INTEGRATION OF FIBARO SYSTEM TO INTRUDER AND HOLD-UP ALARM SYSTEMS

Jan Kaderabek
Czech University of Life Sciences Prague
xkadjan@gmail.com

Abstract. The Fibaro is a system for automation of smart households, which ensures not only the functions of comfort and power saving, but it also offers the security functions. These security functions were checked and examined in this paper from several perspectives. The evaluation of two submitted model realizations of Intruder and Hold-Up Alarm Systems (I&HAS) with using of the Fibaro system was presented: the Proprietary model, which works with manufacturers' detectors, and the Integration model including the standard loop I&HAS to the Fibaro system. These comfort functions were examined in this paper from the point of view of the functional safety and fulfillment of the normative requirements for the I&HAS. The examination of functional reliability consisted of verification of the ability of the control unit to correctly respond to changes in detection conditions inducted through the relevant sensor. The functional tests were conducted in several steps. Thanks to the functional tests the unreliability of the control unit Fibaro HC Lite to register a larger number of detection messages had to be confirmed. The result of this work was the demonstration of inappropriateness of utilisation of installations according to the Proprietary model. Simultaneously the Integration model was evaluated from a point of view of valid norms with assigning of the first security level, however, the conditions unaffected the I&HAS.

Keywords: Fibaro HC Lite, I&HAS, Z-Wave, integration, intelligent building.

Introduction

For a long time we can see many forms of integration the Intrusion and hold-up systems (I&HAS) with others systems in building [1; 2]. In practice we can see I&HAS integrating the technology systems (HVAC, ACC, CCTV etc.) [3] or some complex systems called "the intelligent households", „the intelligent buildings" [4] or even "the intelligent cities" [5] integrating the I&HAS. Generally, the integration of the I&HAS is not easy from the viewpoint of technological feasibility nor adherence of norms [6; 7]. Often we can see the complex systems without the relevant certification. But it may be indicative of worse functional safety, which is at the security systems very important. One of these similar systems (they may have the next commercial names, e.g., "smart home system") is the Fibaro system, which is the subject of evaluation in this paper. It offers useful comfort and saving functions, and also the security functions. However, all components of the Fibaro system do not have the certificated security level related with I&HAS. Therefore, it was appropriate to examine the real reliability of these security functions and also contemplate the options of deployment of the Fibaro system as I&HAS from the point of view of the related norms.

Materials and methods

For the purposes of this paper two models of physical implementation were assembled: the Proprietary model (Fig. 1) using detectors by the manufacturers, and the Integration model (Fig. 2) integrating the conventional loop of I&HAS to the Fibaro system. As the transmission medium the Proprietary model uses the Z-Wave network [8; 9] for all self-functionality (including security features), whereas the Integration model uses for the security features the wired transmission and other features realized through the Z-Wave. Because the Fibaro system is often used for purposes of security features in practice, it was advisable to conduct the tests of the reliability of this model.

Generally, the big problem of wireless I&HAS is usually the problem with the reliability of transmission of information about the detected states to the switchboard. It is often caused by the influence of the natural electromagnetic interference [10; 11], influence of antennas distance or influence of obscuration of transmission, eventually by the influence of the artificial electromagnetic interference. These influences should be firstly the subject of evaluation the reliability of the Proprietary model. However, during the first tests unanticipated influence of reliability transmission was manifested. This unanticipated influence was downgrading the meanings of these firstly proposed tests. It was discovered that on the final reliability of the Proprietary model the influence of the number of packets registering reliability on the number of packets registered by control unit in the measurement period was negatively reflected.

DOI: 10.22616/ERDev2017.16.N228

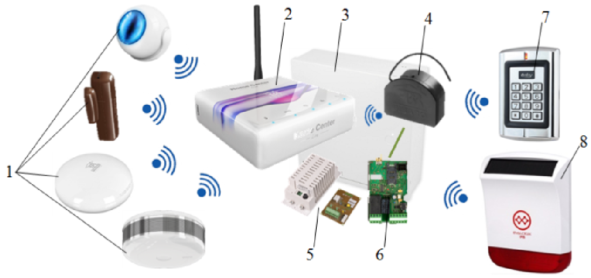

Fig. 1. **Proprietary model:** 1 – Z-Wave detectors; 2 – Fibaro HC Lite (switchboard); 3 – case; 4 – Fibaro relay FGS-211; 5 – backup power; 6 – GSM output; 7 – Z-Wave access keypad; 8 - Z-Wave alarm

