation of the regulator, the range of the input voltage is in the range from 7 V up to 15 V. This range is used for the glass-break prototype.

Increasing the voltage means, that the detector must operate normally even the input voltage increase in the range mentioned before. This situation can be caused by the interference on the cable or it can be caused by the bad power supply in the CIE. However, this situation must not be evaluated as a failure or alarm. It can happen, and the power management must deal with it. When the input voltage is increased, the regulator must additional voltage transform to the heat. This heat can be released by the body of the regulator. The whole process is already guaranteed by the manufacturer of the regulator.

The ripple of the voltage can be caused only by the high external interference mainly caused by big electric devices like a strong or electric motor. The AC power voltage to the motor can multiply the small voltage to the detector and it can cause rippling of the power voltage. The power management of the detector must operate normally even with a sinusoidal change of the input voltage +/- 10% from the nominal value with a frequency of 100 Hz. This distortion can be very easily eliminated by the

frequency filter at the input of the power voltage part which mainly consists of the capacitors, which can smooth the power voltage. The specific schematic can be found in ***Fig. 11 Schematic part focused on the power voltage distribution and measuring (pp. 26)***.

Step increasing of the voltage is the last influence that can affect the proper operation of the detector. Step changes of the input voltage between the maximum and minimum value mentioned before must not trigger any failure message, and at the same time, the detectors must operate normally. This possible influence is solved by the capacitors placed at the output of the regulator to smooth the output of the regulator. The schematic is listed in ***Fig. 11 Schematic part focused on the power voltage distribution and measuring (pp. 26)***.

All used components for this prototype of the glass-break detector are chosen according to the parameters which are meeting all requirements given by the standardization. It means that the further testing of individual components for electric properties is not necessary.

9.7 Signal Processing and Evaluation

This part is focused on the signal processing of the data from MPU-6050 and the CSS811 by the microcontroller ATmega8. This microcontroller was mainly chosen for the small package, important communicating interface, and sufficient computing power. The microcontroller can be programmed using the Arduino platform which provides C/C++ and wiring code language. This approach is used by many people which creates many examples and libraries for the programming.

As mentioned before, the accelerometer MPU-6050 is a 16-bit data register with a range from (0 <-> 65535) with the sensitivity selection of ranges (±2g, ±4g, ±8g, and ±16g). [40] To measure the acceleration in both directions, the idle state of the acceleration must be in the middle of this range. The output scale for any setting is [-32768, +32767] for each of the axes which means that the accelerometer in this configuration can measure 2 g in both directions. These raw numbers which are transmitted by the accelerometer represent the real acceleration in a given time. It can be further represented in g by dividing the raw number. To get the most accurate number, the raw number can be divided by the number 16384 to get the acceleration ±2g. [40] However, this part gives the idea of the transfer of the raw number to the g. The final program and the testing part evaluates the raw number which reduces the further calculation and time of the evaluation by the microcontroller.

The second function of the MPU-6050 is the ability to measure the rotational velocity or rate of change of the angular position over time. The idea of the gyroscope is the same as the accelerometer. The information of the rotation is sent on request to the microcontroller in form of the 16-bit data register with a range from (0 <-> 65535)

with the sensitivity selection of ranges (±250, ±500, ±1000, or ±2000 deg/sec). The information of the angle is calculated by the final program.

The main function of the CCS811 is the measuring of the carbon dioxide and metal oxide levels. The sensor can read and evaluate the data on request automatically using internal logic. The sensor transmits the data in binary form which can be directly converted to the decimal without any calculation and the measuring of the CO2 has only 2 % tolerance.

The first part of the program is the main initialization which is done only once with the first power-up by the input voltage. The microcontroller begins the communication with the MPU-6050 and the CCS811 by using the Wire.begin(); which is used for the mentioned I2C communicating interface. The manufacturer decided, that two independent accelerometers can be connected by the I2C communication interface which means that the program must select between two available addresses each for one possible device. These addresses are fixed in the chip. The default address for a single accelerometer is 0x68 [41] and the unique address for the air sensor is 0x5A the initialization is shown in the following figure.
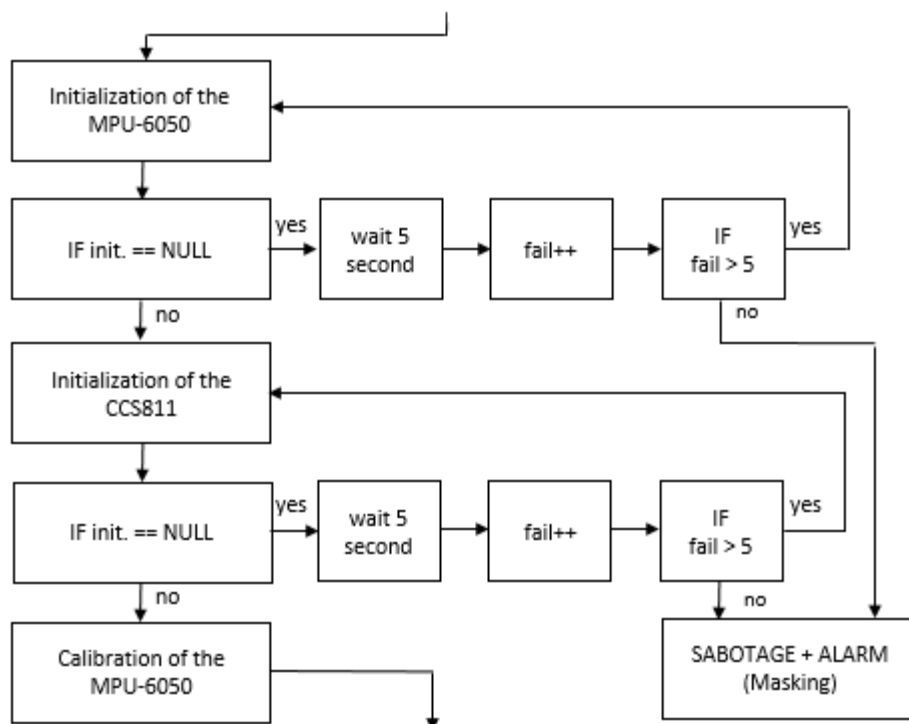
Fig. 26 Initialization part of the final program

The initialization part also consists of the calibration process which must be done before the operation. However, for maximal reliability, the calibration is done each time with the initialization. This function only takes several seconds which meets the time requirements. The sabotage and alarm signal is triggered when the initialization of one of the devices fails 5-times. The initialization part can be called from any part of the code.

The next part of the program is focused on getting and processing the raw data from the MPU-6050 by the microcontroller. This part is done only by the one request for the acceleration and rotation which is also done by the I2C interface using the special command for getting the data. The incoming data must be further processed by shifting the 8-bit data stream. The final 16-bit information is finally stored in the variable for further evaluation.

