DEVELOPMENT OF NEW TESTERS TO IMPROVE QUALITY FOR DATA TRANSMISSIONS IN INTRUSION AND HOLD-UP ALARM SYSTEMS

Jan Hart, Veronika Hartova
Czech University of Life Sciences Prague
jhart@tf.czu.cz

Abstract. Development of new measuring and security technology is always needed and will be to improve the current situation because of the increased safety for I&HAS (intrusion and hold-up alarm systems) or their control. The Czech University of Life Sciences Prague was to increase the safety of I&HAS developed testers. These testers are used for testing of data transfers in I&HAS. Also devices have been developed for enhancing security of wireless transmissions in I&HAS. It increases protection by revealing the jamming wireless bands outside of standard monitored sites. This research and development are guided primarily because it is a security branch in the stage of stagnation, and it is essential that there is continuous innovation and research in this field of science. New security features or upgrades to the existing features in security systems were solved on the basis of the current state of development of the current testers. When developing new technologies grants also help us as well as personal experience with real installation, cooperation with manufacturers (or with distributors) of security systems and a testing ground for current security features.

Keywords: jamming, resistor, development, improve, wireless, loop, tester.

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 to be sufficiently resistant to attack [1; 2].

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 "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. [2]. It is for this reason that at the moment when there is a development of a new technology, someone is already working on sabotage techniques, how to sabotage this technology [3; 4].

This article is dedicated to representatives from the testers, 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. The development is focused mainly on the testers to loop security systems and security systems with wireless transmission [2; 5].

Loop security systems have a very simple principle of indication alarm (breaking the loop). Loop security systems occupy the majority part of the market today, but they are gradually displaced by the bus systems that are safer and easier (simpler that there is no need to consider a large number of cables). The loop security systems contain terminal block zones, which are introduced into the individual loops for connecting the loop detectors. Risk loop connections are predominantly in the possibly shorting line [1; 3].

Wireless security systems are forming a wireless network. This wireless network consists of wireless detectors, peripheral devices and the control panel. The wireless network operates in the ISM band and has either simplex or duplex wireless transmission. The form of wireless transmission depends on the particular manufacturer. Risks of wireless transmissions are mainly in the possibility of making easier jamming [6; 7].

It is therefore important to have testers, that define whether the system is resistant or not. Without adequate testers we will not be able to easily determine whether the system is correct and therefore the development in this area is necessary [4].

Development of testers for loop security systems

Nowadays, security systems are used for closing loop end-of-line (EOL) resistors. This resistor increases their safety and protects the system against sabotage circuiting. Each system has unfortunately certain tolerance, accepting for EOL resistor. A system that uses EOL resistance of one kOhm, accepts, for example, a resistance of 800 ohms [4].

There are methods that sabotage involved in EOL resistors allow, even if knowledge is required of security systems and low voltage electronics. One possibility bridging EOL wiring is called Svoboda bypass. This bypass is constructed using a potentiometer, which provides resistance in the loop – see Fig. 1.

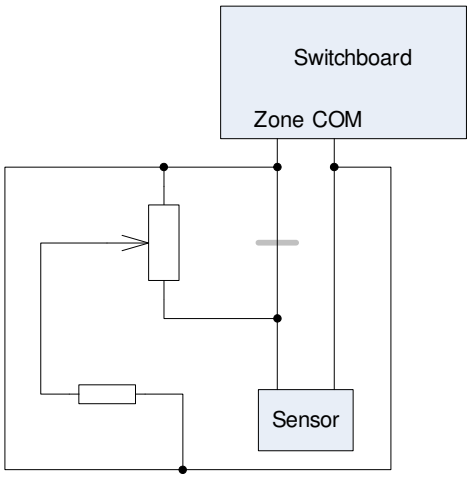

Fig. 1. **Svoboda bypass**

The tester of the balancing resistors established balancing resistors PUV 2011-24387. It consists of a body tester, for which the two are brought from the switchboard loop, potentiometer and display. Using the display it is possible to determine the current and the resistance according to the switchboard will assess how much resistance tolerated [7].

