INTRUSION AND HOLD-UP ALARM SYSTEMS AND THEIR RELIABILITY GLASS BREAK DETECTION

J. Hart, V. Hartová, J. Bradna

Faculty of Engineering, Czech University of Life Sciences Prague, Czech Republic

Abstract

This article is focused on the evaluation of the reliability of glass break detectors in intrusion and hold-up alarm systems (I&HAS). I&HAS serve primarily for protecting buildings against unlawful conduct of third parties, and can be used as monitoring and control systems. Several security risks may arise during the installation of intrusion and hold-up alarm systems, which impair the security of the entire building. The risks which occur due to poor installation or various sabotage techniques are always a serious danger for the guarded premises. In a time of increasing property crime, it is highly important for detectors to be able to achieve efficiency, reliability and faultlessness. In the case of proposal for placement of detectors it is naturally important determine position of detector, the type of detector, but also to guarantee their capability of detection for using. The practical tests conducted on GB detectors brought an insight into their functionality and usability in practice. If a saboteur is instructed about the operation of these detectors, then they can be overcome.

Key words: building, security, control, monitoring, installation, protect, error.

INTRODUCTION

Intrusion and hold-up alarm systems serve primarily for protecting buildings against unlawful conduct of third parties, and can be used as monitoring and control systems. They are therefore primarily a tool for ensuring a state of security. They operate in the material realm (physical protection of property, life and health) and in the emotional realm (providing a feeling of peace, safety and a certain security). As a result it is important for them not to malfunction and for them to be sufficiently resistant to attack (HANACEK, 2015). The critical point of intrusion and hold-up alarm systems is predominantly elements of the building envelope protection (KRECEK, 2006; STAFF, 1999). These elements are highly susceptible to poor installation, and as a result it is very important to pay attention to this problem. One of the most widely used types of detector is the GB detector (glass break), which ranks amongst active detectors. On average, of all the types of the building envelope detectors used, the largest numbers of false alarms occur on these detectors. This high error rate is primarily caused by incorrect installation (MAGNANI, 2016). Thus the aim of this study is to evaluate the reliability of glass break detectors in intrusion and hold-up alarm systems (I&HAS). I&HAS serve primarily for protecting buildings against unlawful conduct of third parties, and can be used as monitoring and control systems.

MATERIALS AND METHODS

Several security risks may arise during the installation of intrusion and hold-up alarm systems, which impair the security of the entire building. The risks which occur due to poor installation or various sabotage techniques are always a serious danger for the guarded premises (CUMMING, 1994; URBANCOKOVA, 2015). They may jeopardise the guarded property or even the lives of the people who the intrusion and hold-up alarm systems are intended to protect (HANACEK, 2015). Above all, however, they have an influence on determining the security risks of buildings.

Upon installation of GB detectors it is necessary to take into account a number of fundamental prerequisites. The first prerequisite is for the detector must be installed on the opposite side than the guarded glass surface. The second prerequisite is for the cabling not to be visibly installed. In addition the relevant norms must be adhered to upon implementation of the cable distribution mechanisms (CAPEL, 1999; PETRUZZELLIS, 1993; UHLAR, 2005). If the cable distribution mechanisms are installed in such a manner that enables access to them, it is possible to sabotage these systems and thus attack the entire installation of the intrusion and hold-up alarm systems.

If no end of line (EOL) resistor is connected to the switchboard loop upon installation of the detector, the system is more vulnerable and can easily be bypassed.

If a resistor is connected, bypassing is far more difficult than in the case of a simple loop (it is not possible to use simple short-circuiting). Upon sabotage it is necessary to create a dual bypass and use it to replace the original loop at a single moment (Fig. 1).

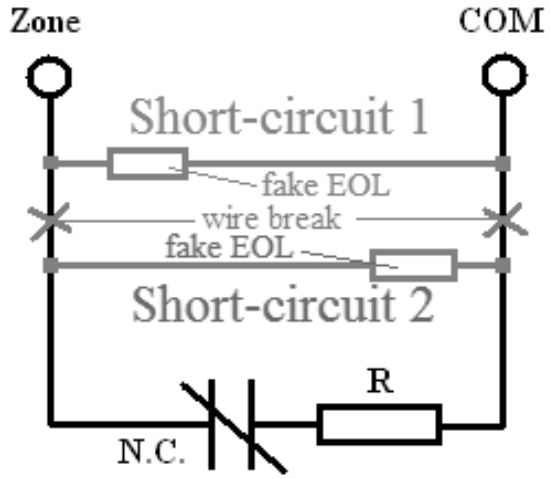

Fig. 1. – Short-circuit systems

Upon use of a bus bar (as wiring), sabotage is far more difficult than in the case of loop wiring. Successful sabotage would require for example the use of scanning communication (or decoding) across the bus bar, with subsequent replacement of this communication with false reports which correspond to the communication of the existing system.