The main program is based on the comparison of the levels which were made by the testing in this chapter. The raw data directly contains the information of the acceleration and concentration of the CO2 where any conversion is not needed. Every raw number is converted to an absolute value and store in an array with the size of 10 integers. With every new execution of the main loop, the function which returns the average value of the array is executed. However, the critical part of the evaluation is the know-how of this thesis, and only the flow chart is listed in the following figure.
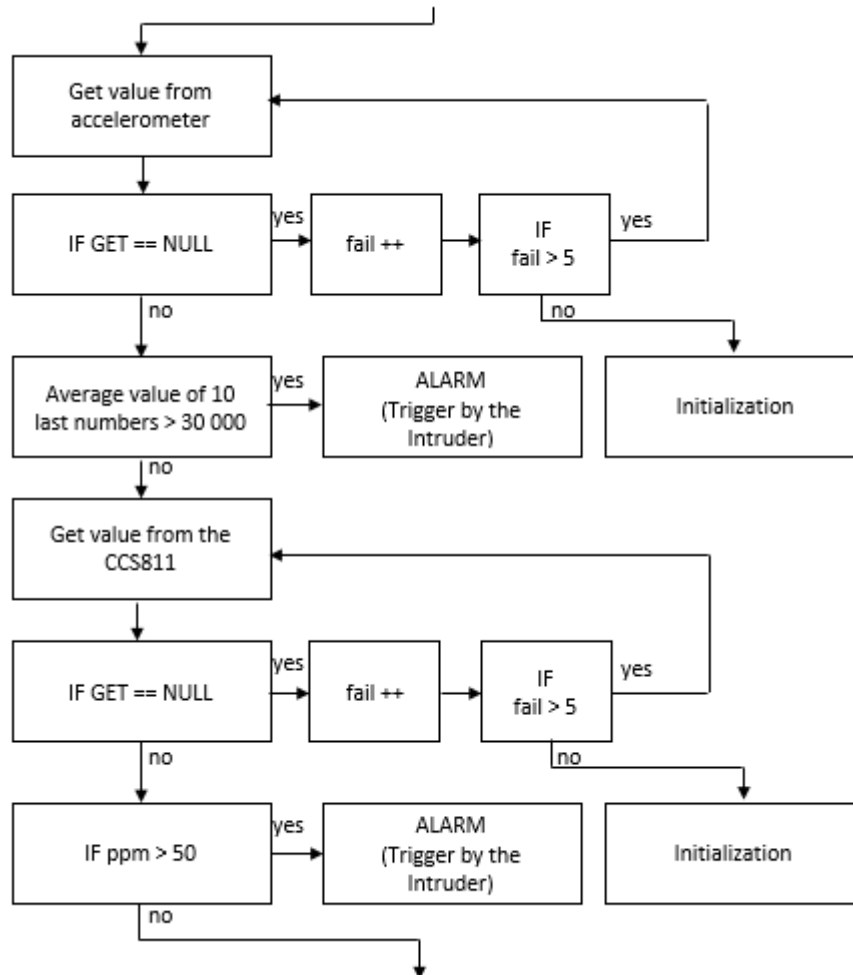
Fig. 27 Initialization part of the main program

The information about the acceleration, rotation, and CO2 concentration is requested by the microcontroller and the values are stored in the variable. The first section is focused on the valid data received from the devices. The function can detect if the data is corrupted or incomplete. The new request for the data to the current device

is done when the data are corrupted or incomplete. This section is also protected against the cycling of the program. When the requesting function is interrupted 5 times the initialization is triggered. The second part is focused on the evaluation of the calculated value. Based on the previous testing, the threshold value for the impact force was created. When this value is exceeded, the detector triggers the alarm by the intruder.

The last part of the program is focused on other additional situations requested by the standardization namely the power consumptions and sabotage triggering. The same situation based on the rotation is created in the program which simulates the window open The flowchart of the complementary parts is listed in the following figure.
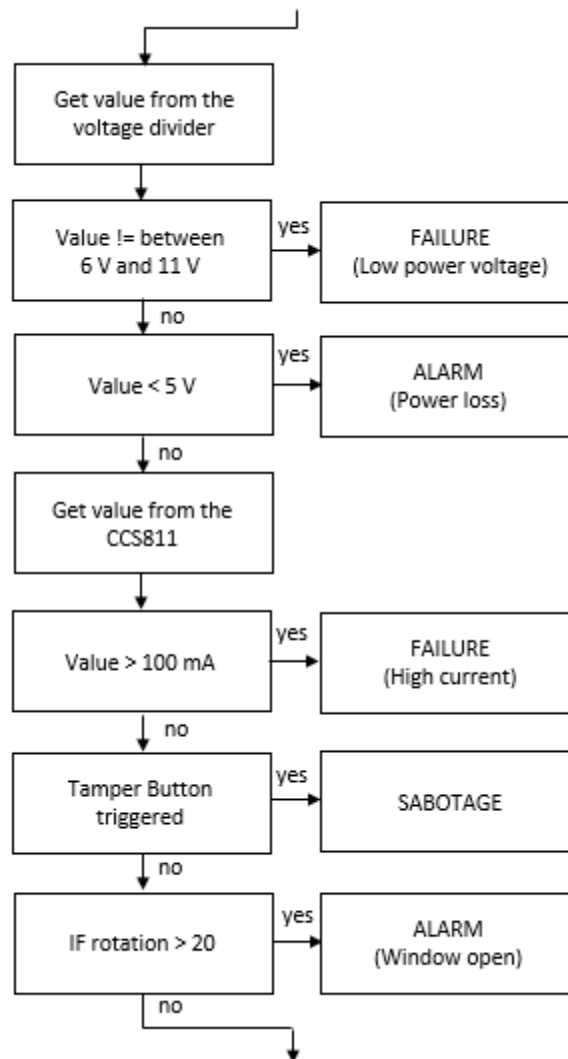
Fig. 28 Complementary part of the final program

As mentioned before, the information from the voltage divider and the ACS712 is analog which means that this information could be measured by the analog inputs integrated inside of the microcontroller ATmega8. The value from the voltage divider is only compared to normal expected values and the deviation is evaluated as Low power voltage or Power loss. The same approach is done by the chip ACS712. The

last part is focused on the tamper trigger. When the micro button is released the detector triggers the sabotage. Each fundamental part of the final program was fragmented and described in detail by using the flowchart diagrams. The final flowchart design of the whole program can be found in the following figure.
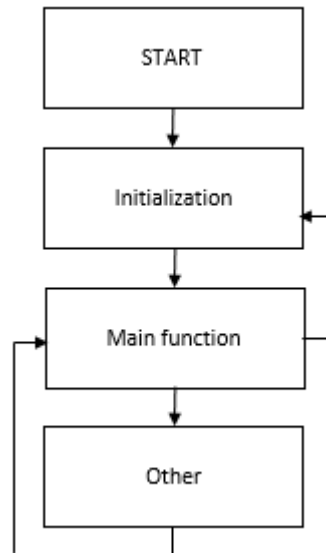
Fig. 29 Final diagram of the program

The program is periodically requesting and evaluating data from the connected devices. The final testing proved, that the detectors can proceed 512 cycles in one second which is enough to achieve standardization given by the standardization. When the main part fails to evaluate the data, the whole program is interrupted and the initialization part is executed.

As mentioned before, the program itself must be written strictly to the expected bus interface which is used by the CIE. However, this thesis brings the concept without any connection to the real CIE. The Complete program needs to have the part which communicates with the CIE. This part is very easy to implement in the final program. Due to the know-how of this thesis, no specific part of the code is shown in this paper.

10. Technical Documentation of the Prototype

Every alarm detector must pass the testing according to the standardization before it gets to the market. The main standardization for the glass-break detector is CSN EN 50131-2-7-2 Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive) and the prototype must pass several tests listed in the standardization. Even the prototype of a new product must have the technical documentation which is critical for the testing. The certified testing facility is testing all aspects of the detector according to the technical documentation. According to this requirement, technical documentation must be created.

The technical documentation is also very important for the people which install the detector in the proper place. In the case of this prototype, the responsible person for installing the active part of the detectors into the glass panel is from the company which manufactures the multi-chamber glass panels. This person does not need any special education, information, or any certificate in technical security, the person only has to follow the installation manual enclosed to the detector which can be found on the following page.

Tab. 14 Technical specification of the glass-break prototype

| Power	from the CIE bus 12 V (7… 15 V)
Current consumption	50 mA (max. 100 mA)
Detection distance	Max. 60cm
Minimum window glass size	60 x 60 cm
Maximal window glass size	120 x 120 cm
Stabilization time after switching on	max. 120 s
Operational environment EN 50131-1	II. Indoor general
Operating temperature range	-10 to +40 °C

The fundamental preview of the designed glass-break detector can be found on the following page. The information and design were taken from other manufacturers that are producing certified alarm glass-break detectors on the market. The next page contains the technical documentation of the detector.

