Reliable Presence and Intrusion Detection with Collaborative Sensor Modules in Electronic Property Protection Systems

Bertalan Beszédes
Óbuda University, Alba Regia Technical Faculty,
Székesfehérvár, Hungary
beszedes.bertalan@amk.uni-obuda.hu

***Abstract* — This article deals with components (that effectuate the electronic protection) of property protection systems. Within this, mostly with to delineate the electronic outdoor protection, the intrusion detection system and some possible additional functions of the access control system. The solutions presented here are aimed to keep the cost low from the viewpoint of hardware requirements, together with to take advantage of the software opportunities.**

Keywords— presence detection, intrusion detection, collaborative sensors, security systems, reliable electronics, radar sensor, ultrasonic sensor, piezoelectric sensor, MEMS sensor, vibration sensor

I. Introduction

The task of the electronic protection is to detect intrusion and intrusion intention, in addition to send a notice to the security service members. As a matter of fact, the attack against property is avertable if the security service members can arrive to the exact venue and respond appropriately. [1]

In this system time is a critical factor. If the security service members can not arrive to the venue and take action on the matter in time – during the unlawful intrusion and departure, the intruder might escape with the acquired goods. The electronical system is able to denote the intrusion, before the intruder would be get into the protected building, the protected part of the building - thus increasing the time to react. In this case, an essential component of the system, depending on the value to be protected, is the appropriate level of mechanical protection designed to prevent intrusion and extend the time to invade.

II. Structure of Electronic Safety Systems

The electronic outdoors protection and intruder signal systems consists of a central unit, at least one sensor and one or more intervener and/or signal unit, depend on structure.

The central unit’s main task is to control the alarm system, to maintain the communication between several units, to interpret the incoming data, and to control the intervener units. The task of the outdoor protection systems is to perceive the intrusion to a protected area. The intervener unit’s responsibility is to act against the intruder, and the signal unit’s is to notify the human security.

A. Communication between devices

The communication between system components can happen on cable or on wireless connection. These devices might be disturbed, jammed or harmed with special tools, so it is subservient to protect them with shielding and optical isolation. Wires can pick up electrical noises, and they might deliver these disturbances to different units. It is expedient to use shielded, or double-shielded wires, and to assemble them in closed pipe networks. For such designs, a major requirement for the pipe connections is to make distinguished galvanic contact between the pipe sections, and the proper damping ability against electromagnetic waves. The extensive metal network should be connected to ground for interference- and life protection reasons. This setup will raise the costs of material and labor, so it is only recommended in justifiable cases.

The wireless connection has reduced expenses because less wiring is needed – especially in afterward installations -, but wireless detectors have higher prices, compared to wired detectors with similar parameters. The optimal solution in most cases is a hybrid system. In case of wireless systems, the signals of these units can be jammed by intruders, which means lower security levels. To eliminate this, there is the opportunity to detect the signals going through the wire system or the incoming electromagnetic signals with an additional detector. In case the signal interference exceeds a specified level, the sub-system signals the center, which recognizes it as a sabotage [2].

It is also subservient to query the operability of the center with an external server. If the center does not respond, or responds with an error message, the server notifies the security service members. The intruders may have the opportunity to infiltrate to the communication networks, so they can falsify or mask the messaging. If they are able to achieve this, it is recommended to set up a physically guarded, galvanically isolated, writable data storage in the center, which allows only one-way data flow. The center archives the incoming and outgoing data – into this storage device. If the data on this storage device and on the external server does not match, sabotage happened [2]. The security service member’s task is to compare these data.

Confirmation of the security service members can be traditionally done by computer network devices or by a GSM network. There is also an alternative channel that has not been used yet to transfer small amount of data.

Narrow Band-IoT is a standardized, LTE infrastructure that is a mobile technology for transferring small data volumes. It uses the existing mobile network to ensure good coverage, licensed (1-2 € per year per device), so the provider guarantees minimal bandwidth and access to the network. It is convenient to simultaneously use multiple channels when communicating with the security members.

