Agronomy Research **12**(3), 949–954, 2014

Reliability of detection of sources of infrared radiation in security alarm and distress signal systems

J. Hart*, V. Nídlová and M. Přikryl

[1]Department of Technological Equipment of Buildings, Faculty of Engineering, Czech University of Life Sciences Prague (CULS), Kamýcká 129, 16521 Prague, Czech republic; *Correspondence: jhart@tf.czu.cz

Abstract. The problem of detecting sources of infrared radiation affects a large proportion of security alarm and distress signal systems. In a time of increasing property crime, it is highly important for passive infrared detectors (PIR) to be able to detect motion within the guarded area reliably and free of error. In the case of installation of passive infrared detectors (PIR) it is naturally important not only to ensure correct installation, to gauge the external influences impacting upon the detector and ensure proper maintenance, but also to guarantee their capability of detection under more arduous conditions. The tests which have been conducted examine both the normal operation of the PIR detectors and the operation of these detectors under extreme conditions (temperature, soiling, screens etc.). These tests are important both from an informative perspective and due to the possibilities of development of potential counter-measures which could lead to their improvement and an enhancement of their level of security.

Key words: security risks, sabotage, intrusion and hold-up alarm systems, passive infrared detector.

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. The critical point of every security alarm and distress signal system is predominantly elements of spatial protection. 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 PIR detector (passive infrared), which ranks amongst passive detectors. On average, of all the types of detectors used, the largest number of false alarms occur on these detectors. This high error rate is primarily caused by incorrect installation.

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. 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. Above all, however, they have an influence on determining the security risks of buildings.

Upon installation of PIR detectors it is necessary to take into account a number of fundamental prerequisites. The first prerequisite is for the detector not to detect the source of interfering of infrared radiation and to be installed so that the envisaged movement of the attacker is tangentially to the detector (Kic, 2013). 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 (Staff & Honey, 1999; Marayeнов, 2007; Capel, 1999). 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 security alarm and distress signal system.

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 (Fig. 1a). If a resistor is connected, bypassing is far more difficult than in the case of a simple loop (it is not possible to use 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. 1b).

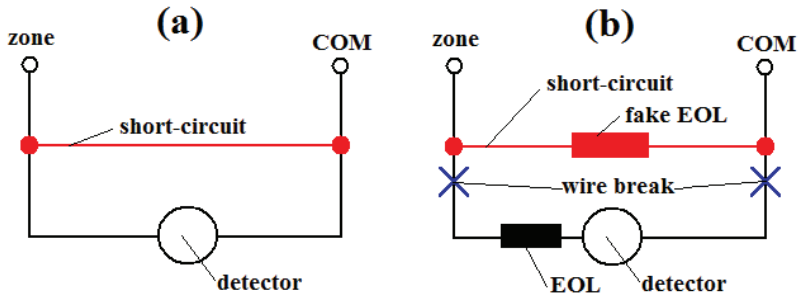

Figure 1. Short-circuit systems.

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 frequencies on 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; Cumming, 1994).

The greatest risk upon use of wireless communication (between detectors and the switchboard) is a signal frequency jammer. 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.

Upon testing of wireless transmissions, deficiencies have been determined in certain systems, and as a result it is necessary to take these deficiencies into account.

Measurement of PIR detectors should be focused primarily on tests which examine the capability of the PIR detector upon use of a shielding screen.

The PIR detector detects IR (infrared) radiation from the guarded area, and the alarm state of the detector is then evaluated on the basis of the difference in electrical charge which ensues upon the flow of IR radiation through the optics. With regard to the fact that IR radiation is emitted by every element with a higher temperature than absolute zero, the pyro-cell is adjusted in order to be most sensitive within the temperature range of approximately 25°C to 40°C. If this temperature can be reduced on the element by whatever method, this will severely affect the capability of the PIR detector.

The detectors PARADOOR (460), PRO plus (476) and DG 55 were used for measurement. These are frequently used detectors, which are installed in both small buildings and large firms.

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

All the above PIR detectors were tested for covering in close proximity, covering in intermittent motion and covering with a screen.Covering in close proximity is testing of testing of a PIR detector, which begins outside the detection boundary of the guarded area at a distance of 2 m ± 0.2 m or at a distance of 0.5 m ± 0.05 m from the reference line (assembly surface) of the detector. Distance is selected according to the degree of security into which the tested detector falls.

Covering upon interrupted motion is testing of a PIR detector beginning outside the boundary of the detection area from the opposite side of the detector and the intersecting centre of the axis of the detector in half the maximum range beneath an angle of 45° to this axis. The standard detection target begins intermittent motion in such a manner that it stands with feet together and then takes two steps 0.5 long at a speed of 0.2 – 0.1 m s^{-1} and stops with feet together. After 5 seconds the cycles are repeated until leaving the detected area.

The tests conducted on the above detectors were performed at two different distances from the detector, namely at a distance of 0.5 m from the detector and at a distance of 50% of the stated range of the detector.

In the tests motion was used at a speed of 0.1 m s^{-1}, 0.2 m s^{-1}, 0.5 m s^{-1}, 1 m s^{-1} and 2 m s^{-1} in the direction designated by the manufacturer (tangentially in the direction of the PIR detector). Ten measurements were taken from each test, and the

materials used as a screen were cloth, polystyrene, carton and glass (at approximately the same temperature as the room).

