Aggregated coefficients for Evaluation of Effectiveness of Alarm Systems

Jan Valouch

Faculty of Applied Informatics
Tomas Bata University in Zlin
Nad Stranemi 4511, CZ 76005 Zlin
Czech Republic
valouch@fai.utb.cz

Abstract— The effectiveness of alarm systems can be evaluated based on several factors. The first factor is the basic technical level of alarm system. The second factor is the method of application of the alarm system in an object. Other factors may include, for example quality of project, quality of installation or maintenance procedures and services. The proposal of alarm systems is based on the system and technical requirements, which are intended series of branch technical standards. These standards, however, does not solve the problems of evaluating the effectiveness of alarm systems. The aim of this paper is the presentation of the proposal aggregated coefficients, as a basic starting point for evaluating the effectiveness of alarm systems**.**

Keywords— Integration, aggregated coefficients, alarm system, designing, evaluation.

I. INTRODUCTION

The proposal alarm systems, which include the following applications:

- intruder and hold-up alarm system (I&HAS),
- closed circuit television used for security and surveillance (CCTV),
- access control system (ACS),
- social alarm system (SAS),

is based on the system and technical requirements, which are intended range of professional technical standards CSN EN 50 13x representing support the process of setting up alarm systems in corresponding quality and structure. However, the technical standards specified range does not address the issue of evaluating the effectiveness of alarm systems. However, the technical standards specified range does not address the issue of evaluating the effectiveness of alarm systems. [7].

The term efficiency, which for example in terms of energy is the ratio of output and input power equipment (expressed in percentages) can be understood as the ability of the alarm system to ensure the security of protected interests. The effectiveness of alarm systems depends on their quality [1].

The aim of this paper is the presentation of the original proposal of aggregate factors, which represent the basic starting point for evaluating the effectiveness of alarm systems with the assumption of the possibility of evaluation of systems according to project documentation, as well as systems already installed.

A. Materials and Methods

The proposed solution to evaluation of the effectiveness alarm systems, including a proposal for the aggregate coefficients is based on the analysis:

- system and technical requirements, which are intended by series of sector technical standards CSN EN 50 13x, which represent support for the implementation of alarm systems in adequate quality and structure,
- scope of application of the various components of the alarm system in the protected object,
- method of integration when deployed multiple types of alarm applications.

II. FIELDS OF EVALUATION THE EFFECTIVENESS OF ALARM SYSTEM

The effectiveness of alarm systems is dependent on many factors. I propose to use the following area of evaluation:

- security requirements,
- technical characteristics,
- application of systems
- systems integration.

The proposal of parameters for evaluation of the effectiveness and proposal of aggregated coefficients are based on the following assumptions:

- security requirements (B parameters) will be specified based on the security levels according to standards (the extent to which the equipment meets / does not meet this requirement in accordance with the output of the safety assessment or customer requirements),
- technical characteristics (T parameters) will be determined by the requirements of relevant branch technical standards and is expected evaluation in terms of "how much resp. to what extent "the device meets,
- application of systems (A parameters) will be based on the draft security and will assess the degree of protection object (placement of individual components of alarm systems) in comparison with the scale of the object,
- systems integration (I parameter) will be evaluated in case of integration of multiple alarm systems. I

parameter will depend on the technical execution of integration,

- effectiveness of alarm systems will be expressed by the coefficient of the effectiveness of protective capabilities of the alarm system KPS respectively in case integration of multiple systems as the coefficient of effectiveness of protective capabilities of the integrated alarm system K_{IPS}.

For each of the above parameters will be proposed evaluation criteria. These criteria are described by coefficients.

III. The Proposal of Aggregated Coefficients

The following text presents a proposal of aggregated coefficients for intruder and hold-up alarm systems. Due to the possibility of comparison of individual coefficients are coefficients always evaluated in a numerical scale [1-10].

A. Security coefficient

Security coefficient of intruder and hold-up alarm system is based on the classification of security levels in accordance with CSN EN 50131-1 [2], which are divided into 4 levels (low risk, low to medium risk, medium to high risk and high risk). Classification is based on assumed knowledge of a potential intruder in IHAS and its technical equipment. The table of coefficients is completed with the possibility where the system does not meet any security level. The output is a coefficient K_B, whose value is in the range [1-10].