Wireless systems for communication most frequently use two unlicensed bands which comply with the Federal Commission for Communication (FCC) and the European Telecommunications Standards Institute (ETSI) (POWEL & SHIM, 2012). These are the bands 433 MHz and 868 MHz. These wireless transmissions should be protected by detecting disturbance of the frequency band, which monitors the load on the communication frequency. In the case of overloading of the frequency, the switchboard evaluates this fact and responds according to the setting (malfunction, alarm etc.). The detectors are also mostly protected, namely by "wireless detector surveillance", which monitors the presence of the detector within the range of the switchboard (PETRUZZELLIS, 1993; URBANCOKOVA, 2015; STAFF, 1999).

The greatest risk upon use of wireless communication (between detectors and the switchboard) is a signal frequency jammer (HANACEK, 2015). This can overload the communication frequency by rendering the switchboard incapable of receiving the signal transmitted from the detector. This signal frequency jammer is dangerous above all because it can attack the system before the saboteur enters the guarded area, where he or she could be detected by one of the detectors (HANACEK, 2015).

Measurement of GB detectors should be focused primarily on tests which examine the capability of detection under more arduous conditions.

The GB detector detects pressure in the room and the characteristic sound of breaking glass.

The detectors GBS 210 and Glasstrek were used for measurement. These are frequently used detectors, which are installed in both small buildings and large firms.

All the tested GB detectors are loop detectors with a simple type of sending of alarm information, which are cheap in comparison with other types of GB detectors (using a different type of data transmission).

During these tests an intrusion into the building was simulated, and a window was broken. To initiate the alarm, 60 x 60 cm glass plates were used, which were modified for various types of sabotage.

The GBS 210 detector (Fig. 2) uses the dual method for detection, wherein negligible changes to the air pressure in the room are evaluated (impact to the glass panel) and the subsequent sounds of breaking glass. The sensitivity of the pressure component of the detector can be easily configured according to the distance and dimensions of the protected windows.

Like the GBS 210 detector, the Glasstrek Detector (Fig. 3) uses the dual method for detection, during which air pressure changes in the room are evaluated (impact to the glass panel) and the subsequent sounds of breaking glass. Although the sensitivity of the pressure component of the detector cannot be configured, the used installation distance (4 or 9 meters) can be configured. This configuration changes the evaluation characteristic of the breaking glass. The pressure compound of the detector is constant.

Six detection ability methods of the detectors were tested with differently-modified initialization materials – standard, with coating and a screen. Coating means that the initialization material is modified by being covered by foil on one side. This modification changes the characteristic of breaking glass, and thus it also affects the functions of the detector. A screen is a barrier between the detector and initialization material which dampens the characteristic of the broken glass arising during an attack.

Fig. 2. – Detector GBS 210

Fig. 3. – Detector Glasstrek

The testing was carried out on ten samples of each type, and testing it was repeated twenty times. During every detection method, both the classical breaking of the initialization material (using a metal rod) and the gradual denting of this material were tested. Through denting, the pressure component arising when the initialization material is punctured, is softened. The basic results from the measurements carried out are shown in Tab. 1, 2.

Tab. 1. – Measured results for the detector GLASSTREK

Method of meassurement	Alarms
Breaking the glass	94%
Breaking the glass with tape	82%
Dent glass	88%
Dent glass with tape	6%

Tab. 2. – Measured results for detector 210 GBS

Method of meassurement	Alarms
Breaking the glass	100%
Breaking the glass with tape	92%
Dent glass	98%
Dent glass with tape	34%

RESULTS AND DISCUSSION

The measured results and the overall comparison of GB detectors (Fig. 4) do not differ greatly, with the exception of the better elimination of false alarms. This is caused by the large demands of the building envelope detector, which leads a thorough checking during certification.

Until all the systems are tested, it is possible only to ask how many detectors and systems are at all secure. A further question is whether any system exists which could provide reliable protection for a reasonable price.

The present state of development of security systems is at a point of stagnation. Although manufacturers are constantly attempting to develop systems, the majority copy old errors in the technical design into new products of a higher class, even despite the endeavours of customers to ensure manufacture is modified. Without innovative approaches and user feedback, this array will career into a blind alley.

As stated in the article "Self-mixing digital closed-loop vibrometer for high accuracy vibration measurements", a mechanical wave is fully dependent on the environment (MAGNANI, 2016). Influencing or changing environment will affect even wave that spread the actual environment. From these foundations based on the structure of measuring glass break detectors. The same assumption affecting the environment was described in the article "The Methods of Testing and Possibility to Overcome the Protection Against Sabotage of Analog Intrusion Alarm Systems" (HANACEK, 2015).