The central unit also contains a battery based backup power source. It is also possible to install solutions that are used in off-grid power supplies [3]. It is important that the system is also designed to overcome such attacks, for example, jamming through interferences, over-voltage sensing and disturbing through solar cell's wires. A redundant power supply system can also be installed [4]. This solution also dramatically increases installation costs.

B. Outdoor protection and intrusion detection systems

To detect intrusion and to track the intruder's activities, protection circles should be created. These can be provided by means of outdoor protection, surface protection or shell protection, indoor protection and object protection. [1]

It is also possible to install video surveillance systems beside the commonly used passages, magnetic field sensors, infrared devices, microwave devices, passive infrared sensors and vibration sensors for movement and/or presence detection.

The aim is to provide cost-effective additional features [5], so in the following low-cost radar sensors, ultrasonic distance, and vibration sensors will be negotiated.

III. Simultaneously Usable Sensor Modules

A. Radar sensors

The radar sensors consist of a transmitter and a receiver unit, the block diagram of their construction is shown in Fig. 1. Using them, information can be obtained by processing an object-reflecting signal. Exploiting the Doppler effect [6] these sensors can be used not only to measure the distance from the sensor, but also the velocity of the object can be determined from the change in the frequency of the reflected wave - typically nx10Hz (Fig. 2). (This speed data is correct from the point of view of the sensor.) These sensors can be placed in a bonding box covered with plaster or wallpaper behind wood, plastic or plasterboard overlay, because they can detect the presence through all the general building materials except the glass.

The various types of the cost-effective additional modules for civilian alarm systems are shown in Figure 3. The main properties are summarized in Table 1. The left-hand type – based on the experiments – is only suitable for presence detection and distance measurement. The other two types can also be used to measure speed.

The presented radar sensors can be used in the field of outdoor protection, for example: building approaching, passing next to a building or column, and door approaching. Moreover they can also be used as tools for space protection, for example: advancement on the corridor, detection of an indoor approach.

B. Ultrasonic distance sensors

The principle of ultrasonic distance sensors is similar to microwave radar sensors. In this case, a transmitter and a receiver module are also required for detection. The signal from the transmitter reflects to the receiver from a subject – within the measuring range. The distance between the object and the sensor can be estimated from the time difference between the signal output and the signal reception.

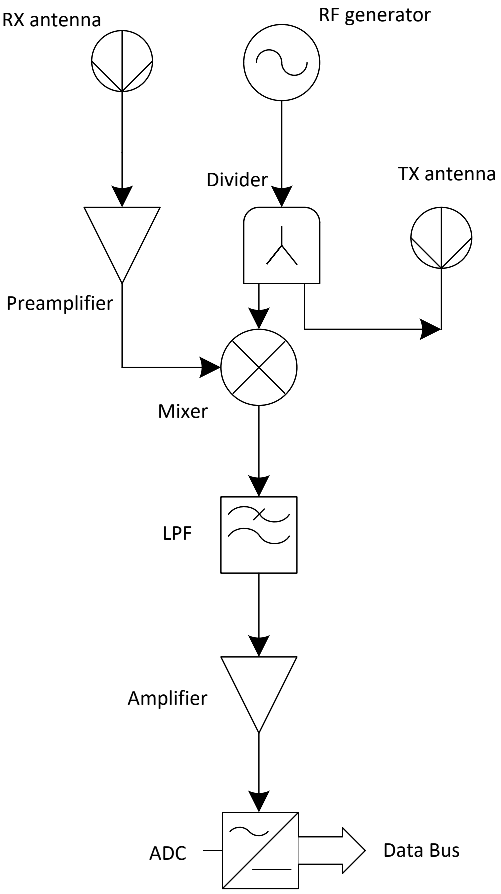

Figure 1. Architecture of the radar sensor

The propagation speed of sound in air depends on temperature and humidity [7]. Even without measuring these