Table 1. Security coefficient

No.	Security coefficient K_B	Evaluation
1	Level of security 1 – low risk	2,5
2	Level of security 2 – low to medium risk	5
3	Level of security 3 – medium to high risk	7,5
4	Level of security 4 –high risk	10
5	System does not meet any level of security	0

B. Technical coefficients

Technical coefficients include the evaluation of system requirements IHAS and technical requirements for the individual used components. System requirements are based on EN 50131-1 [2]. The technical requirements for each component are set out in other parts of series of branch standards 50131-x, for example:

- EN 50131-2-2 Alarm systems - Intrusion and hold-up systems - Part 2-2: Intrusion detectors - Passive infrared detectors [8].
- EN 50131-3 Alarm systems -Intrusion and hold-up alarm systems - Part 3: Control and indicating equipment [9].
- EN 50131-4 Alarm systems - Intrusion and hold-up alarm systems - Part 4: Warning devices [10].
- EN 50131-2-5 Alarm systems - Intrusion and hold-up systems - Part 2-5: Requirements for combined passive infrared and ultrasonic detectors.
- EN 50131-3 Alarm systems -Intrusion and hold-up alarm systems - Part 3: Control and indicating equipment.
- EN 50131-4 Alarm systems - Intrusion and hold-up alarm systems - Part 4: Warning devices.
- EN 50131-5-3 Alarm systems - Intrusion systems - Part 5-3: Requirements for interconnections equipment using radio frequency techniques.
- EN 50131-6 Alarm systems - Intrusion and hold-up systems - Part 6: Power supplies.
- EN 50131-8 Alarm systems - Intrusion and hold-up systems - Part 8: Security fog device/systems.

Table 2. System coefficient

Coeff	System coefficient K_S	Evaluation
K_{S1}	Environmental class	[1-10]
K_{S2}	Fault detection	[1-10]
K_{S3}	Access level	[1-10]
K_{S4}	Requirements for authorization codes	[1-10]
K_{S5}	Avoidance of brought into a condition	[1-10]
K_{S6}	Overcoming conditions to disallowing to set the status of guarding	[1-10]
K_{S7}	Restoration	[1-10]
K_{S8}	Signal processing / intrusion emergency, sabotage and fault	[1-10]
K_{S9}	Indication	[1-10]
K_{S10}	Indication available in the state of	[1-10]
K_{S11}	Reporting requirements	[1-10]
K_{S12}	Operational criteria for alarm transmission systems	[1-10]
K_{S13}	Tamper detection	[1-10]
K_{S14}	Monitoring of substitution	[1-10]
K_{S15}	Maximum unavailability connection	[1-10]
K_{S16}	Intervals verification	[1-10]
K_{S17}	Security of signals and messages	[1-10]
K_{S18}	The generated signals or messages	[1-10]
K_{S19}	Memory capacity	[1-10]
K_{S20}	Event recording	[1-10]
K_{S21}	Minimum time of power supply, charging time.	[1-10]

C. Evaluation of system requirements

The Table 2 presents a content and evaluation of system requirements (coefficient KS) as a part of the calculation of the technical coefficient KT. System requirements in different areas (see table) are classified by technical standard CSN EN 50131-1[2] with regard to security level (with the exception of class environment). Coefficient expresses to what extent IHAS meets the requirements of the standard. Here is the assumption that if it was declared that IHAS meets a security level (1-4), then will be all the system requirements conform to specified security level and the coefficient of KS should be equal to the 10. If this is not, it means that IHAS does not meet the declared security level. This does not mean that it will not effective at the place deployment. However, it will identify a

serious error caused in process of setting up IHAS (tender documents, design, and selection of components, design documentation, installation, repairs or replacement of additional components).

The resulting coefficient of system requirements K_S, represents the arithmetic average of the coefficients K_{S1} and to K_{SN}.

$$K_S = \frac{K_{S1} + K_{S2} \dots \dots \dots . K_{Sn}}{n} \quad (1)$$

D. Evaluation of technical requirements

Evaluation of technical requirements (resulting coefficient KT) is based on an assessment of compliance with the requirements of each type of components used IHAS (Control panel, PIR detectors, dual detectors, warning device, power supplies, security fog device etc.) according to product standards. [11] For example, PIR detector is compared with the requirements of the relevant product standard CSN EN 50131-2-2, parameters of IHAS control panel are compared with the requirements of standard CSN EN 50131-2-3 etc.