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 the panel can accept. The tester balancing resistor is designed so that the potentiometer changes continuously resistance in this loop, so it can deduct the value of resistance, which it can accept. That the resistance is shown in Fig. 2, where it was selected for testing the change continuously resistance 1.1 kΩ. The course of the test is as follows:

- setting the potentiometer to the maximum value (in this case 1100 ohms)
- slow reduction (over 10 seconds) of the resulting resistance (rotation potentiometer to its minimum, which in this case is 800 ohms)
- followed by a slow running of the cycle (cycle time is 20 seconds and is shown in Fig. 3).

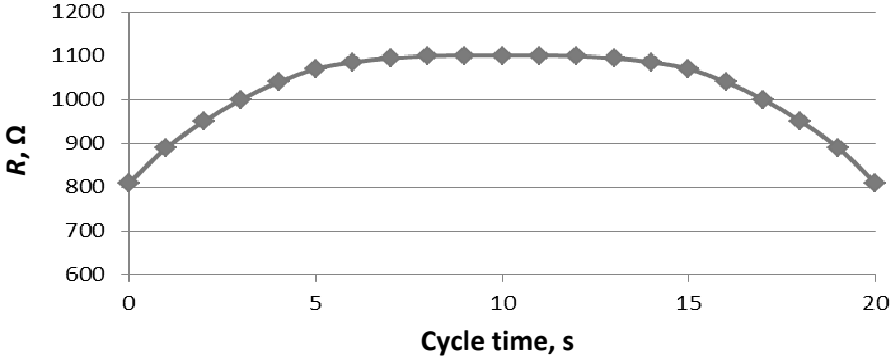

Fig. 2. **Course of the transition potentiometer**

Due to the fact that most of the alarm control panels have a loop response time of about 300 ms (the exact values are dependent on the particular alarm control panels) it is precisely defined, wherein the alarm control panel has its limits.

Tester alarm loops to test resistance of the system against bridging (PUV 2011-24390) serve as a balancing resistance tester for testing loops with loop switchboards. Unlike tester balancing resistors not tested range in which the panel evaluates the presence of resistance, but the reaction time switchboards when possible sabotage. If the test fails to respond, it is not resistant to bridging – see Fig. 3.

Although the system can circumvent a technical solution EOL resistors balancing is one of the best solutions to protect against sabotage bridging loop. It prevents bridging hard (direct bridging wire) and increases the chance of miscalculation potential saboteur.

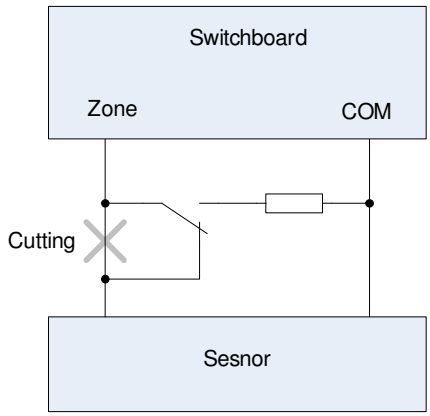

Fig. 3. **Reaction-time tests**

Development tester for increasing security of wireless transmissions

Wireless transfer from the detector to the switchboard is very risky because of the possibility of relatively easy sabotage. For this reason, any wireless system does not receive a higher class of security than wired systems. When a potential saboteur tries to sabotage wired systems, it must first get to the loop or be thoroughly familiar with the principles of the evaluation of the detector and bypass it for physics. In wireless systems, these problems eliminate the need of sabotage jammer signal. Wireless security systems operate mainly on the frequencies 433 and 868 MHz. At these frequencies detectors communicate with the switchboard (used for reporting an alarm, its presence, etc.) [3; 5].

Sabotage by means of the jamming signal is the most dangerous and most effective way to disable the wireless security system. The jamming signal is one of the simplest methods of attack of wireless systems I&HAS. This is a simple and very effective method, which needs only a low frequency jammer.

On the basis of insufficient protection of the existing systems a tester has been developed, which can serve as a detector of the jamming signal named “Tester detection of jamming signals”.