General Information

The Glass-break detector flu senses the vibration of breaking a plate, tempered, laminated, wired, coated, and sealed insulating glass.

The detector requires an interface based on RS-485, which provides the communication interface with the Control and Indication Equipment via a serial interface.

The detector can be used only on one glass panel at once. For more windows, each window must have its detector installed.

Glass Type/Thickness

The minimum size for all types is 60 cm square; glass must be framed in the wall or mounted in a barrier at least 120 cm wide.

Type of the Glass	Thickness	Deviation
Normal	6 mm	± 2 mm
Coated	6 mm	± 3 mm
Hardened	6 mm	± 2 mm
Insulated	4 mm	± 2 mm
Wired	6 mm	± 2 mm

Tab. 1 Nominal Glass Thickness Chart

Coated glass with security films or foils up to 0.35mm thickness (including films for solar protection) may be used.

Installation

The installation can be done by uncertified personnel in the windows assembly line according to Fig. 3. The active part must be glued on the first glass panel in the multi-chamber window.

The glue must be used the same as for joining multiple glass panels together to form one window. Two parts of the detector are assembled by the serviceman during the installation.

Specifications

Power from the CIE bus 12 V (7 … 15 V)

Current consumption 50 mA (max. 100 mA)

Detection distance max. 60 cm

Minimum window glass size 60 x 60 cm

Maximal window glass size 120 x 120 cm

Stabilization time after switching on max. 120 s

Operational environment EN 50131-1II. Indoor general

Operating temperature range -10 to +40 °C

Design
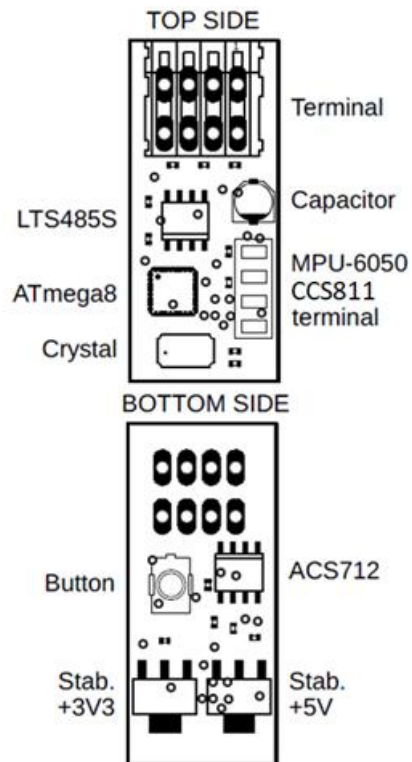
Fig. 1 Design of the detector

Connect detector using 18 to 22 AWG wire, with ends stripped approximately 6mm. Use the appropriate wiring method as shown in this diagram:
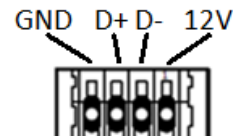

Fig. 2 Wiring Diagram

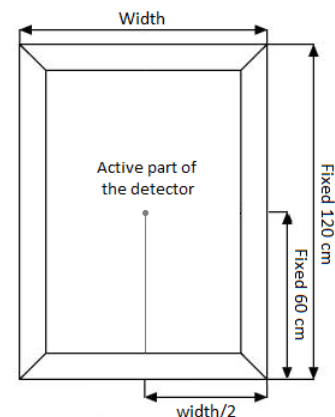## Location of the Sensor

Fig. 3 Location of the detector

11. Results and Discussion

As mentioned at the beginning of this thesis, the most critical layer of the security of life, health, and possession is the casing protection where the most vulnerable part is the glass panels. The state of the art showed that the concept of the main detector for windows is outdated and not reliable. This is caused by many false alarms, and by the construction of the multi-chamber windows. Moreover, the glass-break detectors in their present form do not achieve the highest security grade which can be a critical reason for improving the relevance and reliability of glass-break detectors. The last big issue is focused on the breaking glass itself which is not the most frequent element for the intruder. The more common element for the intrusion is the tearing of the window frame. According to this problem, the main goal of this thesis is to design the combined alarm detector focused on windows.

The combined Glass-break detector

The main focus of this thesis is to design a prototype of the alarm detector which meets the requirements given by the standardization. This design was consulted, created, and tested according to the standardization CSN EN 50131-2-7-2 which is focused on the main function of the alarm detector. Moreover, the problem with the intrusion by tearing of the window was also considered by implementing the gyroscope to the final design.

Preparation of the certified testing

As mentioned before, each of the alarm devices which comes to the market must be tested in certificated laboratories according to the current standardization. This part is focused on the prototype of the alarm detector and to prove the flawless and reliable functionality that must be tested in the certificated laboratory according to the standardization. However, this procedure is quite expensive, and when the model failed in the testing procedure it must be redesigned and tested again. All procedures, limits, and methods needed for the testing are listed in the standardization and the un-certified testing can be done before the certified testing. According to this request, the testing room was built at the Faculty of Applied Informatics of the Tomas Bata University in Zlin.

Testing according to the standardization

The final testing procedure according to the standardization can be divided into four separate parts, each focused on different topics. The first part is focused on function requirements listed in *9.2 Functional Requirements (pp. 44)* which is further divided into Event processing, Signal or message generating, and Time requirements. The final detector can process all events listed in *Tab. 1 Signal processing according to*

Security Grade (pp. 31), which means that the detector can be used in maximal security grade IV. The requirements listed in *Tab. 2 Signal or message generating based on the event (pp. 32)* can also be achieved in the presented design. The second part described in *9.3 Detection (pp. 47)* is focused on the main detection of the detector. This part is divided into three independent tests each dealing with different influences. According to the standardization, all mentioned tests must be done to achieve the maximal security grade IV. The combination of the accelerometer MPU-6050 and the air quality sensor CCS811 integrated inside of the design provides the possibility to detect all scenarios. It means that the design can be used in the highest security grade from the detection point as well. The third one is focused on the false alarm events which must be ignored by the detector. This part is described in chapter *9.4 False Alarm (pp. 50)* where all scenarios must be done regardless of the security grade. The last parts presented in chapters *9.5 Sabotage (pp. 54)* and *9.6 Electrical Requirements (pp. 55)* dealing with the additional testing focused on the sabotage and the electrical requirements. Each part has its requirements based on the security grade. All requirements are implemented to the final design to achieve the maximal security grade IV.

The main part of the program for the main detection is completed. However, the final program must be extended by communication with the CIE. As mentioned before, the manufacturers have a private communication interface that is not public, and this part must be programmed by the final manufacturer.

Result of the final testing

The most critical part of the standardization of the testing is the reaction to the impact or situation which must trigger the alarm. This part is called the *9.3 Detection (pp. 47)*. According to the mentioned information of the numbers and cost of the windows, the final testing was done only once for just one type of glass panel. This testing was successful and the detector was able to trigger the alarm. The concept can success also on different types of glass panels and it can pass the certified testing according to the standardization.

The second part *9.4 False Alarm (pp. 50)* focused on the false alarm which must not trigger the alarm, was completely done according to the standardization. This was possible due to the non-destructible approach 20 times for each of the glass types. All five scenarios were tested and all outputs met the standardization.

The result of the testing does not have any output numbers or waveforms. The output of the testing was only the message triggered by the detector in form of the text of the event. The final statement of the concept is that the designed prototype meets the standardization and it can be sent for certified testing.

12. Benefices for Science and Practice

This chapter summarizes the benefits of this thesis for science and practice. All benefits are created and described also in the previous chapters and briefly summarized in this chapter.