Factors that are evaluated for passive infrared detectors in accordance with CSN EN 50131-2-2:

- event handling,
- generating signals and messages,
- requirements on the speed of passage and body posture targets,
- security against sabotage,
- electrical requirements,
- environmental testing,
- verification of the detection coverage.

Table 3. Coefficients of technical specifications (selected components)

No	Coefficients of technical specifications K_{TS}	Standard
1	Passive infrared detectors	EN 50131-2-2
2	Microwave detectors	EN 50131-2-3
3	Control panels PBX	EN 50131-3
4	Warning devices	EN 50131-4
5	Combined PIR and MW detectors	EN 50131-2-4
6	Combined PIR and US detectors	EN 50131-2-5
7	Power supplies	EN 50131-6
8	Equipment using RF techniques	EN 50131-5-3
9	Opening contacts (magnetic)	EN 50131-2-6
1	Security fog device	EN 50131-8
n	Other used components	Relevant EN

The partial coefficient K_{TSn}. is determined by comparing the parameters PIR detector and requirements standards. Parameters other components IHAS are compared in a similar manner. The following table shows an example of the content and evaluation of the technical specifications of the components IHAS (coefficient KTS) as a part of the calculation of the technical coefficient K_T.

The resulting coefficient of technical specifications KTS, represents the arithmetic average of the coefficients K_{TS1} and to K_{TSn}.

$$K_{TS} = \frac{K_{TS1} + K_{TS2} \dots \dots \dots . K_{TSn}}{n} \quad (2)$$

E. Calculation of technical coefficients

The coefficient K_T is the arithmetic average of the coefficients K_S and K_{TS}. Coefficient takes values in the range [1-10].

$$K_T = \frac{K_S + K_{TS}}{2} \quad (3)$$

F. Applications coefficients

The value of the application coefficient is not dependent on the requirements of the standards. We evaluate the practical deployment of individual components in a specific object [6]. The assessment is based on the basic dividing of types of protection:

- protection of space,
- protection of the building envelope,
- perimeter protection,
- protection of items,
- protection of persons in distress.

The basic prerequisite for evaluation is to determine the scope of protection of each area (in percentage terms), calculated as the coefficient K_{An}. We evaluate the ratio of the total area (or the number of building openings, perimeter length and number of significant items) to the number of deployed technical resources.

For example, we evaluate for protection of space (coefficient K_{APR}) what percentage of the total area of the protected object is covered with motion detectors, i.e. the ratio between the sum of the areas which correspond to the sensing characteristics of the detectors to the total area of the protected object.

Within the protection of the building envelope (coefficient K_{APL}) is evaluated the ratio between the number of building openings to number of all building openings in guarded object.

Coefficient of perimeter protection K_{APE} represents the ratio between the length of the secure perimeter of the protected object to the total length of the perimeter.

Coefficient of protection of items K_{APRE} represents the ratio between the number of secure items and the number of important (valuable) objects (paintings, sculptures, etc.) in the protected object.

Coefficient of protection of persons in distress K_{AT} is the ratio between the number of secure rooms in the building and the total number of rooms in the building.

Output coefficient K_A is the arithmetic average of the coefficients for each types of protection. Coefficient K_A takes values in the range [1-10].

$$K_A = \frac{K_{APR} + K_{APL} + K_{APE} + K_{APRE} + K_{AT}}{5} \quad (4)$$

G. Integration coefficient

In the case of the integration of multiple types of alarm systems in a single object [3], it is necessary in the calculation of the resulting coefficient of the protective capabilities to include the integration factor $\mathbf{K_I}$. The integration coefficient is dependent on methods of integration of alarm applications [4], [5].

The following Table 4 presents an overview of the determined values of the coefficients of integration.

