Agronomy Research **14**(2), 372–376, 2016

New security elements in biometric systems and systems I&HAS

J. Hart[1,*] and V. Hartová[2]

[1]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Technological Equipment of Buildings, Kamýcká 129, CZ165 21 Prague, Czech republic
[2]Czech University of Life Sciences Prague (CULS), Faculty of Engineering, Department of Vehicles and Ground Transport, Kamýcká 129, CZ165 21 Prague, Czech republic
[*]Correspondence: janhart77@gmail.com

Abstract. New security features or upgrades to existing features in biometric and security alarm systems and emergency formed at the Czech University of Life Sciences Prague, mainly due to the teaching of subjects with similar themes. When developing new technologies also help us grants, personal experience with a real installation, cooperation with manufacturers (or with distributors) security systems and a testing ground for current security features.

Key words: development, innovation, biometric systems, intrusion and hold-up alarm system, detector.

INTRODUCTION

In modern times, when the increasing crime rate led to the mass production of low-quality and cheap security systems, it is important to develop testers and measuring systems that help determine how are 'safe' and 'quality' for I&HAS (intrusion and hold-up systems). It is also very important to increase the already mentioned quality and safety of these systems (Damjanovski, 2005; Lukáš, 2011). It is for this reason that at the moment when there is a development of a new technology, so someone already working on sabotage techniques, how to sabotage this technology (Křeček, 2006).

This article is dedicated to representatives from among the testers, active protection and biometric systems, which were developed at CULS Prague. Engineered systems modify the existing solutions and provide insight on the issues solved entirely from a different perspective than it was before. Simultaneously, also these systems extend the full portfolio of security technology on the market today. It is important for the continuous development of protection and of various technological improvements get into a phase of stagnation. This would eventually led to a decline of the modern development of security technologies.

DEVELOPMENT IN I&HAS AND BIOMETRIC IDENTIFICATION SYSTEMS

Svoboda bypass tester established balancing resistors PUV 2011–24387 – see Fig. 1. It consists of a body tester (1), for which the two brought from the switchboard loop (3), potentiometer (4) and display (5). Using the display is possible to determine the current and the resistance according to the response panel (2) will assess how much resistance tolerated (Uhlář, 2005; Hart, 2010).

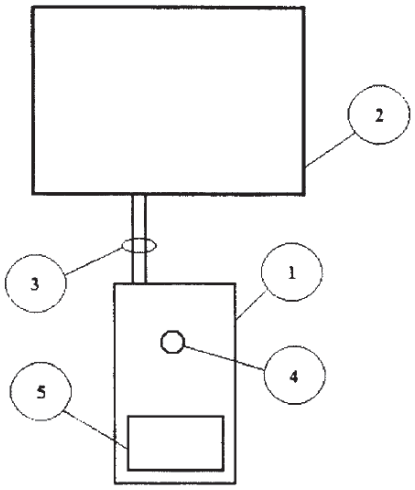

Figure 1. Svoboda tester.

Launcher defense active gas – technical solution concerns the design of active defense launchers gas used in electrical security systems such as active protection against intrusion guarded area. This design allows drain defensive gas from the gas chambers without the process of gradual release of gas (Damjanovski, 2005; Heřman, 2008).

At present, as the active protection of objects often uses smoke hoods that blurs guarded space innocuous, but completely opaque smoke. Furthermore, the use of high-frequency acoustic sirens and strobe lights (Křeček, 2006).

Launch Defence (see Fig. 2) use gas systems that emit gas gradually defensive. Their effect therefore occurs after a relatively long time. Their effectiveness is relatively small, and that because of their insufficient range defense gradually discharged gases (Lukáš, 2006; Heřman, 2008).

At the moment when the launcher defensive gas running, so the body (2) launchers, through the ejector (6) extends above the critical position. This position is bounded box (7) launcher. Fuse (3) remains under this threshold through spring (8) fixed and releases the lid (5) sinus pressure (1). They are due to pressure, rapidly opened and the entire contents of pressurized cavities launches into space. This effect gas infest the whole surrounding area, and potential intruders actively prevented from continuing his criminal activities. Re-gassing is possible by tightening screws (4) that fix the eyelid (Hart, 2010).