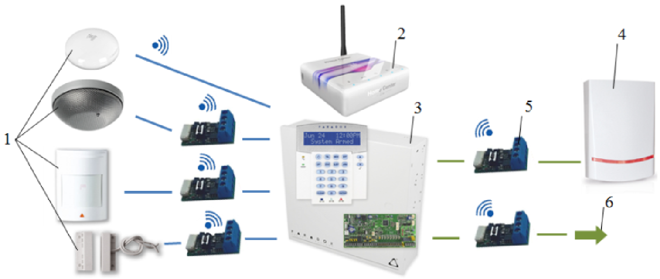

Fig. 2. **Integration model:** 1 – loop detectors; 2 – Fibaro HC Lite (only monitoring features); 3 – loop switchboard with case and keypad; 4 – loop alarm; 5 – Fibaro Universal Binary Sensor; 6 – free PGM outputs

For purposes of this measurement the method according to the Functional Examination was used, which is included in the norm BS EN 50131-3:2009 [12]. It consists of the monitoring of cyclic transmission of information about detections (packets) on the switchboard input. In this case the switchboard was the control unit Fibaro HC Lite and the component transmitting information about detection (transmitter) was the Fibaro Universal Binary Sensor.

The measurement was partly automatized. The microcontroller ATmega168, the part of the board Arduino Uno, was controlling the optocoupler 6N139 which was switching the loop of the transmitter input between open and closed state. Thanks to this method the state-changes on detectors, ordinarily used in I&HAS (e.g. door contacts, glass break detectors, motion detectors, perimeter detectors etc.) was simulated.

The measurement was conducted in the laboratory conditions of the Czech University of Life Sciences in Prague. Before the main measurement of the Fibaro system was conducted, the measurement of intensity of electromagnetic noise in laboratory thanks to the spectrum analyzer SPECTRAN HF-6065 (the manufacturer: Aaronia) was made. This verification of conditions was conducted in the area between the transmitter antenna and the switchboard antenna during one hour. Through the MSC Spectrum Analyzer software the intensity of electromagnetic noise was recorded in the band 868-870 MHz with the mean value of -73 dBm.

The main measurement of the reliability was conducted with direct visibility of both antennas on five distances: 1, 5, 10, 15 and 20 m. Every distance was verified in eight measurement cycles, from four cycles in a row measurements were conducted with previous restart of the control unit and thereafter four cycles in a row were conducted without previous restart. One thousand packets were gradually sent within each measurement cycle. The time period between two sent packets was 0.5 s. After the end of each measurement cycle the extract from the event log was copied to the table (from the Fibaro Home Center Lite web application: PANELS -> ALARM PANEL).

Subsequently, the number of the received records was counted from this extract. In the first evaluation the first four measurement cycles (four thousand packets) for each distance were included. In the second evaluation the next four measurement cycles and the last measurement cycle from the first evaluation (five thousand packets) for each distance were included. The third evaluation was based on the data from the second evaluation, whereas the number of packets registered by the control unit before the measurement cycle was taken into account. All results were converted to percentages and represented reliability.

In the question of the option analysis of application of the Fibaro system as certificated I&HAS there was a concern to verify it according to the two related norms CLC/TS 50398:2009 [1] and BS EN 50131-1:2006 [2] considering both models of realization. Both of these norms are approved by the European Community at present and are valid as the harmonized norms for large part of the states of the EU.

Results and discussion

The evaluation of the reliability was based on the measurement of the percentages of successfully registered packets by the Fibaro HC Lite control unit to its event log. The packets were artificially transmitted by the Fibaro Universal Binary Sensor through wireless with direct visibility of the control unit and transmitter antennas. The results were split among three evaluations, so as they could help point out the major problems of the control unit:

- the reliability of registering of packets with restart of the control unit before the measurement cycle;
- the reliability of registering of packets without restart of the control unit before the measurement cycle;
- the dependence of packet registering reliability on the number of received packets by the control unit before the measurement cycle.

In the first evaluation from the graph (Fig. 3) the unreliability of registering all transmitted packets is obvious. Nevertheless, the deviation from the assumption that the reliability will have a downward trend with increasing the distance between both antennas was not shown there. The average reliability amounted 99 % from this measurement with counting all five distances.