Table 4. Coefficients of integration

No.	Coefficients of integration K_I	Evaluation
	Hardware integration	
1	IN/OUT integration	4
2	IHAS (modular system) / as an integration element	9
3	IHAS as an integration element (including control of home automation)	6
4	Automation system as an integration element	0
5	Integration using function CCTV, ACS, SAS	4
6	Software integration	
7	Software for user administration	1
8	Security software	4
9	Visualization software	6
10	Integration software of systems of buildings	8

a) Methods of integration of Alarm System

The following text describes the basic methods of integration of alarm systems. Technical ways of interconnecting the individual applications can be divided into the following basic groups:

- hardware methods of integration,
- software methods of integration.

Hardware (HW) methods of integration are based on the interconnection of systems through their inputs and outputs and on the technical parameters of alarm systems, which may include, in addition to the basic security functions also specific-expanding elements (modules) to control alarm or non alarm applications (lighting control, heating, access control, etc.). The hardware integration methods also include the use of automation systems (eg intelligent wiring system), which in addition to standard control of technologies for buildings (lighting, heating, air conditioning, blinds, irrigation, sound, etc.) offers the ability to connect security devices (detectors, hold-up devices, control and indicating equipment IAS etc.). Hardware integration methods can be divided into the types listed in Fig. 1.

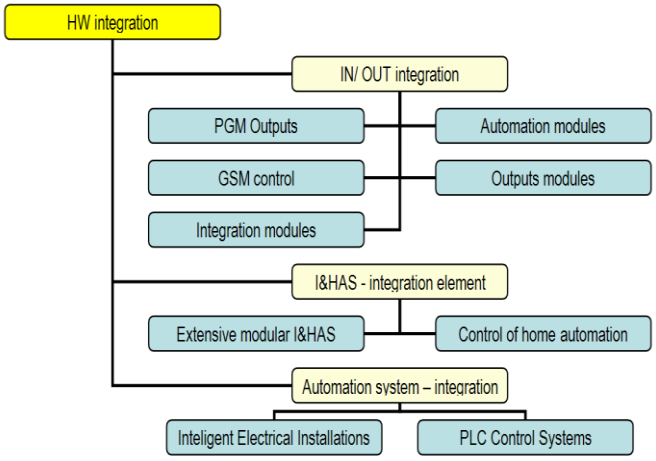

Fig. 1. Hardware methods of Integration of alarm systems

(1) Integration IN / OUT

Technical systems integration solutions labeled as IN / OUT is a way of interconnection systems through their inputs and outputs. The parameters of individual components of alarm systems (eg control and indicating equipment, control units, access control systems, CCTV recording devices, cameras, etc.) allow you to realize the integration of heterogeneous systems to ensure mutual transfer and sharing of information of the sub-systems (I&HAS, CCTV, ACCESS, control of lighting, heating etc.) [8]. This information is then used to control (change state) connected systems in accordance with preset configurations. IN/OUT integration is especially useful for small applications, but it is realizable also in larger projects. Such solutions, however, are technically demanding and limited as the maximum number of programmable outputs or the number of connectable modules. In terms of overall system design with respect to its management, control and visualization capabilities is IN/OUT the weakest variant of integration, but due to wide possibilities of creating a concrete implementation of customer-requested features (such as turn off selected power circuits in the building after arming IAS) is a frequently used solution.

(2) Intrusion and hold-up alarm systems as the integration element

Extensive alarm systems are based on the groups of modules that are connected on the bus. These groups include alarm components (motion detectors, opening, glassbreak etc.) and also can include elements of access control system and elements of automation, allowing control of connected non-alarm technology of buildings. Control panel is the central element of the system in which can be implemented functions of access control system or other alarm and non-alarm applications. [12] This control panel in conjunction with SW product ensures communication with the system operator and

the central control and visualization technology building. All elements of the systems - modules are technologically identical, and therefore there is no compatibility issue. Central control and administration here may seem as an advantage and disadvantages at the same time. Failure of the control panel has resulted in malfunctions of most of the connected technologies. Smaller applications can be realized using control panel of IHAS, which generating signals for home automation systems (such as X -10 control of electrical equipment signals transmitted by power lead 230 V).

