Video Surveillance System Functionality Quantification

J. Sevcik, L. Lukas

***Abstract*—** Quantification of Intelligent Video Surveillance System functionality plays significant role in measuring its effectiveness. Moreover, these systems are deployed still more often as a tool for regulation of crime rate around the world. The theory of aggregate coefficients is utilized as a tool for quantification of quality of these systems. The particular functional blocks of the Intelligent Video Surveillance Systems are determined in order to describe its operational functionality. The classification framework is used as a reference for quantification process. The specification of input data format for quantification process is supposed to be the main contribution of the paper. Exact calculation metrics are proposed for the purposes of intelligent video surveillance systems evaluation.

***Keywords*—** Aggregate coefficients, Intelligent Video Surveillance Systems, quality, effectiveness, quantification.

I. Introduction

THE quantitative evaluation of Intruder and Hold-Up Alarm Systems (I&HAS) is an objective of contemporary research related to their effectiveness, efficiency, reliability, quality and optimality [1]. According to technical definitions, effectiveness is dimensionless number that expresses how close to ideal process a process in evaluated system or device runs. Ideal process is 100% effective [2]. Effectiveness of security system then may analogically express how close the real processes are in security system to ideal processes. Ideal processes are understood as processes that completely or in acceptable degree eliminate risks that were identified and against which the security system was designed. For expression of security system effectiveness it is necessary to utilize specific output variables that are created ad hoc for this purpose and their definition is not unambiguous [1]. Particular subsection of I&HAS are Intelligent Video Surveillance Systems, which is essentially more complex as compared with standard I&HAS. It is important to realize that quantity of IVSS applications are growing increasingly in last three decades. Moreover, the technological evolution has influenced all major parts of these systems; therefore the particular gap has arisen between the technological and design possibilities and shape of real installations of IVSS. The first recommendation within IVSS design is to follow instructions formulated by the European Standards related to objective area [3]. IVSS design is in principle the socio-technical issue; therefore it is relatively difficult to realize quantification of particular functional properties of the system in relation to security task which should be fulfilled. The evaluation of IVSS was investigated in several research papers [4]. Although particular ones discussed evaluation of the Image Acquisition process [5], the majority were aimed to evaluation of overall architecture of the system [6], including all functional blocks such as Image Acquisition, Connections, Image Processing, Activity and data management, connections with other systems, the system and data integrity. The empirical approach was chosen as the appropriate method of quantification in case of the aggregated coefficients establishment process. The European normative documents were utilized as a probably most relevant source to define data inputs as well as determination of particular system functional thresholds. Research paper is divided into 5 main parts. Firstly, the whole functional properties of IVSS are described in detail. In second part the determination of aggregate coefficients research method is provided. This method is consequently adapted on functional properties of IVSS. The design of aggregate coefficients of IVSS is provided in next step. In experimental part the application of aggregated coefficients is accomplished. For this purposes an experimental model locations were proposed and utilized for experimental verification of reliability of the solution designed. These general blocks are created by several parts.

II. Functional properties of IVSS

As was mentioned in previous section the definition of particular functional blocks is the necessary process to specify the exact form of data inputs. In this section the detail definition of IVSS functionalities is provided. Nonetheless, firstly is important to specify classification framework, which is related to theory of aggregated coefficients. Classification of IVSS functionality is closely related to classification of I&HAS, following this fact the I&HAS classification framework proposed by Dr. Valouch within the resort project [7] was utilized also in case of IVSS. In Fig.2 are demonstrated bases of proposed classification framework. Theory of aggregate coefficients is based on the empirical assignment of rates, which are multiplied by relevant scales related to them. Scales are then representing importance of particular coefficient within the system. Logical structure of IVSS´s functional properties is formed into three general blocks:

- Video setting,
- System management,
- System security.

Brief description of each is provided in following subsections.

A. Video setting

Probably the most important part of IVSS, especially from the designer point of view. This functional block is created by three divisions:

- Image Acquisition,
- Communication,
- Image Processing.

Image Acquisition together with its processing is denoted as Image Operational Properties.

Recently, both of these are influenced by the System Intelligence, which is realized through wide spectra of Image interpretation Algorithms. The diagram is provided in Fig.3 by reason of better illustration.