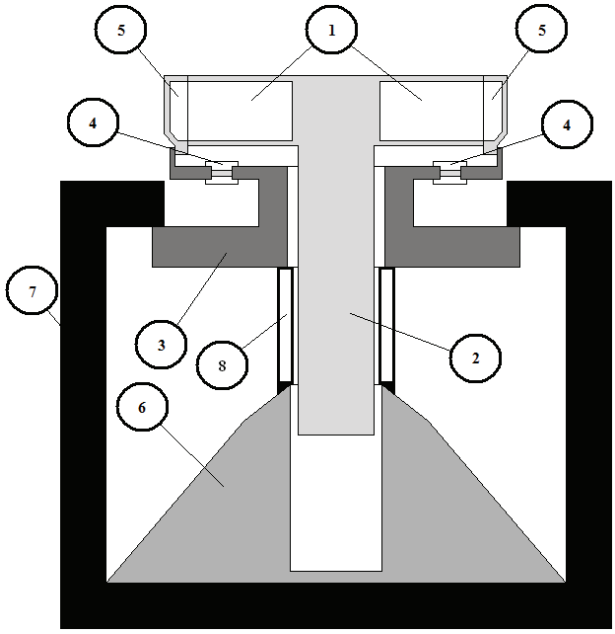

Figure 2. Launcher defense active gas.

The biometric authorization for the use of the service vehicle – this solution is used to prevent movement of company vehicles by unauthorized persons and records of persons who use a company vehicle.

At present, the control of the use of official vehicles only use log book and tachographs. In this way, however, can not fully determine what a person actually manages company vehicle. Company cars are then used for purposes other than those for which they are intended (Damjanovski, 2005).

The technical solution is to create a system for biometric authorization for the use of a company car, which is used to identify the person who wants to use a company vehicle. Biometric authentication for use company vehicles consists of the inlet system that is composed of a biometric fingerprint reader and a biometric identification system for taking 3D scan face.

The input system consists of a biometric fingerprint scanner is positioned to handle the vehicle. Used to identify the person, where there is a fingerprint images and the evaluation of the compliance of a fingerprint with a database of employees for subsequent unlocking of the vehicle. The next step is the identification of 3D face scanner, which is located in the rearview mirror and it is connected to the starter motor unit. After a person's entry into the vehicle and ensuring the safety belt when you press the start button starts the 3D scanner face. If thus the scanned facial scan and to compare with the database staff. In case of a tie the vehicle is started and all components shall be adjusted according to the parameters of the person (personal settings) (Heřman, 2008).

Fig. 3 shows the mirror (1) which are attached to the sensor (2) for 3D face scan and starter cancel the marked file (3).

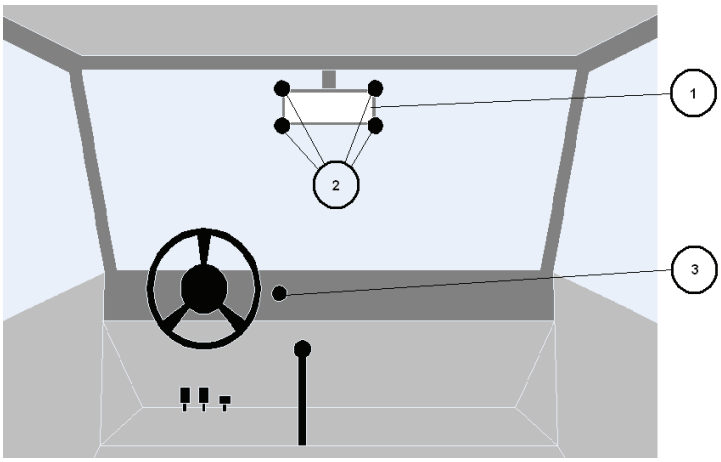

Figure 3. Rearview mirror with four sensors for 3D scan.

RESULTS AND DISCUSSION

At present tests were carried out only on Svoboda bypass tester. These tests demonstrated full functionality of this tester.

There are methods that allow bypass of the classical loop of security systems with end of line resistance, which reduces their safety. In this case it is important to know the boundary resistance that panel can accept . Svoboda bypass tester is designed so that the potentiometer change continuously resistance in this loop so it can deduct the value of resistance, which can accept. That the resistance is shown in Fig. 4, where it was selected for testing change continuously resistance 1,1 kΩ.