(3) Automation system as an integration element

Automation systems used to control technology in buildings (lighting, heating, blinds, irrigation, etc.) contain a central control with PLC (Programmable Logic Controller) controllers and can be used also to security object. Modern automation systems use technology systems of intelligent wiring. These are built on the platform of the wire bus to which they are connected sensor (temperature, humidity, buttons, microphone, detectors ...) and action elements (switches, relays, warning device ...). Individual elements of technology of building (lighting, air conditioning, blinds, heating, boiler ...) can then be controlled locally, remotely (GSM, web) or can centrally set timetable for their activation and reciprocal links.

IAS can be connected to the systems of intelligent wiring through a transducer, which ensures two-way transmission of signals between the control panel IAS and the control unit of wiring system, which further ensures links with other technologies in the building. When arming the system after the departure of persons from an object such as might occur to turn off lights, locking doors, turning off selected socket circuits. In the case of intrusion can be programmed central unit for turn on lights in the building, pull blinds etc. In another variant is possible to create a security system on the platform of the system of intelligent wiring without the use of control panels IAS. In this case, the detectors (motion, open, glass break, vibration, etc.) are connected to other sensors to the bus and based on an assessment of their condition control unit run the program - the transmission of messages on alarm receiving centre, activation of warning devices, etc. Such a method of security cannot be certified in accordance with the line of technical standards EN 50131. Smaller applications can be realized with the use of PLC control systems, which are primarily designed to monitor and control of technologies of building, but their inputs / outputs can be connected to the relevant elements of alarm systems.

(4) Software integration

Software (SW) integration methods are based on linking separate applications via a communication bus, and their control, management, visualization are providing software products, which are installed on an external computer (server, client PC) or at unattended control centers equipped with the necessary software. Individual alarm / non- alarm applications can also be connected to the server via the network (LAN, WAN). [13]For simple applications, the PC client is connected to application using a serial interface or USB port. The common element is the user access to particular functions via PC or through mobile devices. Software products to support the integration can be divided into the following groups.

- Software of control panels of alarm systems.
- Software for user administration.
- Visualization software.
- Security software.
- Integration software of systems of buildings.

IV. Aggregated Coefficients of Effectiveness of Protective Capabilities of Intruder and Hold-up Alarm System

Based on the above described coefficients:

- security coefficient KB,
- technical coefficient KT,
- application coefficient KA,
- integration coefficient KI,

will be calculated:

- coefficient of effectiveness of protective capabilities of the the intruder and hold-up alarm systems $\mathbf{K_{PS}}$, or
- coefficient of effectiveness of protective capabilities of the integrated alarm system $\mathbf{K_{IPS}}$ in case of integration multiple systems.

$$K_{PS} = \frac{K_B + K_T + K_A}{3} \qquad (5)$$

Values K_{PS1} to K_{PSN} are calculated for individual types alarm systems in case of integration of multiple types (n) of alarm applications. The resulting coefficient of the protective capability of the integrated alarm system K_{IPS} will be calculated using the following formula. The resulting value will be in the range [1-10].

$$K_{IPS} = \frac{K_{PS1} + K_{PS2,\ldots\ldots\ldots+K_{PSn}}}{n} + \left[10 - \frac{K_{PS1} + K_{PS2,\ldots\ldots\ldots+K_{PSn}}}{n}\right] * \frac{K_I}{10} \qquad (6)$$

Subsequently we compare the calculated coefficients with the efficiency requirements for alarm systems respectively integrated alarm systems. These requirements may be determined for example by the verbal valuation, as shown in the following table.

Table 5. Evaluation of the effectiveness of alarm systems

No.	K_{PS}	K_{IPS}	Evaluation of effectiveness of protective compatibilities
0	[0]	[0-1]	Inconvenient
1	[1-2]	[2-3]	Sufficient
2	[2-4]	[3-4]	Satisfactory
3	[4-6]	[5-6]	Good
4	[6-8]	[7-8]	Very good
5	[8-10]	[9-10]	Excellent

V. Conclusion

The paper presents an original draft of aggregate coefficients, such as the basic starting point for evaluating the effectiveness of alarm systems with the assumption of the possibility of evaluation systems according to project documentation, as well as evaluation systems already installed. The proposed solution is based on an analysis of:

- system and technical requirements, which are intended by series of sector technical standards CSN EN 50 13x, which represent support for the implementation of alarm systems in adequate quality and structure,
- scope of application of the various components of the alarm system in the protected object,
- method of integration when deployed multiple types of alarm applications.