Currently, only integrated jamming detection zone is used, which has built-in electrical panel security systems. This method of detection is indeed good and safe (for most manufacturers), but does not cover the actual location of the wireless space detectors. This creates space for possible sabotage of the system using low-frequency jammers.

Tester detection of jamming signals consists of an evaluation unit, which is connected to a terminal and the wireless signal receiver with integrated antenna.

Tester detection of jamming signals receives the wireless signal switchboard and data that are sent from the switchboard via bus. Each wireless transmission from the switchboard to the detector is transmitted over the bus. Then the received data are compared in the evaluation unit, which determines the integrity of the transmitted information and whether it ever reached. If biased or not at all, so the counter starts and after a while sends the alarm message to jamming band – see Figure 4.

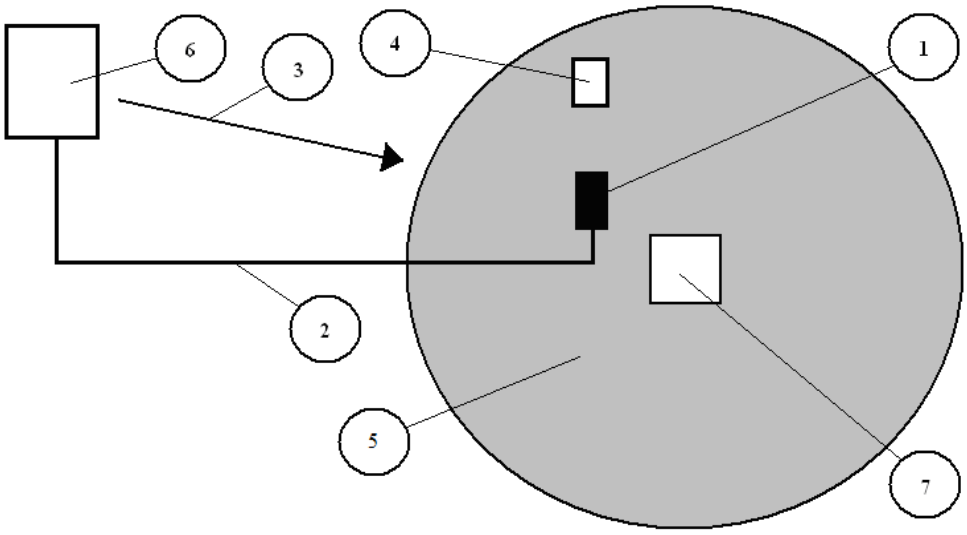

Fig. 4. **Principle of the tester detection of jamming signals:** 1 – Tester detection of jamming signals; 2 – BUS; 3 – wireless signal; 4 – wireless detector; 5 – jamming field; 6 – switchboard; 7 – jammer

Tester detection of jamming signals (1) consists of an evaluation unit, which is connected to a terminal and the wireless signal receiver with integrated antenna. The terminal is connected to the bus (2), which leads from the switchboard (6) electrical security systems.

Tester detection of jamming signals transmitted systems receives a wireless signal (3) switchboard and data that are transmitted from the switchboard via bus. Each transmitted wireless transmission from the switchboard to the detector of wireless systems is also sent over the bus. Then the received data are compared in the evaluation unit, which determines the integrity of the transmitted information and whether it ever reached. If biased or not at all, and runs counter after a certain time, sends an alarm message on the band jamming.

During normal simplex data transfer from the current wireless detector (4) to exchange security systems and electrical panel to a detector of wireless systems any attempt to distortion is not evaluated as the detector of wireless systems is not a low-frequency jammer jamming (7). If the wireless detector gets to jamming field (5) low-frequency jammers, so is its regular simplex wireless jamming and status information arrives to the control of electrical security systems. If this is jamming field detector of wireless systems, so it arrives broadcast wireless transmission from the switchboard and incoming data which it receives the bus, I have nothing to compare. Depending on the defined time after the switchboard sends messages about electrical safety systems jamming band.