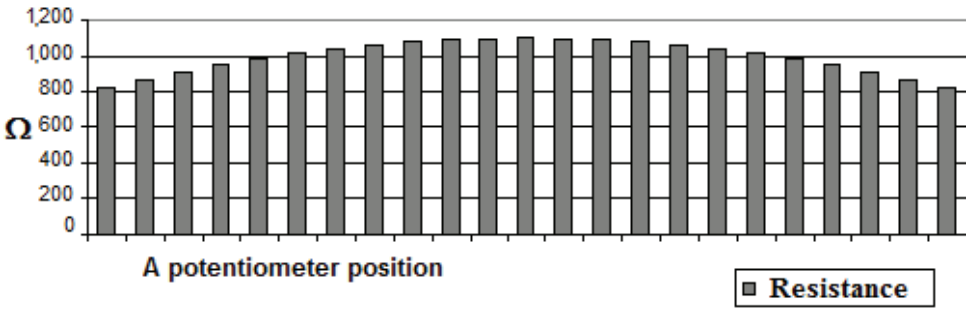

Figure 4. Course of the transition potentiometer.

In order to prevent the possibility of sabotage of security systems, it is very important to continually improve systems. Authors like Hanáček and Sysell in their article 'The Methods of Testing and Possibility to Overcome the Protection Against Sabotage of Analog Intrusion Alarm Systems' and 'Universal System Developed for

Usage in Analog Intrusion Alarm Systems' have the same views. And similarly to this problem is _ Urbančoková, Valouch and Adamek in their article 'Testing of an intrusion and hold-up systems for electromagnetic susceptibility – EFT / B'.

CONCLUSIONS

Testing and improvement of existing technologies is very important. Practical tests performed on loop switchboards bring insight into their functionality and practicality. Tests also showed that all types of loop switchboards can be better or worse sabotage. The tests can be used to draw principles for assault loop switchboards and thus develop and testers that help determine the quality and safety of the I&HAS.

Due to the continuous development of sabotage techniques is always important to continue to develop new and better detectors, modules, switchboards and all components of the systems I & HAS. It is important also to develop new testers that could test the existing schemes and thus determine their safety and quality.

The moment comes when any new or innovative element I&HAS (detector, data logger, the principle of evaluation, etc.) is already a way to circumvent it (sabotage). The biometric and security alarm and emergency systems is therefore very important to always act in the development of new technologies, principles, evaluation, protection detectors and innovation of existing elements I&HAS and biometrics. It is therefore, more difficult to attack as much as possible of the object and of course optimized price-performance ratio of the elements.

ACKNOWLEDGEMENTS. It is a project supported by the CULS IGA TF 2016 'The University Internal Grant Agency' (The transmission quality in wireless communications in the ISM band).

REFERENCES

Damjanovski, V. 2005. *CCTV, Second Edition: Networking and Digital Technology*. 2 edition. [s.l.]: Butterworth-Heinemann, 584 pp.

Hanacek, A. & Sysel, M. 2015. The Methods of Testing and Possibility to Overcome the Protection against Sabotage of Analog Intrusion Alarm Systems. *4th Computer Science On-line Conference (CSOC)*, Volume: 348, 119–128 p.

Hanacek, A. & Sysel, M. 2015. Universal System Developed for Usage in Analog Intrusion Alarm Systems. *4th Computer Science On-line Conference (CSOC)* **348**, 129–138 p.

Hart, J. 2010. *Analysis of security risks of building using system ESS*. Prague: CULS in Prague, 73 pp. (in Czech)

Heřman, J. 2008. *Electrical and telecommunication installations*. Praha: Verlag Dashöfer. (in Czech).

Křeček, S. 2006. *Handbook of security technology*. Blatná: Circetus. 313 pp. (in Czech).

Lukáš, L. 2011. *Security Technologies, Systems and Management I*. 1. vyd. Zlín: VeRBuM, 316 pp. (in Czech).

Uhlář, J. 2004. *Technical protection of objects, Part I, Mechanical barrier systems II*. Praha: PA ČR. 179 pp. (in Czech).

Uhlář, J. 2005. *Technical protection of objects, Part II, electrical security systems II*. Praha: PA ČR. 229 pp. (in Czech).

Urbancokova, H., Valouch, J. & Adamek, M. 2015. Testing of an intrusion and hold-up systems for electromagnetic susceptibility – EFT/B. *International Journal of Circuits, Systems and Signal Processing* **9**, 40–46.