COMMUNICATIONS

COMMUNICATIONS

Libor Hadacek - Tomas Lovecek - Radomir Scurek - Mikael H. L. Zeegers *

ASSESSMENT OF FENCE SYSTEMS USING FUZZY MODELING

The article deals with the use of fuzzy modeling for time estimate of wire fence systems resistance. The resulting time can be used then in quantitative analytical methods for assessing the effectiveness of a technical protection system. The values of the fence system time resistance are very difficult to detect. Neither the technical standards give an exhaustive answer to questions related to time resistance of mechanical barriers. Some experiments were carried out with the aim to determine the time required for penetration of the selected wire fence obstacles. On the basis of the experiment results fuzzy rules were designed allowing, in conjunction with a suitable software tool, precise estimation of the wire fence barriers time resistance.

Keywords: *Fuzzy modeling, fence system, resistance, perimeter protection.*

1. Technical standard requirements for breaching resistance of mechanical barriers

Currently, there are not comprehensively defined times regarding the breach of mechanical barriers for all categories of tools. For example, the standard for opening fillings (EN 1627), such as windows, doors, grilles or shutters, does not state the resistance time corresponding to the categories of all tools, but only for some of them. The standard designed for safety storage units (EN 1143-1) uses more complex approach where the time of breach resistance of appropriate security class is dependent on the intended use of tools, and thus it can be calculated for many tools categories. In the case of breakthrough time of security plastic film and security glazing the standards do not specify time units, but only the number of hits with different instruments to which a relevant passive element should resist (e.g. EN 356). In the case of building constructions by the means of perimeter protection no technical standard defines their breakthrough resistance [1].

It cannot be determined, on the basis of technical standards, their breach resistance expressed in time units. It follows that for many passive protection elements can only verify / certify their conformity of these elements properties. It is, therefore, necessary to search for new ways how to acquire these resistance time data in practice.

2. Description and results of the experiment measuring the breach resistance of wire fence systems

The company F.S.C. BEZPECNOSTNI PORADENSTVI, a.s. in cooperation with the University of Zilina implemented the project "Methodology for physical protection assessment of critical infrastructure elements against terrorist attack and other types of attacks" in the period 2012-2013. The project was financially supported by the Programme Prevention, preparedness and consequence management of terrorism and other security related risks of the European Commission - DG freedom, justice and security.

One of the project objectives was to develop a methodology for testing barriers which were installed at the perimeter and to answer the question concerning the attacker´s delay during the breach of a wire fence system made from interlocking or welding of individual structural wires. It makes sense to deal with the breach resistance only in the case if the surrounding measures represent for a potential attacker a larger obstacle than the penetration fence.

Proposed structure of the groups and tools selection into each group was inspired by the technical standard [2]. The choice of instruments was selected from the catalogue of tools [3] which contained 83 pieces of tools. When selecting the typical representatives of tools, the following issues were monitored: availability, method of operation, noise generated by their use, aggressive action, the possibility of further use when the attacker approaches the target. Selected instruments were categorized into 5 groups. The final list of instruments is given in Table 1 [4].

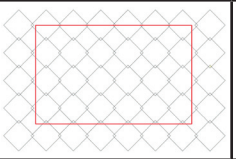
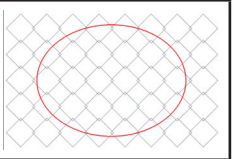
* [1]**Libor Hadacek,** [2]**Tomas Lovecek,** [3]**Radomir Scurek,** [4]**Mikael H. L. Zeegers**
[1]Depatment of Security Services, Faculty of Safety Engineering, VSB Technical University of Ostrava, Czech Republic
[2]Department of Security Management, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Depatment of Security Services, Faculty of Safety Engineering, VSB Technical University of Ostrava, Czech Republic
[4]Mikael H. L. Zeegers, Zeegers Management Security Bureau, Kanne-Riemst, Belgium
E-mail: libor.hadacek.st@vsb.cz

Overview of the tools in groups before tests performing Table 1

Group	Group Identification	Tool		
1	Manpower	Crowbar	Rock	Manpower
2	Mechanical tools	Handsaw	Pliers	Hammer
3	Lever mechanical tools	Lever shears	Car jack (screw)	Clamp
4	Cordless power tools	Cordless grinder	Cordless saw	Cordless shears
5	Electric or gas tools	Handheld gas burner	230 V grinder 125mm	230 V – jigsaw

Four types of fencing were tested. Fence component can be described by the strength of the used wire and the area of netting mesh. The aim of the tests for the test engineer was to make the hole for crawling through the fence component which was set up in accordance with the technical standards for the opening fillings [2], see Table 2. The test engineers, working on the tests, were well experienced in fencing systems testing and they had experience in the use of given tools.