Integration of the glass-break detector into the window

The active and the passive part of the glass-break detector is integrated to the windows for two reasons. The first one is the placement of the active part of the detector placed on the first glass panel in the multi-chamber window, where it can collect the vibrations caused by the impact. The second is that the possible intruder is not able to reach the glass-break detector without breaking through the window and the detector is hidden inside of the frame. The main part of the detector which is responsible for the evaluation can be easily replaced.

Evaluating the current position of the window frame

The detector can process the incoming signal from the gyroscope and it can evaluate the opened and closed window or ventilation. This information can be used in non-alarm applications like heating or arming the alarm system and it can be also used for triggering the alarm by the window opening or tearing.

Detection of the potential intruder before breaking through the window

Standard detectors triggering the alarm after the intruder break into the protected place or area. Namely, the acoustic glass-break detector triggering the alarm after the glass is broken. Using the security foil and the new design of the detector is possible to detect an intruder even before it gets through the glass. The first big impact by some weapon is detected by the detector and the intruder must get through the firm foil which can take up to several minutes. This time is beneficial for the security departure to the protected place.

The certified product which can be placed on the market

The whole design was made according to the standardization aiming for the certified testing and placing on the market. This thesis can be used as a guide for the successful application of the new design of the glass-break detector with many advantages and high reliability.

13. Conclusion

This thesis is focused on the casing layer of security which forms the main and the most important layer between life, health, possession, and the potential intruder. The most vulnerable part of the casing layer is the glass panel which is usually protected by the glass-break detectors. The publications and other information proved that the current design of these detectors is outdated and must be improved. According to this problem, the new concept of the combined detector is used for the protection of the glass planes.

The prototype of the detector is divided into two parts and each part is embedded into the window. The active part which is embedded into the multi-chamber glass panel is a flexible PCB with an accelerometer MPU-6050 for measuring the vibration and the air pollution sensor CCS811 for the measuring of the inner gas concentration. The evaluating part is composed of the microcontroller and additional parts that provide reliable communication via the RS-485 interface with the CIE. Both parts are described in detail in previous chapters with detailed schematics documentation.

The constructed detector can detect the force caused by the impact which can destroy the glass panel inside of the protected window. Moreover, the detector can evaluate the change of the glass integrity which is the critical parameter for the maximal Security grade. The additional function can also detect the change of the position caused by the opening of the window.

The prototype was designed according to the current standardization CSN EN 50131-2-7-2, moreover, the design also meets the highest security grade which is not possible for common glass-break detectors currently on the market. The created design was manufactured and tested according to the mentioned standardization to prove flawless and reliable function in real-time. The final testing proved, that the designed detector achieved all requirements for achieving the highest security grade given by the standardization. The outcome of this thesis is also the technical documentation for the further certified testing by the authorized standardization office. After a certified testing procedure, the design of the detector can be placed on the market.

References

[1] Landa, Jiang, Chu Jun, and Miao Jun. Implementation of a Remote Real-Time Surveillance Security System for Intruder Detection. 2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 2017. doi:10.1109/icmtma.2017.0032.

[2] HART, J. – HARTOVÁ, V. Development of new testers to improve quality for data transmissions in intrusion and hold-up alarm systems. In 15th International Scientific Conference on Engineering for Rural Development 25.03.2016, Jelgava; Latvia. Latvia University of Agriculture: Latvia University of Agriculture, 2016. s. 523-528.

[3] Urbančoková, Hana, Jan Valouch and Milan Adámek. Testing of an Intrusion and Hold-up Systems for Electromagnetic Susceptibility - EFT/B. International Journal of Circuits, Systems, and Signal Processing. 2015, vol. 9, s. 40-46. ISSN 1998-4464.

[4] BOROŠ, Martin, Martin HALAJ and Andrej VEĽAS. Possibility of Transmitting Alarm Messages Over the Radio Network to the Monitoring and Alarm Receiving Centre. CBU International Conference Proceedings. 2018, 1013-1016. ISSN 1805-9961. DOI: 10.12955/cbup.v6.1287

[5] Valouch, Jan. The Proposal of Methodology for Evaluating the Effectiveness of Alarm Systems. Applied Mechanics and Materials 736 (2015): 183-88. doi:10.4028/www.scientific. net/amm. 736.183.

[6] STAUFFER, Todd a Peter CLARKE. Using alarms as a layer of protection. Process Safety Progress. 2016, 35(1), 76-83. ISSN 10668527. DOI: 10.1002/prs.11739

[7] Hanacek, Adam and Martin Sysel. The Methods of Testing and Possibility to Overcome the Protection against Sabotage of Analog Intrusion Alarm Systems. Intelligent Systems in Cybernetics and Automation Theory, 2015, p. 19-128. DOI: 10.1007/978-3-319-18503-3_12. ISBN 978-3-319-18502-6.

[8] HONEY, G. Intruder alarms. 3rd ed. Burlington, MA: Newnes, 2007. ISBN 9780750681674.

[9] CSN EN 50131-1 ed. 2 (334591) Alarm systems - Intrusion and hold-up alarm systems - Part 1: System requirements. Prague: The Office for Standards, Metrology, and Testing, 2013.

[10] Odolnost výplní otvorů proti vloupání – základní principy zabezpečení | iMaterialy. Portál pro odborníky ve stavebnictví – projektanty, stavaře z praxe, architekty i řemeslníky | iMaterialy [online]. Copyright ©. Available: https://www.imaterialy.cz/rubriky/materialy/odolnost-vyplni-otvoru-proti-vloupani-zakladni-principy-zabezpeceni_45579.html

[11] Hart, Jan and Veronika Hartova. Testing of combined space detectors in intrusion and hold-up alarm systems. In: 2018-05-23, s. DOI: 10.22616/ERDev2018.17.N279.

[12] Hart, Jan, Veronika Hartova, and Jiri Bradna. Intrusion and Hold -Up Alarm Systems and Their Reliability Glass Break Detection. 6th International Conference on Trends in Agricultural Engineering 7-9 September 2016, Prague, Czech Republic. 2016, 171-174.

[13] Nídlová, V and J Hart. Reliability of detection of Glass Break in Intrusion and Hold-Up Alarm Systems. HU, Jong, ed. Advanced Materials and Structural Engineering. CRC Press, 2016, 2016-02-03, s. 445-448. DOI: 10.1201/b20958-95. ISBN 978-1-138-02786-2.

[14] Lojka, Martin, Matúš Pleva, Eva Kiktová, Jozef Juhár, and Anton Čižmár. Efficient acoustic detector of gunshots and glass breaking. Multimedia Tools and Applications. 2016, 75(17), 10441-10469. DOI: 10.1007/s11042-015-2903-z. ISSN 1380-7501

[15] Valenzise, G., L. Gerosa, M. Tagliasacchi, F. Antonacci, and A. Sarti. Scream and Gunshot Detection and Localization for Audio-surveillance Systems. In: 2007 IEEE Conference on Advanced Video and Signal Based Surveillance. IEEE, 2007, p. 21-26. DOI: 10.1109/AVSS.2007.4425280. ISBN 978-1-4244-1695-0.

[16] Gestner, Brian, Jason Tanner, and David Anderson. Glass Break Detector Analog Front-End Using Novel Classifier Circuit. In: 2007 IEEE International Symposium on Circuits and Systems. IEEE, 2007, s. 3586-3589. DOI: 10.1109/ISCAS.2007.378528. ISBN 1-4244-0920-9.

[17] Bemke, Ireneusz and Romuald Zielonko. Improvement of Glass Break Acoustic Signal Detection Via Application of Wavelet Packet Decomposition. Metrology and Measurement Systems. 2008, 15(4), 513-526.

[18] CSN EN 50131-2-7-1 (334591) Alarm systems - Intrusion and hold-up systems - Part 2-7-1: Intrusion detectors - Glass break detectors (acoustic). Prague: The Office for Standards, Metrology, and Testing, 2013.