The initial functional step of VSS is an Image Acquisition by the system sensing element which in this case is a Surveillance camera. Primary ability of the camera is gathering the Image information which is then transmitted through the communication interface, nonetheless first generations of the IVSS was enhanced by these major functionalities. Contemporary possibilities of the IVSS advanced a lot, mostly because of the convergence between CCTV and the area of Information and Communication Technologies (ICT). Moreover, the applicability of IVSS has been increasing due to these new possibilities. For the purposes of the evaluation we could imagine Surveillance camera as a set of optical elements by which the exposed scene are scanned, whereas the field of view of the camera are depended on following parameters:

- Image sensor format,
- Focal length of lenses.

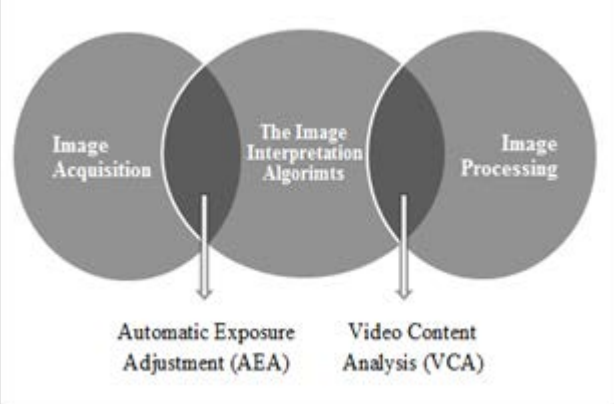

Figure 2: The Image Operational Properties

Field of view (FOV) of camera is in three-dimensional (3D) characterized as a polygon, which could be divided into several segments. Segment marks the area between two particular distances from the camera and serves to express the particular levels of detail in the scene. Specification of concrete parameters is formulated in the European standard [8], where particular metrics are described. Communication expresses the data transfer inside video setting. Continual functionality in operational regime is defined as a requirement on communication within the IVSS; whereas the importance is placed on minimization of signal or message latency, modification or substitution.

B. System management

The user´s interface is very important for data activity within the scope of IVSS. From the system management point of view the system is logically divided into two main parts:

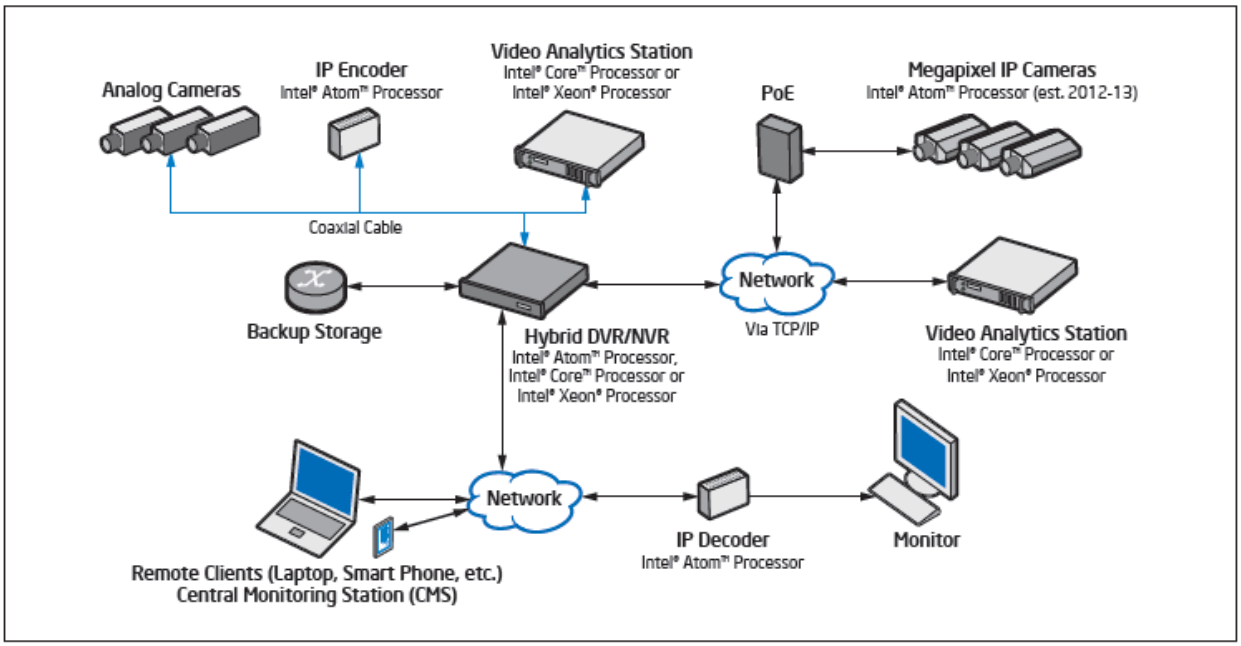

Figure 1: IVSS topology

- The activity management,
- Interfaces.