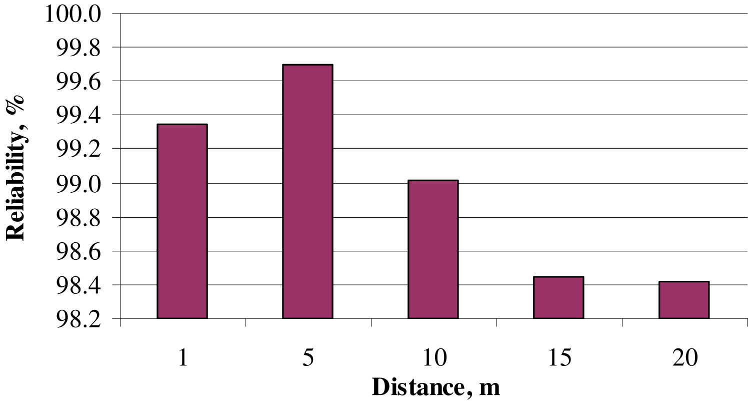

Fig. 3. **Reliability of registering of packets, with restart of the control unit before the measurement cycle**

In the second evaluation, where the restart was conducted every time, from the graph (Fig. 4) it can be seen that only in the first measurement cycle the reliability was worse. After averaging all five measurement cycles about five distances the reliability was 57 %. The distance of both antennas apparently did not affect the result. As in these two evaluations only the act of execution or non-execution of restart of the control unit before the measurement cycle differs, it can be surmised that the reliability is dependent on this act. Furthermore, it can be assumed that this property negatively affects the reliability in the previous time when the control unit received the first thousand packets that were probably reflected in the results of the first evaluation (Fig. 3).

The third evaluation (Fig. 5) was drawn based on the same data used for the second graph (Fig. 4). With ignoring the influence of the distance of the cycles, the same number of transmitted packets on the control unit before the measurement was averaged. The first column of the graph (Fig. 5) shows the average reliability 98 % that was the measured value closest after the restart of control. Conversely, the fifth column shows the average reliability 33 % in time when to control unit four thousand packets are already sent. There is well visible the decreasing reliability of the control unit.

Based on the Pearsons correlation coefficient (α = 0.05; r = -0.9484) we could declare that the reliability and the number of packets registered by the control unit before the measurement cycle are dependent on themselves.

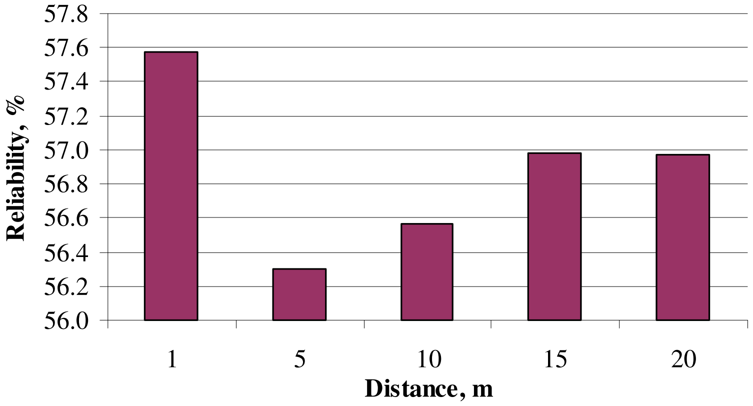

Fig. 4. **Reliability of registering of packets, without restart of the control unit before the measurement cycle**

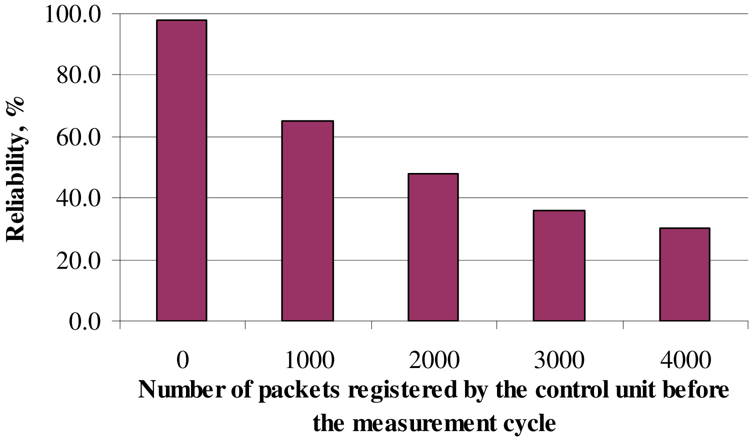

Fig. 5. **Dependence of packet registering reliability on the number of packets registered by the control unit before the measurement cycle**

These results clearly indicate that the problem with reliability was not in the wireless transmission, but in the capability of the control unit to process big amounts of packets. Since the control unit can work with 230 devices (although the manufacturer recommends maximally 150) that can transmit quite often, the same situation may arise as in these measurements. Thus, the risk of security threats occurs where the system is deployed. The found rate of unreliability of this system is for I&HAS unexepted.