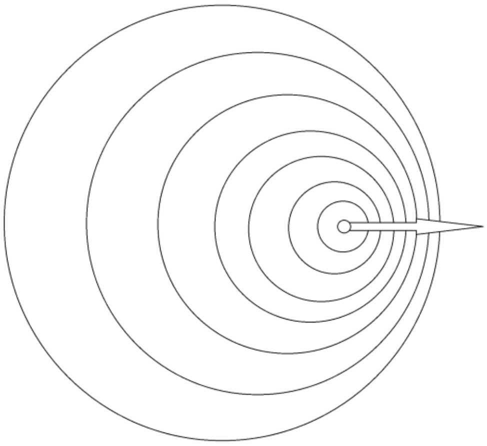

Figure 2. Doppler-effect

parameters, it is well applicable for sensing the presence and estimating distance [8]. For accurate distance measurement, it is necessary to examine the airspace properties [9]. Temperature and humidity can be measured using inexpensive sensors. The corrected distance can be defined by the following expression:

$$d = \left(v_0 + 0,606T + 0,0124H\right)\frac{t}{2}, \qquad (1)$$

where v0 = 331.39m/s, the ultrasound velocity in dry air, at 0 °C, T is the temperature in degrees of Celsius and H is the humidity.

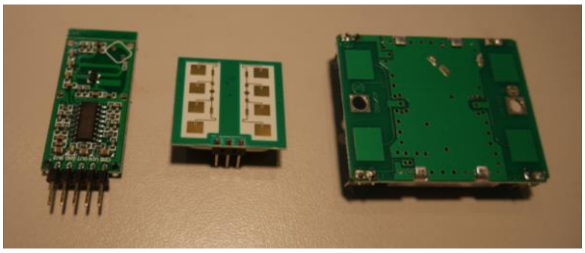

Figure 3. Different type of radar sensors: RCWL-0516, PD-V11, HB100

TABLE 1. COMPARISON OF RADAR SENSOR PROPERTIES

	RCWL-0516	PD-V11	HB100
Detection Angle Range	360°	180°	180°
Operating frequency	3.181 GHz	24.125 GHz	10.525 GHz

It is important to note that ultrasonic distance sensors can be used indoors only. Air movement can easily divert ultrasonic waves, avoiding the receiver module, and therefore the measurement may be defective.

In contrast, the transmitter and receiver units in one module can be used for space protection as well as physically separated transmitter and receiver units. In a later case, it is possible to secure a variable space, for movement. When arming the alarm system - in a static area position - sound waves come from the transmitter and these return to the receiver with the reflections, already attenuatedly. The incoming sample is stored by the subsystem, comparing the samples received later. If the insured area has an object that changes space or shape, the attenuation of sound waves and reflections will change. The altered signal will be different from the reference signal, sampled at arming [10]. This starts a signal sending to the control panel which triggers an alarm. The permissible deviation from the current reference sample can be used to influence the sensitivity of the subsystem.

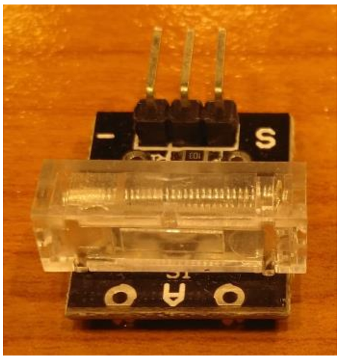

Figure 4. Vibration sensor module

It is possible to use the ultrasonic sensor for combined use with a radar sensor and a PIR sensor to provide more reliable space protection.

C. Vibration sensors

The following low-cost vibration sensors [11] can be used as shell protection tools (Fig. 4). The closing contact or the pattern of the vibration also has information content for the subsystem that controls it. Spring vibration sensors can be obtained with variable characteristics, depending on geometry and material properties. Sensor modules that are sensitive to lower or higher frequencies (depending on the design) can be selected, furthermore, the method of mounting – for example monitoring a door – also can influence its sensitivity.