The audiovisual data and metadata capturing, broadcasting, storage and imaging are realized by the activity management. Moreover, this part also contains operative commands of the IVSS operator and automatically generated reports, which are for instance alarm messages and operator´s alerts.

On the other hand the interfaces serve to connect IVSS with other systems, which are for instance I&HAS, security management systems or other applications out of the security systems scope.

Suitable examples of such events as alarm messages or alerts the operator. Within the data management are frequently encountered with the following examples of metadata:

- data associated with the current image data ,
- identification files generated and stored by describing the activities of the system or operator,
- system data in the form of system status, use of storage media, etc.

Taking Operator response to displayed information is defined in the operational requirements of the system.

Management activities, unlike management of data dedicated to specific real scenarios and responses to them. The resulting events can automatically trigger predefined sequence of activities as part of the system, so by the operator. Events can be triggered by the operator based on the analysis of video or video directly - analytic functions of the system.

Other functional areas of management system VSS are the connections to other systems. These are especially the I&HAS, security control systems, intelligent building systems, access

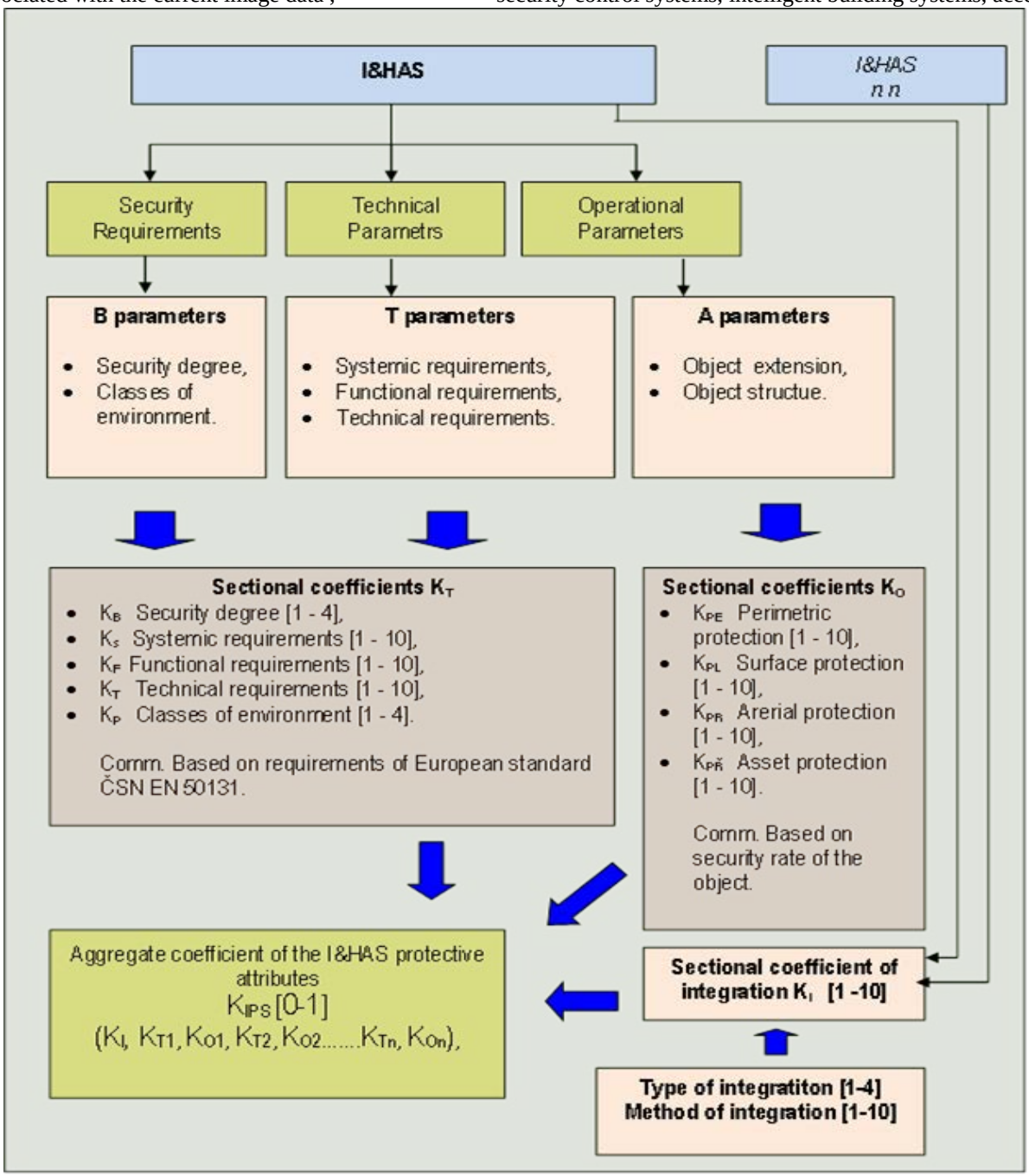

Figure 3: Protective attributes of the I&HAS integrated coefficients design bases

control systems, logistics systems and other systems that can be both the software and the hardware level logically bind the functional possibilities of VSS.

C. System security

Generally, the system security is defined by two functional parts:

- Integrity of the system,
- Data integrity.

Protection of particular components of IVSS and also protection on the system level are included in the integrity of the system. Integrity of the system is realized on next three logical units:

- components, software and connections breakdown detection,
- protection against physical disruption,
- protection against unauthorized access to the system.

Data integrity overlaps second part of IVSS assets and generally is divided into:

- data identification,
- data authentication,
- data protection;

whereas for data identification the exact source, time and date of capture is monitored. The prevention against data modification, deletion, or unauthorized import is realized within the data authentication. The last category, the data protection is similar on the hardware and data layer of the system and it is aimed to prevent against unauthorized access to the database.

III. Security degrees of the system

Unlike the I&HAS security degrees are VSS´s bound to specific components, where in one system there may be multiple subsystems with different security degrees. Security levels explicitly express the system's ability to deal with defined levels of risk (consequences) that can be applied with a certain probability. The required security degrees for each VSS components are specified within the operational requirements design process. Contemporary European standard systems are classified into four security levels.