In question of evaluation of deploying the Fibaro system as eventually certificated I&HAS was drawn from work [3]. In this work the author collected the possibilities and the requirements related to the problematics of integration of I&HAS to so called “Intelligent building” in technical and normative terms. Further it was drawn from work [8], where the author detailed discusses the meanings of related norms. For definition of integration options of the Fibaro system from the legislative perspective two norms were essential. The first CLC/TS 50398:2009 [1] in the point 4.2.says that integrated building systems must fulfill the related norms for each application. In case of integration I&HAS, it is related to the second norm from the mentioned norm BS EN 50131-1:2006 [2]. It defines four security levels, stricter with increasing range, and says that if the system is divided into subsystems, the security level of the whole system corresponds to the security level of the component with the least security level. However, further this norm in point 5 says that the components others than I&HAS can be integrated with I&HAS assuming that the properties of every component of I&HAS will not be adversely affected. Since the control unit or its components of the Fibaro system do not own certification, it was evident that the Proprietary model cannot be marked with any from the four safety levels. The Integration model had a different situation. Because there was I&HAS managed by the certified security system and the uncertified component Fibaro Universal Binary Sensor played a role of integration of elements only, they ostensibly did not affect the function, it was on the spot to investigate this unaffected result. However, it proved that this element is not able to recognize the protection resistors in the loop (the sabotage protection) due to the absence of input analog ports. The sabotage protection is necessary for security level from the second and more according to the norm BS EN 50131-1:2006, point 8.7.2. If inability of negative influence of I&HAS (the Fibaro Universal Binary Sensor must have a backup power, e.g., form the switchboard) is ensured, it is possible to acknowledge the first security level for the Integration model. Nevertheless, the benefit of the first security level is small and, moreover, the need of verification of negatively unaffecting of I&HAS arises there, exactly the reliability of dismissal the information upon the transmission route through this component.

The current scientific publication does not engage in the Fibaro system for the time being. Some publications are entraining the issue of reliability or security of the Z-Wave protocol or, for example, the issue of the energy consumption of the equipment that uses the Z-Wave [13]. The Z-Wave communication generally is described in the works [14;15]. The parameters of the Z-Wave with the other protocols used in the home automation are compared in the scientific works [8; 16]. The author [17] said that the Z-Wave principle generally has a complicated transmission process of monitoring features compared to the ZigBee, the alternative protocol used in home automation. This could be one of more factors affecting the found unreliability of the Fibaro system in this research and it will be investigated in the process of search for the causes in future research of the author. The study [18] is focusing on the influences, which generally influence the reliability of equipment used in the wireless ISM band. Some studies, for example, the study [19], are focusing on pitfalls of the cyberattacks on the Z-Wave equipment. The study [20] describes in detail the discovered vulnerability of the door locks Z-Wave through interception of communication and subsequently injecting these obtained data to the communication channel. However, it is necessary to say that the works are also bringing the actions, for example, [21] is bringing the action in form of improvement of the intrusion detection system for Z-Wave communication.

On the market we can meet the systems included in the functions of I&HAS the manufacturers of which are ignoring the valid norms. The argument for this ignoring could be the partial obsoleteness arising from inability of the norms to adapt fast to the modern technologic trends in integration. The strictness of the norms has its justification. They are defined as such that they could form a system through its principles, which will protect the property, the health and also the feeling of safety of the users. Therefore, it is essential to make conclusions accepting the actions for reducing of risks arising from integration of I&HAS with other systems of modern buildings.

Conclusions

The main purpose of this paper was the demonstration of the unreliability of the Fibaro system used as I&HAS according to the Proprietary model. This unreliability demonstrably is bound to the unreliability of the control unit Fibaro HC Lite to register a larger number of detection messages transmitted from detectors. The first evaluation of reliability with restart of the control unit before each measurement cycle had the result 98 % in average and in the second evaluation of reliability without restart of the control unit before the first measurement cycle only had the result 57 % in average. It was declared that this reliability was dependent on the number of packets registered by the control unit before the measurement cycle. In the following work it would be suitable to examine this problem more in details, performing the same method of evaluation with using the alternative control unit Fibaro HC-2 and also with the variable period of packet transmitting.