[19] ET AL., Naing. Glass breaks detection system using deep auto-encoders with fuzzy rules induction algorithm. International Journal of ADVANCED AND APPLIED SCIENCES [online]. 2019, 6(2), 33-38 [cit. 2020-12-26]. ISSN 2313626X. doi:10.21833/ijaas.2019.02.006

[20] CONKA, David and Anton CIZMAR. Acoustic Events Processing with Deep Neural Network. In: 2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA) [online]. IEEE, 2019, 2019, s. 1-4. ISBN 978-1-5386-9322-3. doi:10.1109/RADIOELEK.2019.8733502

[21] CSN EN 50131-2-7-2 (334591) Alarm systems - Intrusion and hold-up systems - Part 2-7-2: Intrusion detectors - Glass break detectors (passive). Prague: The Office for Standards, Metrology, and Testing, 2013.

[22] BAGATURIA, Y, O BARUTH, H.B DREIS, et al. Studies of aging and HV break down problems during development and operation of MSGC and GEM detectors for the inner tracking system of HERA-B. Nuclear Instruments and Methods in Physics Research. 2002, 490(1-2), 223-242. ISSN 01689002. doi:10.1016/S0168-9002(02)01002-1

[23] CSN EN 50131-2-7-3 (334591) Alarm systems - Intrusion and hold-up systems - Part 2-7-3: Intrusion detectors - Glass break detectors (active). Prague: The Office for Standards, Metrology, and Testing, 2013.

[24] ZHANG, Dengzhuo, Jun LIU, Lan QIN, Jingcheng LIU a Min LI. Multiparameter Modeling of Piezoelectric Six-Degree-of-Freedom Accelerometer About Sensitivity Characteristics. IEEE Sensors Journal [online]. 2020, 20(13), 7129-7137 [cit. 2020-07-15]. DOI: 10.1109/JSEN.2020.2966013. ISSN 1530-437X.

[25] DELFAN HEMMATI, Kamran a Bahram AZIZOLLAH GANJI. A new structure and modeling of a three-axis MEMS capacitive accelerometer with high dynamic range and sensitivity. Microsystem Technologies [online]. [cit. 2020-07-15]. DOI: 10.1007/s00542-020-04932-4. ISSN 0946-7076.

[26] DWIVEDI, Apoorva a Gargi KHANNA. A microelectromechanical system (MEMS) capacitive accelerometer-based microphone with enhanced sensitivity for fully implantable hearing aid: a novel analytical approach. Biomedical Engineering / Biomedizinische Technik [online]. 2020, 65(6), 735-746 [cit. 2020-12-26]. ISSN 1862-278X. Dostupné z: doi:10.1515/bmt-2017-0183

[27] CHAVAN, Somnath K. Impact Correlation with Accelerometer in Home Appliance Industry. Journal of Failure Analysis and Prevention [online]. [cit. 2020-07-15]. DOI: 10.1007/s11668-020-00906-w. ISSN 1547-7029

[28] RUDYK, Andrii V., Andriy O. SEMENOV, Natalia KRYVINSKA, Olena O. SEMENOVA, Volodymyr P. KVASNIKOV a Andrii P. SAFONYK. Strapdown Inertial Navigation Systems for Positioning Mobile Robots—MEMS Gyroscopes Random Errors Analysis Using Allan Variance Method. Sensors. 2020, 20(17). ISSN 1424-8220. doi:10.3390/s20174841

[29] GHOSH, Arijit, Hiranmoy ROY a Soumyadip DHAR. Arduino Quadcopter. In: 2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) [online]. IEEE, 2018, 2018, s. 280-283 [cit. 2020-12-26]. ISBN 978-1-5386-7638-7. Dostupné z: doi:10.1109/ICRCICN.2018.8718695

[30] HASSAN, Arfa, Zhenbao LIU, S M SHEHZEB ABBAS, Yongbo LI, Lina WANG, Xin LIU a Peng ZHAO. Statistical scheme for fault detection using Arduino and MPU 6050. In: 2019 Prognostics and System Health Management Conference (PHM-Qingdao). IEEE, 2019, 2019, s. 1-7. ISBN 978-1-7281-0861-2. doi:10.1109/PHM-Qingdao46334.2019.8942922

[31] ROS, IMU, and an Arduino: How to read IMU sensor output and send it to ROS - Atadiat. [online]. Copyright © Copyright 2021, All Rights Reserved. Available: https://atadiat.com/en/e-ros-imu-and-arduino-how-to-send-to-ros/

[32] ZHANG, He, Ravi SRINIVASAN a Vikram GANESAN. Low Cost, Multi-Pollutant Sensing System Using Raspberry Pi for Indoor Air Quality Monitoring. Sustainability [online]. 2021, 13(1) [cit. 2021-01-27]. ISSN 2071-1050. DOI:10.3390/su13010370

[33] LYU, Yuan-Li, Wen-Jie LIU, Hua SU a Xuan WU. Numerical analysis on the advantages of evacuated gap insulation of vacuum-water flow window in building energy saving under various climates. Energy [online]. 2019, 175, 353-364 [cit. 2020-12-26]. ISSN 03605442. Dostupné z: doi:10.1016/j.energy.2019.03.101

[34] LI, Chunying a Haida TANG. Evaluation on year-round performance of double-circulation water-flow window. Renewable Energy [online]. 2020, 150, 176-190 [cit. 2020-12-26]. ISSN 09601481. Dostupné z: doi:10.1016/j.renene.2019.12.153

[35] NOVIANTO, Dwi, Ika SETIYOWATI a Erry PURNOMO. Design and calibration soil moisture sensor for rise seedling using Arduino nano as a controller [online]. In: 2019, s. 030010- [cit. 2020-12-26]. Dostupné z: doi:10.1063/1.5098185

[36] HALIM, Dareen K., Tang Chong MING, Ng Mow SONG a Dicky HARTONO. Arduino-based IDE for Embedded Multi-processor System-on-Chip. In: 2019 5th International Conference on New Media Studies (CONMEDIA) [online]. IEEE, 2019, 2019, s. 135-138 [cit. 2020-12-26]. ISBN 978-1-7281-0726-4. Dostupné z: doi:10.1109/CONMEDIA46929.2019.8981862

[37] CHIU, Yi, You-Zen CHEN, Chia-Chun HSIEH a Hao-Chiao HONG. A Wireless Gauge Pressure Sensor with Enhanced Sensitivity Fabricated by Flexible PCB Technology For Intracranial Pressure Sensing. In: 2019 IEEE SENSORS [online]. IEEE, 2019, 2019, s. 1-4 [cit. 2020-12-26]. ISBN 978-1-7281-1634-1. Dostupné z: doi:10.1109/SENSORS43011.2019.8956931

[38] Natesh, Aswin, Gandhi Rajan, Balasubramanian Thiagarajan and Vineeth Vijayaraghavan. Low-cost wireless intelligent two hand gesture recognition system. In: 2017 Annual IEEE International Systems Conference (SysCon). IEEE, 2017, p. 1-6. DOI: 10.1109/SYSCON.2017.7934745. ISBN 978-1-5090-4623-2.

[39] Pospisilik, Martin, Tomas Smekal, Milan Adamek, Petr Neumann, and Tomas Dulik. Remote controlled gate controller using a GSM network and Arduino platform. MATEC Web of Conferences 76 (2016): 02036. doi:10.1051/matecconf/20167602036.

[40] Arduino accelerometer MPU-6050 - Stack Overflow. Stack Overflow - Where Developers Learn, Share, & Build Careers. From: https://stackoverflow.com/questions/54599310/arduino-accelerometer-mpu-6050

[41] MuttipleMPU/MuttipleMPU.ino master Shuvashish Sarker / batikkrom.com GitLab. From: https://gitlab.com/shuvashish/batikkrom.com/blob/master/MuttipleMPU/MuttipleMPU.ino

List of Figures

List of Tables

Publication of the Author

KOVÁŘ, Stanislav, MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan. Electromagnetic Compatibility of Arduino Development Platform in Near and Far-Field. International Journal of Applied Engineering Research, 2017, roč. 12, č. 15, s. 5047-5052. ISSN 0973-4562.