RESULTS AND DISCUSSION

The measured results and the overall comparison of digital and analogue detectors (Fig. 2) do not differ greatly, with the exception of the better elimination of false alarms in the case of digital processing of the output from the pyro-cell. This is caused by the large demands on spatial detector, which leads a thorough checking during certification.

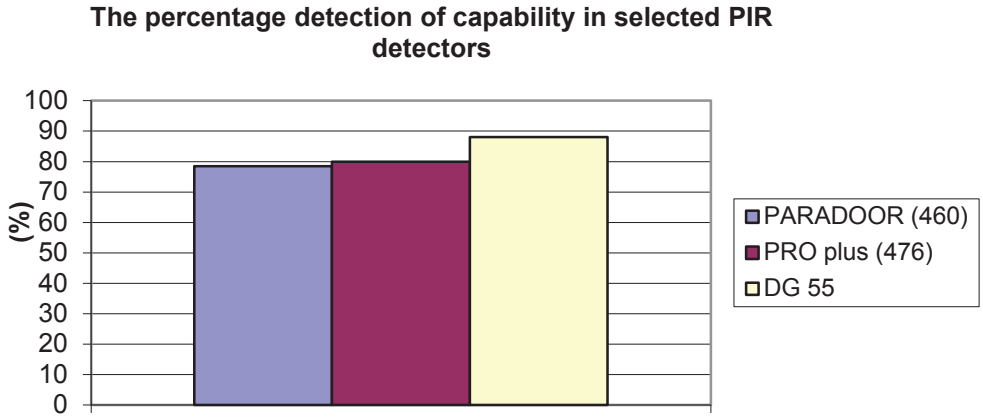

Figure 2. Comparison of analog and digital PIR detector.

One of the greatest potential hazards in the case of a PIR detector is that the offender uses a screen which absorbs IR radiation and thus prevents the PIR detector from detecting movement within the guarded area. Tests conducted in individual types of screens and the detection capability of PIR detectors clearly showed that cloth and carton screens are 30% detectable. By contrast, polystyrene and glass screens present a serious risk, because they were detectable only in values around 5% of the total number of measurements – see Fig. 3.

The tests we conducted pointed to deficiencies in heat detection by a PIR detector upon the use of a screen. The risks which most affect the security risks of PIR detectors were evaluated on the basis of standard and experimental measurement.

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.

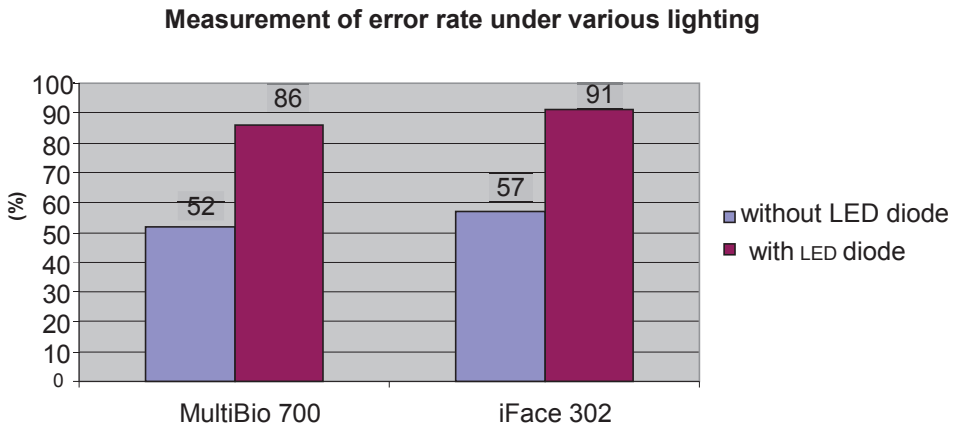

Figure 3. Detection capability of PIR detectors for movement with screen.

Thanks to many years of testing security risks of I&HAS and also thanks to the cooperation with several manufacture of I&HAS we found that the present state of the development of security systems at the 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.

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 PIR 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.

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 IGA 2014 ‘The Internal Grant Agency TF’ (31170/1312/3124).

REFERENCES

Capel, V. 1999. *Security Systems & Intruder Alarms*. Elsevier Science, 301 pp. ISBN-13: 9780750642361.

Cumming, N. 1994. *Security: A Guide to Security System Design and Equipment Selection and Installation*. Elsevier Science, 338 pp.

Kic, P. 2013. Hot-air heating of family houses with accumulation of energy in the floor. *Agronomy Research* **11,** 329334.

Магауенов, Р. 2007. *Охранная сигнализация и другие элементы систем физической защиты.* Краткий толковый словарь. Горячая Линия - Телеком, 98 стр. (in Russian).

Petruzzellis, T. 1993. *Alarm Sensor and Security*. McGraw-Hill Professional Publishing, 256 pp.

Powell, S. & Shim, J.P. 2012. *Wireless Technology: Applications, Management, and Security*. Springer-Verlag New York, LLC, 276 pp. ISBN-13: 9781461429364.

Staff, H. & Honey, G. 1999. *Electronic Security Systems Pocket Book*. Elsevier Science, 226 pp.