IV. Aggregate coefficients of IVSS

VSS functionality should be assessed at the level of individual functional blocks, and for the system as a whole. Based on this assumption, the structure was designed and utilized aggregated coefficients. Is used as a template parameter groups and their relations, which have been designed to quantify the function of I & HAS in Chapter 1.1. Within the design of aggregated coefficients is essential to define the methods of classification of input variables, so that the properties of the system at its different levels. In principle, the resulting evaluation factor consists of three sub-parameters , which are:

- **security requirements** (B parameter) , here are determined security level VSS as a whole ,
- **functional requirements** (T parameter) , there is a conformity assessment system functionality required for proper degree of safety and environmental class ,
- **application parameter** (A parameter), here is assessed VSS at the proposal stage , and location of the camera to the shooting scene , and it is evaluated photogrammetric calibration and frame rate of the camera.

A. Determination of B Parameter

The four major security degrees are evaluated within the IVSS system. The form of data input for purposes of this sectional coefficient are supposed to be from interval <0; 4>. Specification of particular security degree is determined European standard [9]. Second element influencing the B parameter is class of environment in which the IVSS components are able to proper operate. It is also specified through four characteristic defined in European standard [9]. The input data format is from interval <0; 4> as well. Role of B parameter is to compare elementary parameters of the system with the thresholds defined by European standards. Security degree and classes of environment requirements fulfillment are influenced by following IVSS functional parameters:

- system components compliance,
- system functionality compliance.

The formal and legislative requirements compliance of the IVSS is represented by its B parameter value.

Security parameter P_B is also decisive for specifying checklists for the calculation of the F parameter.

Table 1: Security parametr

p.n.	Security parameter $\mathbf{P_B}$	Evaluation [1-10]
1	Sec. degree 1 – low risk	2,5
2	Sec. degree 2 – low to medium risk	5
3	Sec. degree 3 – medium to high risk	7,5
4	Sec. degree 4 – high risk	10
5	No security degree coplliance	0

B. Determination of T Parameter

On the basis of security levels are also determined performance requirements VSS at various levels. In the process of determining the T parameter is evaluated by the degree of conformity required functionality with the features of the real system under assessment. Evaluation takes place in the following functional blocks:

- Storing,
- Archiving and backup,
- System Logs,
- Monitoring of interconnection,
- Tamper detection.