KOVÁŘ, Stanislav, URBANČOKOVÁ, Hana, VALOUCH, Jan, ADÁMEK, Milan, MACH, Václav. Helical Antenna Design for Image Transfer. International Journal of Applied Engineering Research, 2017, roč. 12, č. 14, s. 4741-4746. ISSN 0973-4562.

KOVÁŘ, Stanislav, VALOUCH, Jan, URBANČOKOVÁ, Hana, ADÁMEK, Milan, MACH, Václav. Simulation of Shielding Effectiveness of Materials using CST Studio. WSEAS Transactions on Communications, 2017, roč. 2017, č. 16, s. 131-136. ISSN 1109-2742.

MACH, Václav, ADÁMEK, Milan. Advanced Hardware Protection of Metallic Loops. In MATEC Web of Conferences. Les Ulis : EDP Sciences, 2017, s. nestrankovano. ISSN 2261-236X.

MACH, Václav. Hybrid Extension for Advanced Technology Zone. In MATEC Web of Conferences. Les Ulis : EDP Sciences, 2017, s. nestrankovano. ISSN 2261-236X.

MACH, Václav, ADÁMEK, Milan. Zvýšení Efektivity Poplachových Smyček. In Bezpečnostní technologie, systémy a management 2017: Sborník příspěvků 6. mezinárodní konference. Zlín : Univerzita Tomáše Bati ve Zlíně, 2017, s. nestrankovano. ISBN 978-80-7454-696-9.

KOVÁŘ, Stanislav, MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan. Design of shielding enclosure to protect security devices. In Progress in Electromagnetics Research Symposium. Cambridge: The Electromagnetics Academy, 2018, s. 2424-2429. ISSN 15599450. ISBN 978-153861211-8.

KOVÁŘ, Stanislav, MARTÍNEK, Tomáš, MACH, Václav, POSPÍŠILÍK, Martin. Composite material to protect security devices against electromagnetic interference. In Progress in Electromagnetics Research Symposium. Cambridge: The Electromagnetics Academy, 2018, s. 2445-2450. ISSN 15599450. ISBN 978-153861211-8.

MACH, Václav, KOVÁŘ, Stanislav, VALOUCH, Jan, ADÁMEK, Milan, RUI, Silva. Threshold levels of electromagnetic susceptibility for unarmed air vehicles. In Progress in Electromagnetics Research Symposium. Cambridge: The Electromagnetics Academy, 2018, s. 2483-2488. ISSN 15599450. ISBN 978-153861211-8.

MACH, Václav, KOVÁŘ, Stanislav, VALOUCH, Jan, ADÁMEK, Milan, RUI, Silva. Electromagnetic compatibility of Raspberry Pi development platform in near and far-field. In Progress in Electromagnetics Research Symposium. Cambridge: The Electromagnetics Academy, 2018, s. 2466-2472. ISSN 15599450. ISBN 978-153861211-8.

MACH, Václav, KOVÁŘ, Stanislav, RUI, Silva, VALOUCH, Jan, ADÁMEK, Milan. A Safety of the International Mobile Equipment Identity. Transylvanian Review of Administrative Sciences, 2018, roč. 26, č. 25, s. 124-131. ISSN 1842-2845.

MACH, Václav, KOVÁŘ, Stanislav, VALOUCH, Jan, ADÁMEK, Milan. Brushless DC Motor Control on Arduino Platform. Przeglad Elektrotechniczny, 2018, roč. 94, č. 11, s. 105 -107. ISSN 0033-2097.

MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan. A design of integrated alarm system for modern households. In MATEC Web of Conferences. Les Ulis : EDP Sciences, 2018, s. nestrankovano. ISSN 2261-236X.

MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan. Glass-break detector using accelerometer. In MATEC Web of Conferences. Les Ulis : EDP Sciences, 2018, s. nestrankovano. ISSN 2261-236X.

MACH, Václav, ADÁMEK, Milan, VALOUCH, Jan, MUŠÁLEK, Miroslav. Limitation of the Advanced Technology Zone. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vienna : DAAAM International Vienna, 2018, s. 719-724. ISSN 1726-9679. ISBN 978-3-902734-20-4.

MACH, Václav, ADÁMEK, Milan, VALOUCH, Jan, TOMÁŠEK, Pavel. Software Extension for Advanced Technology Zone. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2018, s. 725-730. ISSN 17269679.

ADÁMEK, Milan, MACH, Václav, NEUMANN, Petr. The possibilities of using drones in the 3D object modelling field. In MATEC Web of Conferences. Les Ulis: EDP Sciences, 2018, s. nestrankovano. ISSN 2261-236X.

ADÁMEK, Milan, MATÝSEK, Miroslav, MACH, Václav, NEUMANN, Petr, POSPÍŠILÍK, Martin. A monitoring network system and its practical demonstration on a model technological process. WSEAS Transactions on Systems and Control, 2018, roč. 2018, č. 13, s. 520-528. ISSN 1991-8763.

BLAHOVÁ, Marta, MACH, Václav, ZIMEK, Ondřej, ADÁMEK, Milan. Method of device diagnostics, operating status logging, and configuration changes. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, s. 1014-1018. ISSN 17269679.

BLAHOVÁ, Marta, MACH, Václav, PAVLÍK, Lukáš, FICEK, Martin, HROMADA, Martin. THE INFORMATION SECURITY TO SOFTWARE OF CRISIS MANAGEMENT. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, s. 1019-1025. ISSN 17269679.

KOTKOVÁ, Barbora, HROMADA, Martin, MACH, Václav, BLAHOVÁ, Marta. DETECTION AND FACE RECOGNITION OF PEOPLE BY CAMERA FOR SECURITY APPLICATIONS. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, s. 610-614. ISSN 17269679.

MACH, Václav, VALOUCH, Jan, ŠEVČÍK, Jiří, RUI, Silva. Accelerometer-based glass-break detector for alarm applications. In MATEC Web of Conferences 292. Les Ulis : EDP Sciences, 2019, s. 1-5. ISSN 2261-236X.

MACH, Václav, VALOUCH, Jan, ADÁMEK, Milan, ŠEVČÍK, Jiří. Virtual reality – level of immersion within the crime investigation. In MATEC Web of Conferences 292. Les Ulis: EDP Sciences, 2019, s. 1-4. ISSN 2261-236X.

MACH, Václav, ADÁMEK, Milan, VALOUCH, Jan, ZIMEK, Ondřej, BLAHOVÁ, Marta. Peripheral Component Interconnect Express Card for the Closed-Circuit Television Application. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, s. 605-609. ISSN 17269679.

POSPÍŠILÍK, Martin, DULÍK, Tomáš, NAVRÁTIL, Milan, MACH, Václav. Implementation of low pass filters with real opamps: Where is the limit?. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vídeň: Danube Adria Association for Automation and Manufacturing (DAAAM), 2019, s. 248-253. ISSN 17269679.

MACH, Václav, ADÁMEK, Milan, VALOUCH, Jan, BARČOVÁ, Karla. Control and indicating equipment communicating via the peripheral component interconnect express bus. Bulletin of Electrical Engineering and Informatics, 2020, roč. 9, č. 2, s. 729-738. ISSN 2089-3191.

DROFOVÁ, Irena, ADÁMEK, Milan, MACH, Václav. The 3D scanning image quality of the interior with the mirror surface. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vienna : DAAAM International Vienna, 2020, s. 826-830. ISSN 17269679. ISBN 978-390273429-7.