Description of the holes for crawling through Table 2

	Rectangle	Ellipse
Shape		
Dimensions	400 mm ± 2 mm x 250 mm	400 mm ± 2 mm x 300 mm

For the methodology verification 60 breakthrough resistance tests were carried out. It means that 15 selected tools were used for all 4 types of fencing. The overview of fence characteristics is given in Table 3. Fence components were produced from galvanized steel wire.

Used tools had different effectiveness on the tested samples. The measured values, therefore, do not lie exactly on the straight line. For the estimation of searched dependence parameters linear regression analysis was used. The course of time resistance of fence depending on the tools used and the values of the regression analysis are shown in Fig. 1.

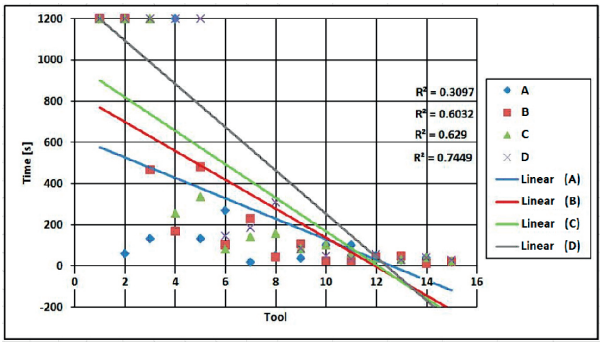


Fig. 1 Linear regression analysis of time resistance depending on verified samples on the used tool

The results proved that decision to divide tools into five groups was correct. Tools groups were modified according to the test results. Negative symptom was the noise made by some tool, which limited the possibilities of its use for fence breach.

The methodology evaluation and results were discussed with the chairman of the technical committee CEN / TC388 perimeter protection. The chairman of the technical commission accepted the proposal for a methodology as a working paper which the technical committee would deal with.

The classification of tools into groups was adjusted on the basis of test results. Tools were arranged in descending order by the sum of times of the breach resistance of the tested fence components and they were assigned with a coefficient according to interrelations (1)

$$c_i = 5000 - \sum (A_r, B_r, C_r, D_r). \quad (1)$$

The value of tool coefficient is a dimensionless number where (A_r, B_r, C_r, D_r) are values for time resistance of tool dependence in test samples and i is the tool serial number.

3. Proposal for the assessment of fencing systems using fuzzy modeling

For the determination of the breach resistance of similar mechanical barriers in a non-destructive manner it is appropriate to create a model. The breach resistance of a fence component can be described as a socio-technical system created by man – by a tool – by a mechanical barrier. The influence of the external environment is not taken into consideration in the model, whereas the experimental tests were carried out on a summer day in sunny weather when the air temperature did not exceed 30°C.

The fence resistance can be expressed by relation (2)

$$R = f(O,F,T) \quad (2)$$

R – resistance of fence component
O – offender
F – fence
T – tool.

An attacker may be described as a someone who is motivated for his action, has the necessary knowledge and skills for tool using and has adequate physical skills to carry out the attack (relation 3)

$$O = f(M,K,P) \quad (3)$$

O – offender
M – motivation
K – knowledge of tool use
P – physical skills.

The fence basic data describes its structure characterized by mesh size and wire diameter (relation 4).

$$F = f(A,D) \quad (4)$$

F – fence
A – meshes size
D – wire diameter.

The used tool is identified by a coefficient (relation 5) which was determined by the results of experimental use and expresses the total success time of the tool used by testing samples.

$$T = c \quad (5)$$

T – tool
c – tool coefficient.

In the test, the attackers were represented by test engineers who had many years of experience with tested fences and used tools. Their motivation was to verify in person how durable the fences, which they use each day, were. The fence resistance function for fuzzy model creations was simplified to relationship (6).

$$R = f(F,T) \quad (6)$$

and which has, after the replacement, the final form according to relation (7)

$$R = f(A,D,c). \quad (7)$$

For creation of a fuzzy model properties of approximate reasoning were used, as presented in [5] and [6]. The general fuzzy controller, shown in Fig. 2, is formed on the basis of knowledge, inferential mechanism and defuzzification.

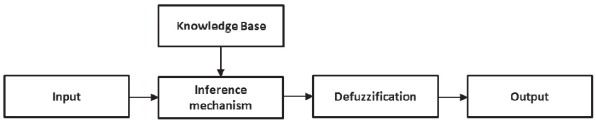


Fig. 2 General fuzzy controller

Knowledge base consists of a fuzzy model using approximate reasoning which in the real process describes the relationship between the conditions, observation and conclusion using the IF-THEN rules. Linguistic variable represents the properties of the input variables, e.g. "small", "large", etc. A function value can be assigned to linguistic variables in the context of the problem which should be solved. The context indicates the range limit of minimum and maximum of function values. One rule expresses local knowledge about the relationship among conditions, observation and conclusion. A set of rules creates general knowledge. IF-THEN rules may have a form, i.e.:

Condition: IF the speed is *medium* AND the obstacle is *close* THEN intervention - *hit the brake.*
Observation: speed *slow* AND obstacle is *close.*
Conclusion: intervention - *hit the brake.*

The conclusion can be made by comparing the observation with the input condition.