European standard [11] lays down different requirements for different security levels. For the implementation of the evaluation should use these checklists.

Table 2: Checklist - Storing

VSS archieving should provide	Security degree			
	1	2	3	4
authentication of each individual image, and image sequence				X
automatically scheduled backup alarm image data				X
backup alarm image data on automatic request			X	X
verify successful backup images			X	X

Table 3: Checklist – Archiving and backup

VSS should be able to	Security degree			
	1	2	3	4
backup data			X	X
keep in case of failure of memory or switch automatically from one storage location to another in the event of failure				X
respond to the activation pulse with a maximum delay		1s	500 ms	250 ms
reproduce an image from memory with a delay after the incident or during the current recording interval			2 s	1 s

Table 4: Checklist - System logs

The system must be recorded along with a timestamp, an event source	The degree of security			
	1	2	3	4
alarm		X	X	X
violation of protection against tampering			X	X
video loss and recovery			X	X
power outage		X	X	X
failure of function and recovery			X	X
error messages displayed to a user				X
system reset, turning off		X	X	X
diagnostic events (system review)				X
export, printing / copying, including identification of the source image, the time range			X	X
login and logout to / from the system on a workstation			X	X
login and logout to / from the system on a workstation			X	X
changes in authorization codes			X	X
control camera functions				X
search and playback images			X	X
manually change the recording parameters			X	X
alarm / alarm restore			X	X
system configuration changes			X	X
date and time settings and time changes with the current new time			X	X

Table 5: Checklist – Monitoring of inteconnection

System have to	The degree of security			
	1	2	3	4
continuously verify the accuracy of links on a regular int. the maximum length			30 s	10 s
try to reconnect with the following number of attempts before the announcement			5	2
failure to notify the operator connection at the latest after			180 s	30 s

Table 6: Checklist – Tamper detection

System should detect	The degree of security			
	1	2	3	4
disruption devices (such as opening or disconnection) defined in the OR			X	X
video loss		X	X	X
change position (orientation) of the sensor device (camera kit)			X	X
intentional blackout or aperture area of interest sensing device			X	X
substitution of any image data from sources, links or processing				X
A significant decrease in image contrast				X

If the parameter T, the number of ranking positions may vary depending on the security level. The largest range of desired functional properties of the systems at the 3rd and 4th grade. In the calculation of the parameter T is evaluated where the percentage level of agreement;

N - total number of scoring functions

Fs - number of functions in accordance with control leaves,

Fn - number of functions in disagreement with control leaves,

Pt - parameter T.

For the calculation of the use of the following equation:

$$P_t = F_s/N * 10 \quad (1)$$

C. Determination of A Parameter

Definition of application coefficients is the most complex task within the IVSS quantification process. The rules designed in two previous steps were relatively parallel to I&HAS classification framework, the A parameter is reasonably characteristic. While the entirely detection criteria is utilized by I&HAS sensor components, in case of IVSS are their sensing function described by more complex object recognition functionality. The main IVSS application requirements are specified in [8]. In chapter 2.1.1 the determination of FOV is provided as well as the operational parameters of cameras. The visualization of FOV is provided in Fig.4. Evaluation of image functional properties,

respectively application properties of IVSS is relatively complex task and it is necessary to simplify input data format for the purposes of aggregate coefficients. I order to utilize quantification of operating requirements of IVSS in sophisticated way, the following three coefficients were proposed:

C_{LOD} - Level of detail compliance coefficient,
C_{OT} - Object of interest trajectory coefficient,
C_{OS} - Object of interest speed coefficient.

C_{LOD} is the coefficient which represents the percentage of compliance between level of detail determined within the operational requirements process and the level of detail of real system camera. The compliance rate is evaluated within each level of detail of camera FOV. The input data format is then from interval <1,10>, where value equal 1 expresses 10% compliance and value equal 10 expresses 100% compliance.

C_{OT} utilizes the geometrical relation between movement vector (orientation) of the object of interest and the axis of camera FOV in particular level of detail; whereas the evaluation is realized always for the most detailed region of camera FOV. A second criterion which has to be fulfilled is the minimal and maximal level of the angle between object orientation axis and the camera FOV axis. It has to be from interval 45° to 90°. Quantification is then realized in interval <1,10>, where the minimal value is represented by 1 and the maximum level of compliance is represented by value 10.