BLAHOVÁ, Marta, VALOUCH, Jan, MACH, Václav. PREDICTIVE CONTROL OF PROCESSES WITH UTILIZATION OF ARTIFICIAL INTELLIGENCE ELEMENTS. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vienna : DAAAM International Vienna, 2020, s. 1-6. ISSN 17269679. ISBN 978-390273429-7.

MACH, Václav, ADÁMEK, Milan, DROFOVÁ, Irena, BLAHOVÁ, Marta, VALOUCH, Jan. False Alarms of the Contact Glass-break Detectors Caused by the Multi-chamber Window. In Annals of DAAAM and Proceedings of the International DAAAM Symposium. Vienna : DAAAM International Vienna, 2020, s. 0431 - 0435. ISSN 17269679. ISBN 978-390273429-7.

Curriculum Vitae

Personal Information

Name	Václav Mach
Address	Bařinka 179, 76311 Zlín (Czech Republic)
Phone	(+420) 702 119 294
E-mail	v2mach@utb.cz
Date of birth	08/03/1991
Nationality	Czech

Education and Training

2006–2010 Graduation Certificate in Electrical Engineering
Střední Průmyslová Škola Polytechnická - COP Zlín, Zlín (Czech Republic)

2010–2014 Bachelor's degree in Engineering Informatics
Univerzita Tomáše Bati ve Zlíně, Zlín (Czech Republic)

08/2014–05/2015 Erasmus Exchange
Vaasan Yliopisto, Vaasa (Finland)

2014–2016 Master's degree in Engineering Informatics
Univerzita Tomáše Bati ve Zlíně, Zlín (Czech Republic)

2016–Present Doctoral degree in Engineering Informatics
Univerzita Tomáše Bati ve Zlíně, Zlín (Czech Republic)

07/2017–09/2017 Erasmus Exchange
Polytechnic Institute of Beja, Beja (Portugal)

06/2019–09/2019 Erasmus Exchange
Polytechnic Institute of Beja, Beja (Portugal)

Work Experience

05/2017–Present Research Project Worker
Univerzita Tomáše Bati ve Zlíně, Zlín (Česká republika)
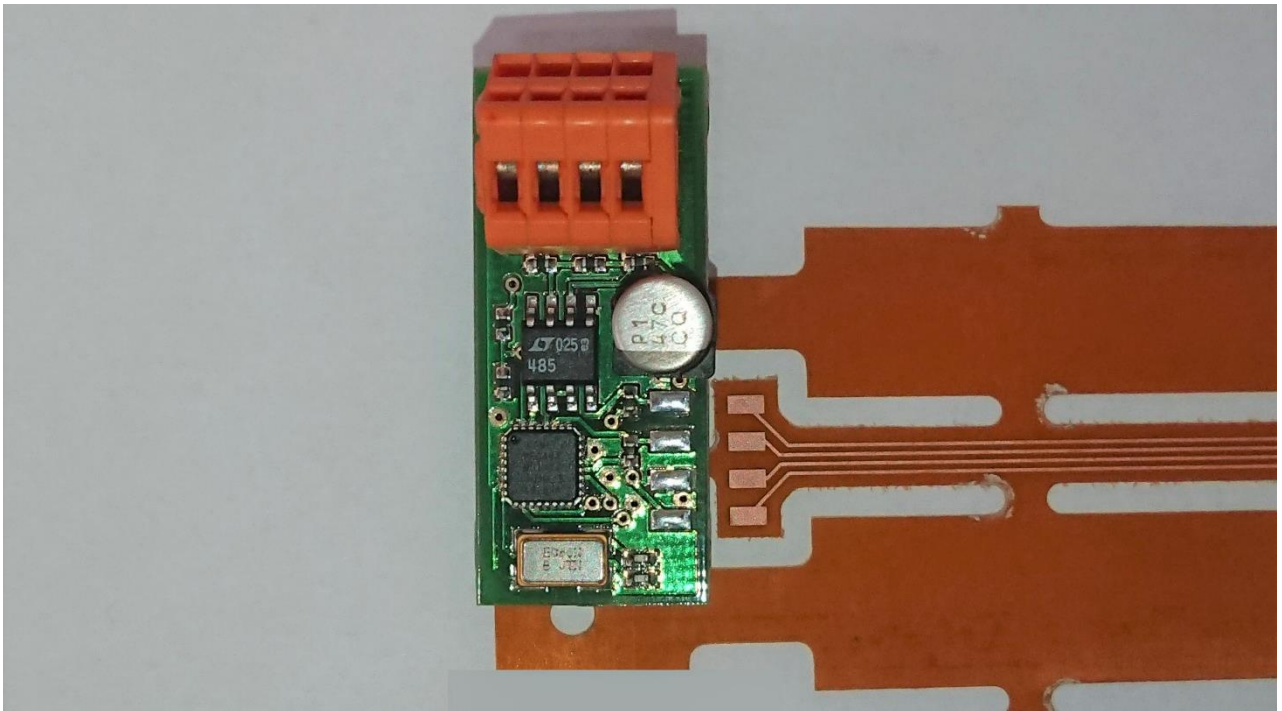
List of Appendices