D. Piezoelectric sensors

Piezoelectricity is a physical phenomenon where electric polarization (charge disconnection) is caused by mechanical force. Thus, the mechanical force – voltage conversion is feasible simply. This type of sensor reacts to higher frequency vibrations [12] with higher output voltage (Fig. 5). To highlight skin protection and object protection devices, from the wide range of using possibilities, these devices can be used well and cost-effectively to detect vibrations (Fig. 6).

E. MEMS sensors

Two and three axis accelerometers can also be purchased at low cost. Many sensors can also measure the

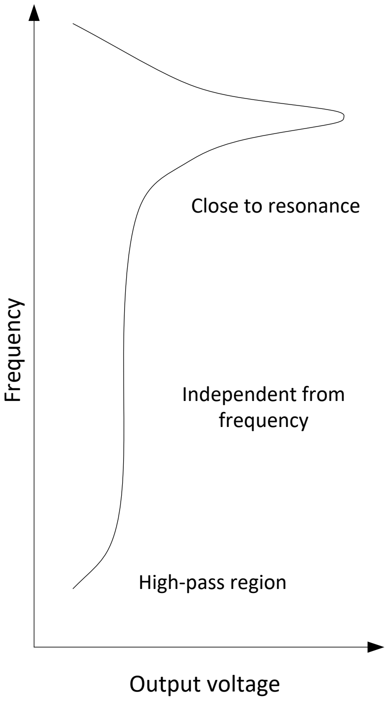

Figure 5. Voltage output of the piezoelectric sensor, as a function of the frequency of a constant amplitude mechanical vibration

rotation around the axes. The measured speed and acceleration values can be traced back to the principle of capacity measurement. This is possible in the sensors with the help of a mass, capable to move if it is affected by a force. They can be used well in the areas of object protection and shell protection, for example: movement -, glass break -, door opening -, drilling -, tensioning vibration detection. The subsystem, which processes the sensor signals [13], is able to distinguish a penetration pattern from, for example: the pattern of the door tricked into the neighboring apartment (Fig. 7) – based on the measured values [14]. A reference pattern from the X axis is shown on Fig. 8.

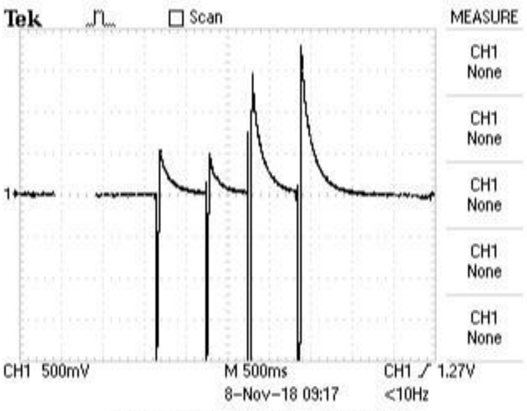

Figure 6. Voltage output of the piezoelectric sensor, as a function of time

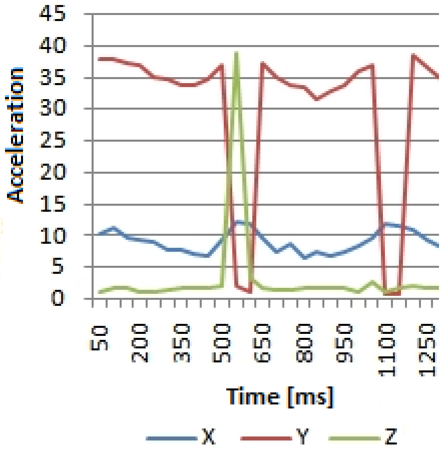

Figure 7. Door handle opening acceleration pattern

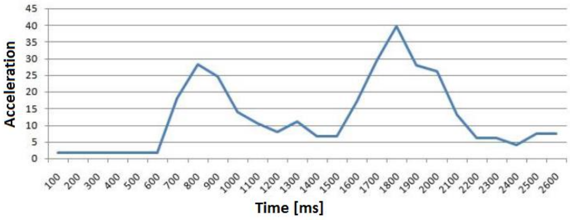

Figure 8. The reference pattern from the X axis

F. *Changing physical properties*

In case of shell protection, the interior space testing devices can be used as an additional sensor to detect intrusion detection. If measured values of air temperature, humidity, air pressure [15], carbon dioxide level and brightness change locally with a high slope, it can refer to a door or window opening. It is safer to evaluate if we know the outside air parameters. It is important to consider factors that disturb the evaluation when positioning the sensors. For example: the light and the heat effect of solar radiation entering the window, and the synchronization with the subsystem, for example: using automatic ventilation or heating / cooling devices – to prevent false alarms.