The last coefficient related to A parameter is C_{OS}. The function of this coefficient is to evaluate the frame rate of particular camera of the system. The human beings are assumed in our case. The evaluation is realized in the most detailed FOV segment, where the frame rate between two thresholds is analyzed. The evaluation interval is between 4 and 14 frames per second. For 4 fps the value 1 is assigned for 14 fps value 10 is utilized.

C_{LOD} is evaluated based on the quality of the made document assessment of operational requirements, and it is evaluated whether the agreement between the desired detail of surveillance in the area and the actual state surveillance. Compliance is measured as a percentage and for each level of recognition and separated. It should be noted that the evaluation system can be made for individual security levels. After assessing the conformity we get the following results, see table.7.

Table 7: C_{LOD} data gathering process

Level of detail compliance	The degree of security			
	1	**2**	**3**	**4**
Inspection	0	0	20	60
Identification	0	0	30	80
Recognoscation	0	20	50	90
Observation	50	70	70	95
Detection	60	60	80	90
Monitoring	40	50	70	90

Average surface Sn matching is further evaluated for each step Sn, where n is the weighted degree of security.

Use the following equation then we get C_{LOD}:

$$C_{LOD} = (S_1+S_2+S_3+S_4) /40 \quad (2)$$

On the basis of the value calculated the value of the resulting coefficient will be from the interval <1,10>.

The object of interest trajectory coefficient is used for derivation of its completely different mechanism. First you need to determine the highest possible level of detail that particular camera is able to provide. Furthermore, a 2D projection FOV of the camera and the object being observed interest, including its trajectory. Important in this process is the relationship between the axis and the axis of the camera FOV trajectory of the object of interest, but only in the segment highly detailed recognition. If we crosses axis perpendicular trajectory of the object, we obtain intercept FOV of the camera. The observed parameter is the angle between these two lines. Let's call this angle α. The angle α should be in the range of <45 °, 90 °>. In another case, the primary purpose of monitoring cameras selected object of interest. The resulting coefficient of determination must be based on the following table.

Table 8: C_{OT} coefficient establishment

Angle α[°]	Ctra coefficient value
45	1
50	2
55	3
60	4
65	5
70	6
75	7
80	8
85	9
90	10

Determination of the object of interest speed coefficient in this case is adapted to cases where the object of interest of a human being. Curfew is predefined frame rates, which are defined by the European standard. Determination of the coefficient carried out using the following table evaluates the set frame rate of security cameras.

Table 9: C_{OS} coefficient establishment

FPS value	C_{FPS} coefficient value
5	1
6	2
7	3
8	4
9	5
10	6
11	7

12	8
13	9
14	10

The final calculation of A parameter is made through the following formula:

$$A= (C_{LOD} * C_{OT} * C_{OS}) /3 \quad (3)$$

D. Aggregate coefficient calculation

The final calculation is then performed using three parameters defined in the previous steps. It should be noted that the apparatus is designed to be confirmed by the real tests and on their basis to adjust the level of the individual weights w_n. To calculate the resultant aggregate coefficient VSS the following formula is utilized:

$$AC= (B * w_1) + (T * w_3) + (A * w_3) /3 \quad (4)$$

V. Conclusion

The work related to the IVSS design process is relatively diverse, whereas the variation is especially within the classification of input and output data format. The unique solution of IVSS functional parameters quantification is proposed in this paper, however rather empiric methods were utilized within the data gathering process.

References

[1] Loveček, T., Vaculík, J., Kittel, L.,2012, Qualitative approach to evaluation of critical infrastructure security systems. In: European journal of security and safety, ISSN 1338-6131. - 2012. - Vol. 1, no. 1, online, s. 1-11.: http://www.esecportal.eu/journal/index.php/ejss/article/view/3/2

[2] LOVEČEK T. 2009. Systémy ochrany majetku a možnosti ich kvalitatívneho a kvantitatívneho ohodnotenia : Habilitačná práca. Žilina.

[3] 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. 19. vyd. Valencia, Spain: WSEAS Press, 2013, 174 - 178. ISBN 978-960-474-316-2ISSN 1790-5117. Dostupné z: www.wseas.org

[4] Péter L. Venetianer, Hongli Deng, Performance evaluation of an intelligent video surveillance system – A case study, Computer Vision and Image Understanding, Volume 114, Issue 11, November 2010, Pages 1292-1302, ISSN 1077-3142.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[5] Aldridge JJ994, CCTV Operational Requirements Manual JSDB Publication 17/94, ISBN 1 85893 335 8.