Discussion

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. It is therefore essential that security systems are in detail tested [4-7].

In order to prevent the possibility of sabotage of security systems, it is very important to continually improve the systems. The 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 [8; 9]. And similarly Urbančoková, Valouch and Adamek approach this problem in their article “Testing of an intrusion and hold-up systems for electromagnetic susceptibility – EFT / B” [10].

As stated in “Security Systems & Intruder Alarms” the security design is one of the most important parts of the entire installation.[1] This can minimize false alarms and lower the costs for acquiring the system. The same is stated in “Security: A Guide to Security System Design and

Equipment Selection and Installation", and that is why we would recommend primarily development of a new technology [2].

All important facilities must have adequate testers. This hypothesis is supported by the articles "Development of Transmission Error Tester for Face Gears," "The Development of the Tester for the DSD Series High Frequency Electric Brush Planting Power Supply" and "Development of a New Short-Circuit Tester for 1.7 kV High Current Power Devices " [11-13].

Based on the lack of sophisticated measuring equipment there was a need to develop new testers to test alarm control panels. The development was primarily aimed at testers monitoring functionality of the communication component of the panel. Protection alarm information is indeed as one of the most important activities that the panel should do. That is why we developed tester loops and wireless communications in I&HAS.

Conclusions

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

Based on the current situation and weaknesses some sophisticated testers were developed for monitoring security systems. The development was primarily aimed at testers for the transmission of alarm information. "Tester of the balancing resistors" was developed that can determine the maximum and minimum resistance which the panel accepts as an EOL resistor. As a further developed there were "Tester alarm loops" that test the durability of the alarm control panel to deliberate sabotage by means of a short circuit on the loop. "Tester alarm loops" are testing the system so that it performs sophisticated short circuit on the loop. If the alarm control panel will respond to this test, it is resistant to this type of sabotage. The last tester "Tester detection of jamming signals" is used to detect sabotage of wireless transmissions. Wireless devices (detectors, modules, etc.) are the most vulnerable part of I&HAS. There are many ways to attack wireless components but the most effective way seems to use low-frequency jammers, which (if not jamming detection zone) disable communication between the detectors and the switchboard from service. "Tester detection of jamming signals" can detect attempts at jamming.

Due to the continuous development of sabotage techniques it 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.

Acknowledgements

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

References

1. Capel 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, 199,. 338 p.
3. Damjanovski V. CCTV, Second Edition: Networking and Digital Technology. 2 edition. Butterworth-Heinemann. 2005, 584 p.
4. Křeček S. Handbook of security technology. Blatná: Circetus, 2006. 313p
5. Petruzzellis T. Alarm Sensor and Security. McGraw-Hill Professional Publishing, 1993. 256p.
6. Staff H., Honey G. Electronic Security Systems Pocket Book. Elsevier Science, 1999. 226p.
7. Uhlář J. Technical protection of objects, Part II, electrical security systems II.. Praha: PA ČR, 2005. 229 p. (in Czech)

8. 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. pp. 119-128,
9. Hanacek A., Sysel M. Universal System Developed for Usage in Analog Intrusion Alarm Systems. 4th Computer Science On-line Conference (CSOC). 2015, pp. 129-138.
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, pp. 40-46.
11. Shi Z.Y., Lu X.N., Chen C.H., Lin J.C. Development of Transmission Error Tester for Face Gears. 6th International Symposium on Precision Mechanical Measurements (ISPMM) Guiyang: Proceedings of SPIE, 2013.
12. Zhang R., Piao X.F., Jin H. The Development of the Tester for the DSD Series High Frequency Electric Brush Planting Power Supply. International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC). Shenyang: AER-Advances in Engineering Research. 2015, pp. 930-934.
13. Maresca L., Cardonia M., Avallone G., Riccio M., Romano G., de Falco G., Irace A., Breglio G. Development of a new Short-Circuit Tester for 1.7kV High Current Power Devices. 29th International Conference on Microelectronics (MIEL). Belgrade: International Conference on Microelectronics-MIEL. 2014, pp. 85-88.