The well-prepared interior monitoring subsystem [16] get a signal about the operation of the devices which influence the indoor parameters. (These actuators are not parts of the alarm system.) Because of these external lines, the physical parameters based tamper-indication can be time-dependent and weighted. The above subsystem requires low financial resources, but can significantly increase the reliability of the electronic security system.

IV. Realization

Fig. 9 shows a system plan for the model of an alarm system to test the presented solutions. The central microcontroller controls the modules and units built around it. [17]

The sensors, in this embodiment, consist of a zone-doubled open wire detection and an ultrasonic distance measuring module, suitable for detecting presence.

The user interface is located on the keypad and contains the RFID module used to identify the user. In this configuration, the system is armed and deactivated via this interface. There are an LCD display and status LEDs for fast status display. In this configuration, the system is armed and deactivated via this interface. [18]

The sending and receiving of data to the outside world is possible through two channels: via wired ethernet and / or via GSM network.

The ultrasonic sensor used in the model is HC-SR04. The microcontroller built into the sensor, changes the sampling frequency depending on the measured distance. This is done to avoid the collision of sent and received signals. (Lower distance is paired higher frequency.)

The used Ethernet shield and RFID read/write module also communicates with the microcontroller via SPI bus. It was difficult to secure the long-term cooperation of the devices connected to the bus. (The Ethernet shield could not reconnect to the system every time it was detached from the bus.) That's why it had been made the devices detachable by a tri-state buffer.

The low number of microcontroller input pin also represented as a limit during development. [19] This and the problem of sharing the SPI bus [20] led to the development of an improved model, which contains two controllers, these are working on separate tasks, but communicate with each other [21]. The first controller is responsible for communicating with the outside world and the user. The newly-fitted, large pin number controller is responsible for querying sensors and detecting alarm and tampering events.