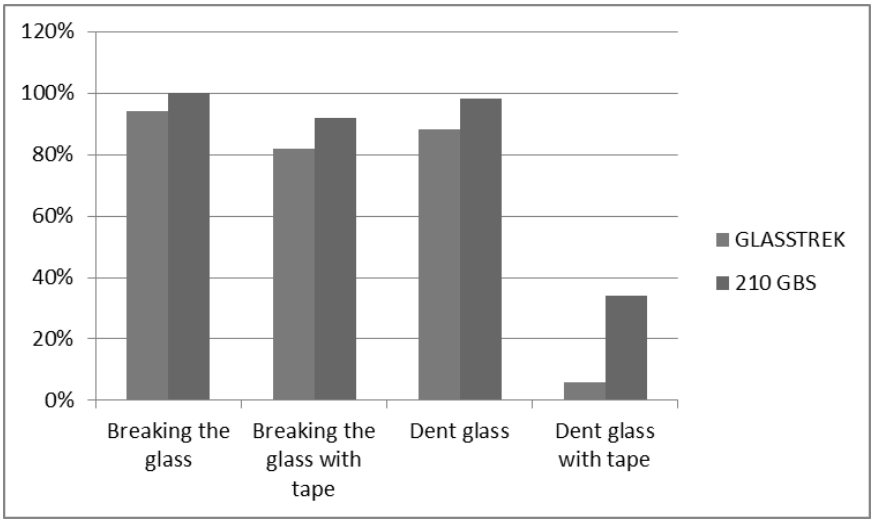

Fig. 4. – Comparison of GB detectors

CONCLUSIONS

The technical design of security systems is unique for the majority of manufacturers. In the case of every manufacturer it is possible to find some poor technical designs which require modification. This deficiency can be resolved by technical development of the given product and adaptation to customer requirements.

The practical tests conducted on GB detectors brought an insight into their functionality and usability in practice. If a saboteur is instructed about the operation of these detectors, then they can be overcome. At the same time the saboteur can also bypass the individual loops, and if skilled, can also bypass loops with an EOL resistor.

Tests have proved that a glass break detector GBS 210 better processing and evaluation of the situation caused alarm. Glass break detector Glasstrek not qualitatively adequate evaluation of alarm situations.The only protection which would be usable against current sabotage techniques is the development of new technologies. It is very important not to cast doubt on this development and to apply a constant endeavour to advance towards new technologies and greater security.

ACKNOWLEDGEMENTS

It is a project supported by the CULS IGA TF 2016 “The University Internal Grant Agency” (Innovation of systems for verification of a person according to his characteristic).

REFERENCES

1. CAPELL, V.: Security Systems & Intruder Alarms. Elsevier Science, 1999: 301 p.
2. CUMMING, N.: Security: A Guide to Security System Design and Equipment Selection and Installation. Elsevier Science, 1994: 338 p.
3. HANACEK, A., SYSEL, M.: The Methods of Testing and Possibility to Overcome the Protection against Sabotage of Analog Intrusion Alarm Systems. 4th Computer Science On-line Conference (CSOC). 2015: 119-128 p.
4. HANACEK, A., SYSEL, M.: Universal System Developed for Usage in Analog Intrusion Alarm Systems. 4th Computer Science On-line Conference (CSOC). 2015: 129-138 p.
5. KRECEK, S.: Manual security technology. Blatná: Circetus, 2006: 313 p. (in Czech).
6. MAGNANI, A., MELCHIONNI, D., PESATORI, A., NORGIA, M.: Self-mixing digital closed-loop vibrometer for high accuracy vibration measurements. OPTICS COMMUNICATIONS, 2016: 133-139 p.
7. PETRUZZELLIS, T.: Alarm Sensor and Security. McGraw-Hill Professional Publishing, 1993: 256 p.
8. STAFF, H., HONEY, G.: Electronic Security Systems Pocket Book. Elsevier Science, 1999: 226 p.
9. UHLÁŘ, J.: Technical protection of objects, Part II, electrical security systems II. Prague: PA ČR, 2005: 229 p. (in Czech).
10. URBANCOKOVA, H., VALOUCH, J., ADAMEK, M.: Testing of an intrusion and hold-up systems for electromagnetic susceptibility - EFT/B. International Journal of Circuits, Systems and Signal Processing. 2015: 40-46 p.

Corresponding author:
Ing. Jan Hart, Ph.D., Department of Technological Equipment of Buildings, Faculty of Engineering, Czech University of Life Sciences Prague, Kamýcká 129, Praha 6, Prague, 16521, Czech Republic, phone: +420 22438 3330, e-mail: jhart@tf.czu.cz