Furthermore, this paper is a collection of the norm requirements for integration of I&HAS into other systems and it evaluates the Integration model according to them. If the condition of not affecting of I&HAS is fulfilled, then the Integration model can be marked only with the first from the four security levels. To ensure this unaffected, it should be useful and advisable to continue other examinations of the component Fibaro Universal Binary Sensor in future work.

Acknowledgements

This work was supported by Czech University of Life Sciences internal project IGA “Evaluation of Accuracy of Determing Position by RTK Recievers”.

References

1. CLC/TS 50398:2009 “Alarm systems – Combined and integrated alarm systems – General requirements”
2. BS EN 50131-1:2006 “Alarm systems – Intrusion and hold-up systems – Part 1: System requirements”
3. Garlík B. Inteligentníbudovy (6. část – 5. Díl). Elektro, vol. 10, 2013, pp. 52-53. (In Czech)
4. Chen H., Chou P., Duri S., Lei H., Reason J. The Design and Implementation of a Smart Building Control System. IEEE International Conference on e-Business Engineering.2009, pp. 255-262.
5. Caragliu A., Del Bo C., Nijkamp P. Smart Cities in Europe. Journal of Urban Technology, 2011, 18(2), pp. 65-82.
6. Čandík M. Objektovábezpečnost II. Zlín: Academia centrum, 2004, pp. 100. (In Czech)
7. Votruba Z. Chytrédomy a bezpečnost. PřílohačasopisůElektroaAutoma, 2012, pp. 22. (In Czech)
8. Gomez C., Paradells J. Wireless home automation networks: A survey of architectures and technologies. IEEE Communications Magazine, 2010, 48(6), pp. 92-101.
9. Yassein M. B., Mardini W., Khalil A. Smart Homes Automation using Z-wave Protocol. 2016
10. Urbancokova H., Kovar S., Valouch J., Adamek, M. Electromagnetic Interference of Components of Intrusion and Hold-up Alarm Systems. 2016, pp. 443-452. (In Czech)
11. Hart J. Testovánípásem ISM 433 a 868 u přenosů v poplachových, zabezpečovacích a tísňovýchsystémech. Automa, 2016, pp. 40-42. (In Czech)
12. BS EN 50131-3:2009 “Alarm systems – Intrusion and hold-up systems – Part 3: Control and indicating equipment”
13. Abbas Z., Yoon W. A Survey on Energy Conserving Mechanisms for the Internet of Things: Wireless Networking Aspects. Sensors, 2015.
14. Miller M. Z-Wave Wireless Communications for Smart Devices and IoT Z-Wave Wireless Communications For Smart Devices and IoT Z-Wave Wireless Communications for Smart Devices and IoT. [online] [30.3.2017]. Available at: http://www.embeddeddeveloper.com/documents/zwavewirelesscommunications.pdf
15. Pa̎tz C. Z-wave basics : remote control in smart homes. Create Space, 2017.
16. Mahmood A., Javaid, N., Razzaq, S. A review of wireless communications for smart grid. Renewable and Sustainable Energy Reviews, 2015, 41, pp. 248-260.
17. Ferrari G., Medagliani P., Di Piazza S., Martalò M. Wireless Sensor Networks: Performance Analysis in Indoor Scenarios. EURASIP Journal on Wireless Communications and Networking, 2007.
18. Ghayvat H., Mukhopadhyay S., Gui X., Suryadevara N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors, 2015.
19. Badenhop C. W., Ramsey B. W., Mullins B. E., Mailloux, L. O. Extraction and analysis of non-volatile memory of the ZW0301 module, a Z-Wave transceiver. Digital Investigation, 2016, pp. 14–27.
20. Fouladi B., Ghanoun S. (n.d.). Security Evaluation of the Z-Wave Wireless Protocol. [online] [30.3.2017]. Available at: https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security Evaluation of Z-Wave_WP.pdf
21. Fuller J. D., Ramsey B. W., Rice M. J., Pecarina J. M. Misuse-based detection of Z-Wave network attacks. Computers & Security, 2017, pp. 44-58.