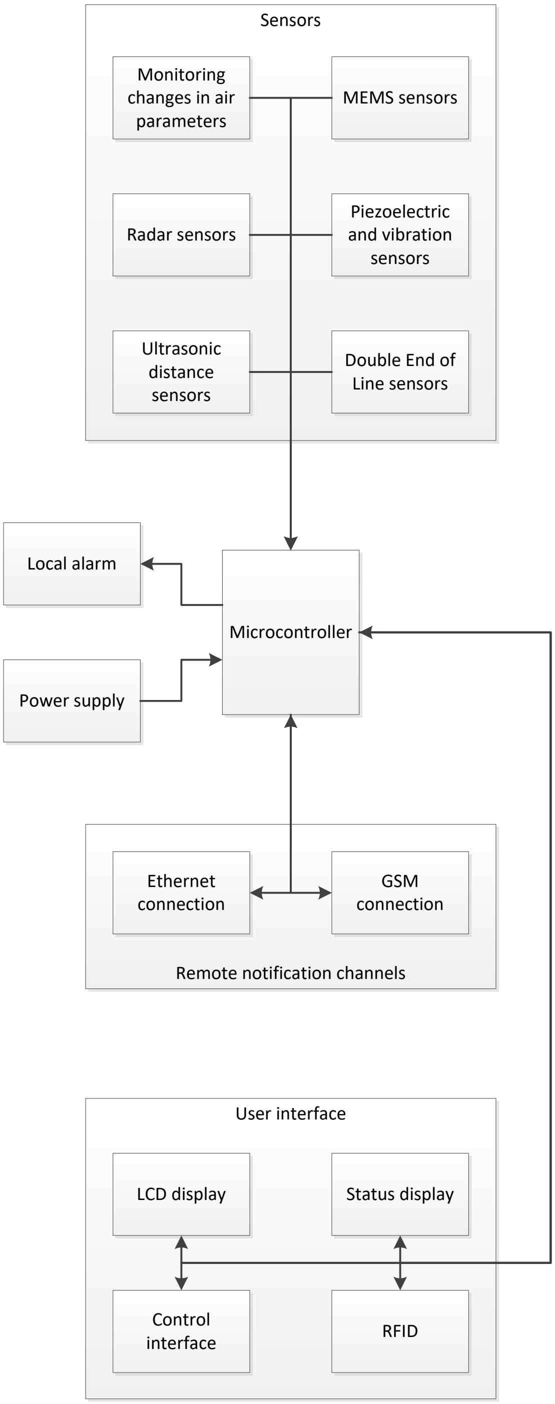

Figure 9. Architecture of the system

Conclusion

The reliability of individually developed systems is significantly higher, because the intruder is unable to try to bypass or break the system, apart from the installation site. (If the technical documentation is not available to the intruder.) The modular hardware and software architecture of the system also supports the further developments.

Besides the hardware and software solutions provided by the often used electronic property protection, it is possible to incorporate rarely used functions. In this case, the goal is to maintain a more complex system while keeping costs low and increasing the level of security. The examples presented above fulfill the above conditions, including electronic outdoor protection, intrusion detection system and access control system. The relevance of the recommended solutions - as hoped by the author - is also significant in civil and industrial areas.

Acknowledgment

The authors would like to thank all the faculty staff and member that provide help and assistance throughout the project completion.

References

[1] Berek Lajos. Biztonságtechnika. Budapest: Nemzeti Közszolgálati Egyetem. 2014. 48 p.

[2] György Györök, Bertalan Beszédes. Highly reliable data logging in embedded systems. In: Anikó Szakál, Iveta Zamecnikova. SAMI 2018: IEEE 16th World Symposium on Applied Machine Intelligence and Informatics : Dedicated to the Memory of Pioneer of Robotics Antal (Tony) K. Bejczy : proceedings. 237 p. Košice; Herlány, Szlovákia. 2018.02.07-2018.02.10. Seattle (WA): IEEE, 2018. pp. 49-54. ISBN:978-1-5386-4771-4

[3] Vass Attila, Berek Lajos. Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei. HADMÉRNÖK 24:(2) pp. 41-57. (2015)

[4] Györök György, Bertalan Beszedes. Fault tolerant power supply systems. In: Orosz Gábor Tamás. 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország. 2016.11.17. Budapest: Óbudai Egyetem. 2016. pp. 68-73.

[5] Gy, Györök ; M, Seebauer ; T, Orosz ; M, Makó ; A, Selmeci. Multiprocessor Application in Embedded Control System. In: Szakál, A (szerk.) 2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics, SISY 2012, Subotica, 2012, September, 20-22. Piscataway (NJ), Amerikai Egyesült Államok : IEEE, (2012) pp. 305-309. , 5 p.

[6] Horváth Csaba, Kocsis Bálint, Towards a Doppler effect based beamforming method for rotating coherent noise sources, In: 7th Berlin Beamforming Conference (BeBeC), (2018) Paper: BeBeC-2018-D27 , 14 p.

[7] FŐZŐ Ladislav, ANDOGA Rudolf, KOVÁCS Radovan. Thermodynamic cycle computation of a micro turbojet engine / Ladislav Fozo, Rudolf Andoga, Radovan Kovacs - 2016.In: CINTI 2016. - Danvers : IEEE, 2016 P. 000075-000079. - ISBN 978-1-5090-3909-8

[8] KOMJÁTY Maroš, FŐZŐ Ladislav, ANDOGA Rudolf. Experimental identification of a small turbojet engine with variable exhaust nozzle / Maroš Komjáty, Ladislav Főző, Rudolf Andoga - 2015. In: CINTI 2015. - Danvers : IEEE, 2015 P. 65-69. - ISBN 978-1-4673-8519-0