Appendix 1: Photo of the Evaluating part of the Detector

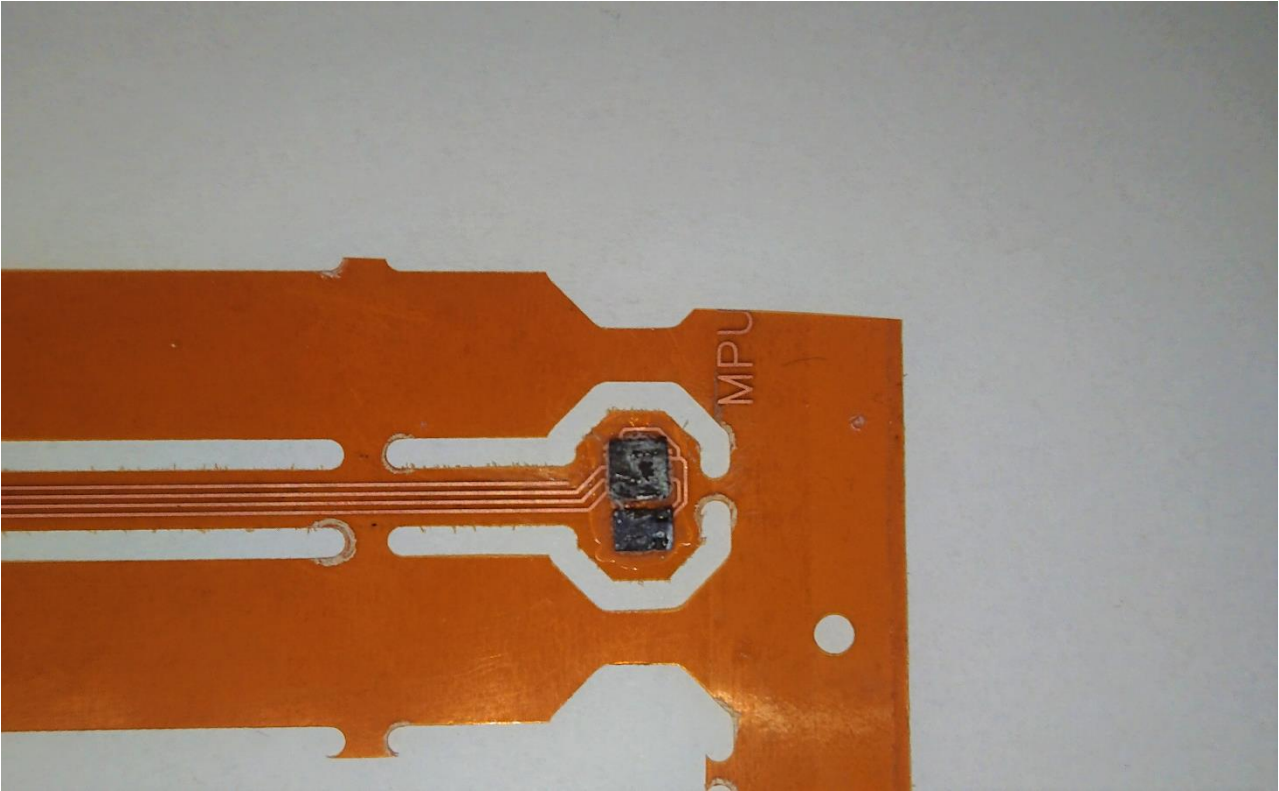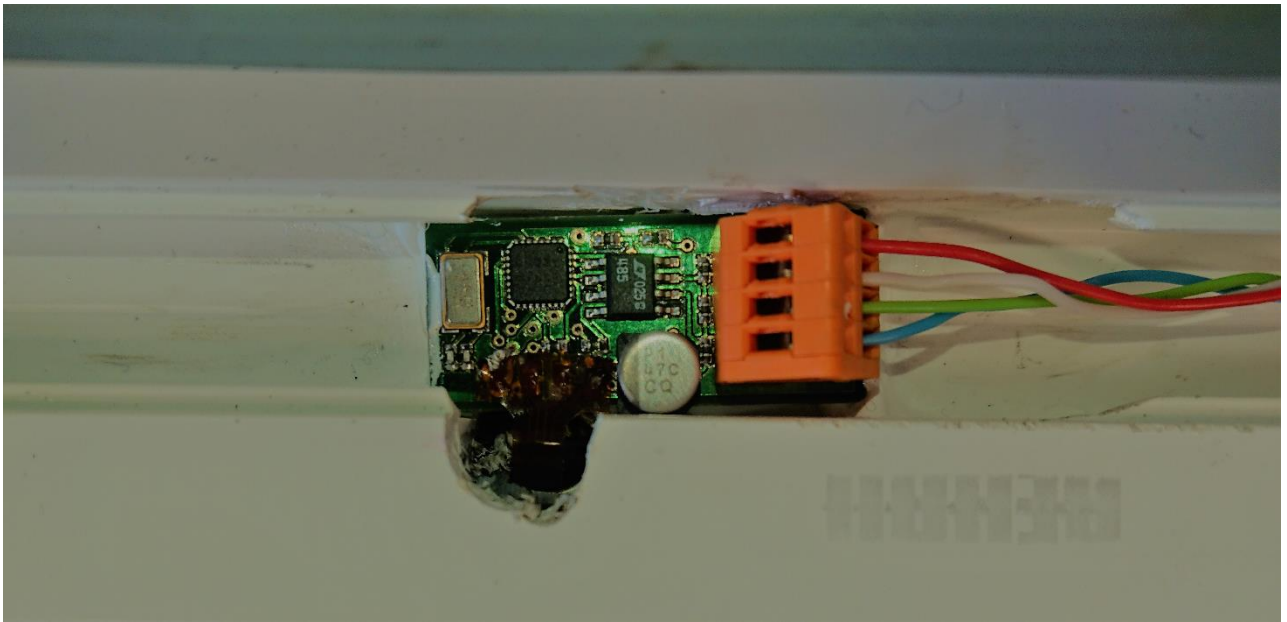Appendix 2: Photo of the Active part of the Detector

Appendix 3: Photo of the Detector together

Appendix 4: Photo of the Detector embedded inside of the multi-chamber windows

Appendix 1: Photo of the Evaluating part of the Detector

Appendix 2: Photo of the Active part of the Detector

Appendix 3: Photo of the Detector together

Appendix 4: Photo of the Detector embedded inside of the multi-chamber windows
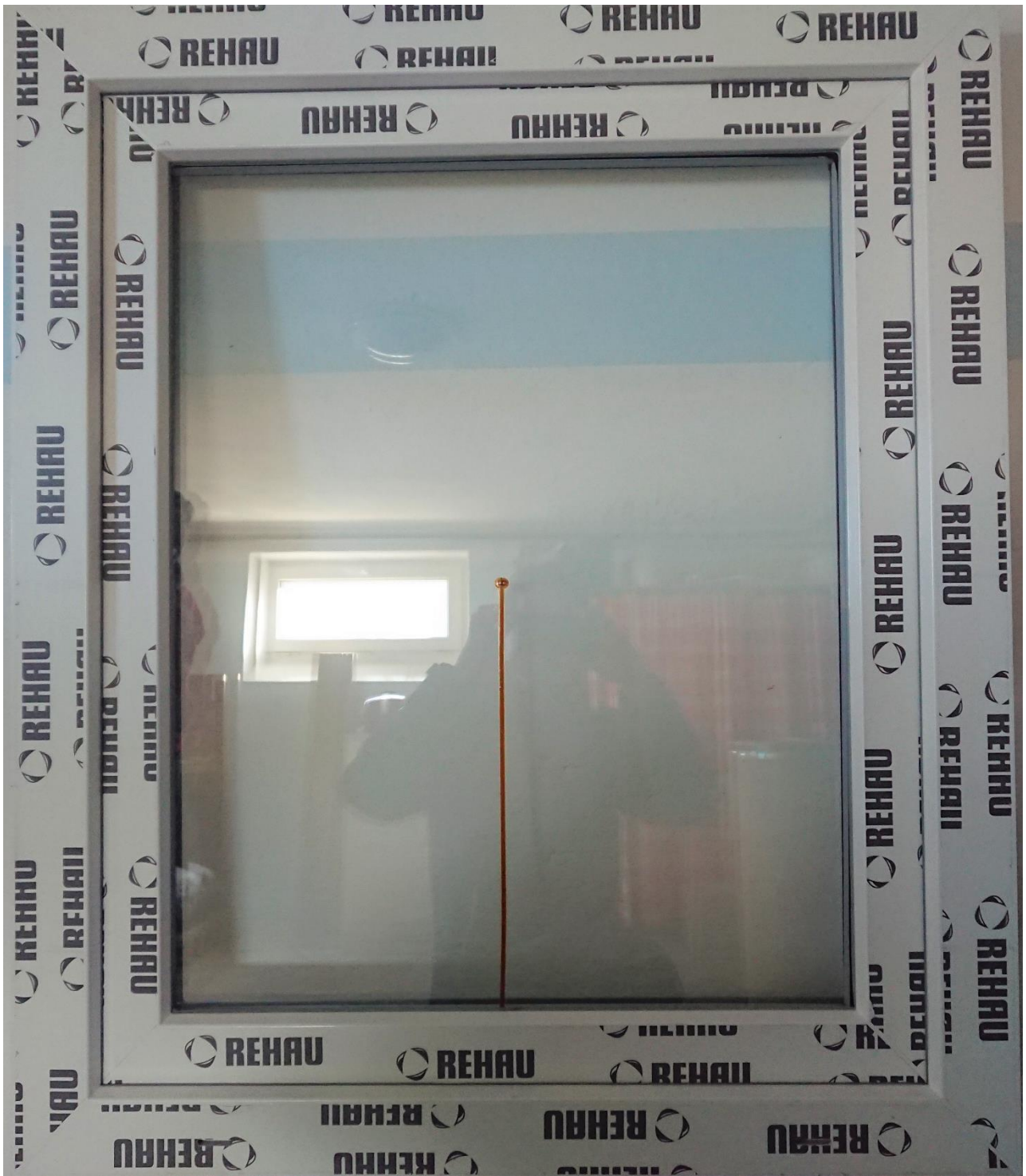
Václav Mach

Modernization of alarm detector used for the protection of glass panels

Modernizace poplachového detektoru
určeného pro ochranu skleněných ploch

Doctoral thesis

Tomas Bata University in Zlín,

nám. T. G. Masaryka 5555, 760 01 Zlín, the Czech Republic