With regard to the assessment of the proposed system or alarm system already installer, using partial coefficients:

- security coefficient K_B,
- technical coefficient K_T,
- application coefficient K_A,
- integration coefficient K_I.

is calculated coefficient of effectiveness of protective capabilities of the alarm systems, K_{PS}, respectively coefficient of effectiveness of protective capabilities of the integrated alarm system K_{IPS} in case of integration multiple systems. Based on the assumption that the designer makes the proper selection of components depending on the security level and class environment, the value (coefficient of the protective capabilities) depends primarily on the application and integration coefficient, i.e., the range of use of system components in the protected object respectively proposed technical way of integration.

The paper presents an example of a method to calculate the coefficient effectiveness of protective capabilities of the intruder and hold-up alarm system (IHAS). Calculation of the same coefficient for other types of alarm applications (CCTV, ACS, SAS) will comply with the requirements the relevant technical standards series IEC 5013x, and comply with the technical objectives of the installation in terms of the type of protection that is provided.

References

[1] UHLÁŘ, J. Technical protection of objects II. Jan. Electrical security systems. 1st edition Prague: Police Academy of the Czech Republic, 2005. 230 p. ISBN 80-7251-189-0. (in Czech).

[2] CSN EN 50131-1 ed.2: 2007. Alarm systems- Intrusion and hold-up alarm systems Part 1: System requirements. (in Czech).

[3] CSN CLC/TS 50398: 2009. Alarm systems- Combined and integrated alarm systems - General requirements. (in Czech).

[4] VALOUCH, Jan. Integrated Alarm Systems. In Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. Series: Communications in Computer and Information Science, Vol. 340, 2012, XVIII. Berlin: Springer Berlin Heidelberg, 2012. Chapter, p. 369 -379. ISBN 978-3-642-35267-9.

[5] VALOUCH, Jan. Integration Alarm Systems. In IJDRBC International Journal of Disastery and Business Continuity. Sandy Bay, Tasmania, Australia: Science & Engineering Research Support Society, November 2012. Vol. 3. p. 21-30. ISSN 2005-4289.

[6] VALOUCH, Jan. Projecting of Security Systems. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 p. (in Czech).

[7] VALOUCH, Jan. Security Assessment of the Object in terms of Alarm system design. In the Science for Population Protection. Lázně Bohdaneč: Ministry of the Interior. Fire Rescue Service of the Czech Republic. Population Protection Institute. Vol. 4. p. 185 - 190. ISSN: 1803-568X.

[8] CSN EN 50131-2-2 Alarm systems - Intrusion and hold-up systems - Part 2-2: Intrusion detectors - Passive infrared detectors.

[9] CSN EN 50131-3 Alarm systems -Intrusion and hold-up alarm systems - Part 3: Control and indicating equipment.

[10] CSN EN 50131-4 Alarm systems - Intrusion and hold-up alarm systems - Part 4: Warning devices.

[11] URBANČOKOVÁ, Hana. PADŮCHOVÁ, Alena. VALOUCH, Jan. ADÁMEK, Milan. The Possibilities os Security Object of Territorial Sejf-Goverment. In Recent Advances in Circuits, Systems and Automatic Control. Series: Recent Advances in Electical Engineering Series, Vol. 27, 2013, XVIII. Budapest, Hungary: WSEAS Press, 2013. p. 366 -370. ISBN 978-960-474-349-0, ISSN 1790-5117.

[12] ŠEVČÍK, Jiří, SVOBODA Petr a PADÚCHOVÁ Alena. Novel Approach to the Video Surveillance System Image Operational Properties Evaluation. In: Recent Advances in Automatic Control, Information and Communications. Vol 19. Valencia, Spain: WSEAS Press, 2013, 174 - 178. ISBN 978-960-474-316-2 ISSN 1790-5117.

[13] SVOBODA Petr, ŠEVČÍK, Jiří a LUKÁŠ, Luděk. The Research of the Use of Training Simulators in the Security Forces In: Recent Advances in Computer Science. 6th WSEAS World Congress: Applied computing Conference (ACC´13), Nanjing.. Istanbul: WSEAS Press, 2013, 180-183. ISBN 978-960-474-354-4. ISSN 1790-5109.

.