[6] Ra□ty, T.D., "Survey on Contemporary Remote Surveillance Systems for Public Safety," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol.40, no.5, pp.493, 515, Sept. 2010.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.

[7] HROMADA M., a kol. Systém a způsob hodnocení odolnosti kritické infrastruktury/The system and approach to critical infrastructure resilience evaluation, 1. vyd., Ostrava: SPBI, 2014, str. 177, ISBN 978-80-7385-140-8

[8] EN 50 132-7. Alarm system - CCTV surveillance systems for use in security applications - Part 7: Application guidelines. B - 1000 Brussels: Management Centre: Avenue Marnix 17, 2011.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[9] ČSN EN 50132-1. Poplachové systémy: CCTV sledovací systémy pro použití v bezpečnostních aplikacích: Část 1: Systémové požadavky. 1. vyd. Praha, 2010

[10] HROMADA, M., LUKAS L., The Status and Importance of Robustness in the Process of Critical Infrastructure Resilience Evaluation, The 13th annual IEEE Conference on Technologies for Homeland Security (HST '13), held 12-14 November 2013 in Greater Boston, Massachusetts. Pp. 589-594, ISBN 978-1-4799-1533-0

[11] VALOUCH, Jan. Integrated Alarm Systems. In Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity. Series: <http://www.springer.com/series/7899>Communications in Computer and Information Science, Vol. 340, 2012, XVIII.

[12] P. N. Belhumeur, J. P. Hespanha, and D. J.Kriegman, "Eigenfaces vs. Fisherfaces: RecognitionUsing Class Specific Linear Projection," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 711-720, 1997.

[13] Anagnostopoulos, C and et all, License Plate Recognition From Still Image and video Sequences: A Survey in proceedings of IEEE Transactions on Intelligent Transportation Systems. 2008.

[14] A. J. Lipton, H. Fujiyoshi, and R. S. Patil, Moving target classification and tracking from real-time video, in Proc.IEEE Workshop Applications of Computer Vision, 1998, pp. 8–14.

[15] . A. J. Lipton, H. Fujiyoshi, and R. S. Patil, Moving target classification and tracking from real-time video, in Proc.IEEE Workshop Applications of Computer Vision, 1998, pp. 8–14.

[16]

[17] W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.

[18] G. W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IEEE Summer power Meeting, Dallas, TX, June 22–27, 1990, Paper 90 SM 690-0 PWRS.

[19] J. G. Kreifeldt, "An analysis of surface-detected EMG as an amplitude-modulated noise," presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

[20] J. Williams, "Narrow-band analyzer (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.

[21] N. Kawasaki, "Parametric study of thermal and chemical nonequilibrium nozzle flow," M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

[22] J. P. Wilkinson, "Nonlinear resonant circuit devices (Patent style)," U.S. Patent 3 624 12, July 16, 1990.

[23] *IEEE Criteria for Class IE Electric Systems* (Standards style), IEEE Standard 308, 1969.

[24] *Letter Symbols for Quantities*, ANSI Standard Y10.5-1968.

[25] D. Miao, J. Fu, Y. Lu, S. Li, W. Chen: Textureassisted Kinect depth inpainting, IEEE International Symposium on Circuits and Systems (ISCAS), pp.604-607, 2012.E. E. Reber, R. L. Michell, and C. J. Carter, "Oxygen absorption in the Earth's atmosphere," Aerospace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (420-46)-3, Nov. 1988.

[26] Lukas,L., Hruza, P., Research of the information support of management activities. Research report.Brno: VSKE, 2010, 70p

[27] N. A. Razak, M. A. Lubis, M. A. Lumbi and R. B. Mustapha." IT Literacy of Language Teachers in Malaysian Technical Schools". In: „International Journal of Education and Information Technologies". Issue 3, Volume 4, p. 149-156, 2010.

J. Sevcik - was born in 1986. In 2011 completed a master's degree in Security technologies, systems and management at the Tomas Bata University in Zlin, where he attends postgraduate studies. The object of her interest is in the Effective design of the Video Surveillance System and the Security assessment of the environmental conditions influencing the object.