[9] ANDOGA Rudolf, FŐZŐ Ladislav, MADARÁSZ Ladislav, KAROĽ Tomáš. A Digital Diagnostic System for a Small Turbojet Engine / Rudolf Andoga ... [et al.] - 2013. In: Acta Polytechnica Hungarica. Vol. 10, no. 4 (2013), p. 45-58. - ISSN 1785-8860

[10] Gy, Györök. Self Organizing Analogue Circuit by Monte Carlo Method. In: A, Szakál (szerk.) LINDI 2007 - International Symposium on Logistics and Industrial Informatics 2007. Wildau, Németország : Institute of Electrical and Electronics Engineers (IEEE), (2007) pp. 1-4. , 4 p.

[11] Gy, Györök. The FPAA Realization of Analog Robust Electronic Circuit. In: Szakál, A (szerk.) IEEE 7th International Conference on Computational Cybernetics : ICCC 2009. Budapest, Magyarország : IEEE Hungary Section, (2009) pp. 1-5. Paper: 10 , 5 p.

[12] RP Buck, E Lindner, W Kutner, G Inzelt, Piezoelectric chemical sensors, PURE AND APPLIED CHEMISTRY 76 : 6 pp. 1139-1160. , 22 p. (2004)

[13] György, Györök. Continuous Operation Monitoring of Electronic Circuits with Embedded Microcontroller. In: Szakál, Anikó (szerk.) IEEE 18th International Symposium on Computational In-

telligence and Informatics (CINTI 2018) Budapest, Magyarország : IEEE Hungary Section, (2018) pp. 000155-000160. , 6 p.

[14] Michael A. Mahler, Qinghua Li, Ang Li. SecureHouse: A Home Security System Based on Smartphone Sensors. De-partment of Computer Science and Computer Engineering, University of Arkansas. IEEE International Conference on Pervasive Computing and Communications (PerCom). March 2017. https://www.researchgate.net/publication/313508127_SecureHouse_A_Home_Security_System_Based_on_Smartphone_Sensors.

[15] Muchen Wu, Parth H. Pathak, Prasant Mohapatra. Monitoring building door events using barometer sensor in smartphones. 2015 ACM International Joint Conference. September 2015. https://www.researchgate.net/publication/311490862_Monitoring_building_door_events_using_barometer_sensor_in_smartphones

[16] Györök, György. The Veterinary Horse Circuit for a Microcontroller Supervised System. In: Anikó, Szakál (szerk.) IEEE 16th International Symposium on Intelligent Systems and Informatics : SISY 2018. Budapest, Magyarország : IEEE Hungary Section, (2018) pp. 000227-000230. , 4 p.

[17] Dr. Györök György. Mikrokontrollerek hardver-hatékony alkalmazása. In: Nagy Rezső, Hajnal Éva. Garai Géza Sza-badegyetem II. Székesfehérvár: Óbudai Egyetem, 2015. pp. 5-15. ISBN:978-615-5460-62-3

[18] Györök György. Programozható analóg áramkörök mikrovezérlő környezetben. Óbudai Egyetem, ISBN 978 615 5018 97 8, Budapest, 2013.

[19] Gy. Györök. A-class amplifier with FPAA as a predictive supply voltage control. In: 9th International Symposium of Hungarian Researcherson Computational Intelligence and Informatics (CINTI2008). 2008. 361–368. p.

[20] B. Madoš, N. Ádám, J. Hurtuk, and M. Čopjak, “Brain-computer interface and Arduino microcontroller family software interconnection solution,” in Proc. of the 14th International Symposium on Applied Machine Intelligence and Informatics, Herlany, Slovakia, 2016, pp. 217–221.

[21] J. Hurtuk, A. Baláž, and N. Ádám, “Security sandbox based on RBAC model,” in Proc. of the 11th International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, 2016, pp. 75–80.