The inference mechanism consists of logical deduction based on the observation perception. The resulting output fuzzy set enters into defuzzification. Defuzzification method of evaluation expressions DEE (Defuzzificaton of Evaluative Expressions) gives on the output a value which represents the size of any intervention. Type "small" means that the fuzzy set corresponding to the shape of the extension of pure evaluation term with atomic term like a small and similarly type "great". If the fuzzy set is "medium", the defuzzification method is method COG (relation 8)

$$COG(A) = \frac{\sum_{i=1}^{n} A(u_1) \cdot u_1}{\sum_{i=1}^{n} A(u_1)} \quad (8)$$

$COG(A)$ – focus of fuzzy set A
$A(u_i)$ – membership function
u_i – value.

It follows that it is sufficient to know the regulatory strategy and accordingly it is possible to design a fuzzy controller. For the application of fuzzy control is used following approach:

1) There are set the dependent and independent variables (intervence).
2) We decide on the type of fuzzy controller and method of approximate deduction.
3) We assemble the knowledge base - based on expert information, by which is described control strategy by means of language descriptions.
4) For all variables there is determined the context in which it is specified interval of meaningful values, of which the variables can take.

On the basis of the procedure there was determined form of function rule for determination of the breakthrough resistance (relation 9).

$$R_n = IF\ X_1\ is\ A_n\ AND\ X_2\ is\ A_n\ AND\ X_3\ is\ A_n\ THEN\ Y\ is\ B_n \quad (9)$$

R_n – resistence of fence component/panel
X_1 – input variables independently
A_n – characteristics independently variables
Y – output dependent variables
B_n – characteristics dependent variables.

For the verbal description of the wire fence resistance quantitative characteristics of the fence and tools were used. Distribution of the values into the qualitative groups was carried out uniformly in the range of possible values. The overlap of individual groups did not allow creating sharp intervals which could border each group. This causes inaccurate values located near the left or right boundary of the interval. Distribution of independent and dependent variables in the qualitative groups of linguistic variables is shown in Table 3.

Distribution of values and assigning linguistic variables Table 3

Input value	Indication	Description	Spread	Tool	Indication	*c*
Mesh [mm^2]	MS	Small	0-3 500	Rock	VMU	200
	MM	Medium	2 500-6 500	Manpower	VMU	1 342
	MB	Big	5 500-9 500	car jack (screw)	MU	2 002
	MVB	Very Big	8 500-12 000	Crowbar	MU	2 178
Wire [mm]	WS	Small	0-2.8	Clamp	MU	2 854
	WM	Medium	2.2-5.2	Hammer	SU	4 405
	WB	Big	4.7-7.8	Handsaw	SU	4 429
	WVB	Very Big	7.2-10	Pliers	SU	4 446
Tool	TVS	Very Small Effect	0-1 400	handheld gas burner	VU	4 692
	TS	Small Effectivness	900-2 800	cordless saw	VU	4 730
	TM	Medium Efficiency	2 200-4 200	cordless shears	VU	4 782
	TB	Big Efficiency	3 600-5 000	lever scissors	VU	4 812
Output value	**Indication**	**Description**	**Spread**	230V - grinder 125mm	VU	4 869
Resistance [min]	RS	Small	0-3	cordless grinder	VU	4 874
	RM	Medium	2-5	230V – jigsaw	VU	4 914
	RB	Big	4.6-20			

Overview of IF-THEN rules Table 4

Rule Num.	IF			THEN
	Mesh $X_1 = A_n$	Wire $X_2 = A_n$	Tool $X_3 = A_n$	Resistance $Y=B_n$
1	if mesh is MS	and wire is WM	and tool is TVS	then resistance is RB
2	if mesh is MS	and wire is WM	and tool is TS	then resistance is RM
3	if mesh is MS	and wire is WM	and tool is TM	then resistance is RM
4	if mesh is MS	and wire is WM	and tool is TB	then resistance is RS
5	if mesh is MM	and wire is WM	and tool is TVS	then resistance is RB
6	if mesh is MM	and wire is WM	and tool is TS	then resistance is RM
7	if mesh is MM	and wire is WM	and tool is TM	then resistance is RM
8	if mesh is MM	and wire is WM	and tool is TB	then resistance is RS
9	if mesh is MM	and wire is WB	and tool is TVS	then resistance is RB
10	if mesh is MM	and wire is WB	and tool is TS	then resistance is RM
11	if mesh is MM	and wire is WB	and tool is TM	then resistance is RM
12	if mesh is MM	and wire is WB	and tool is TB	then resistance is RS
13	if mesh is MVB	and wire is WVB	and tool is TVS	then resistance is RB
14	if mesh is MVB	and wire is WVB	and tool is TS	then resistance is RB
15	if mesh is MVB	and wire is WVB	and tool is TM	then resistance is RB
16	if mesh is MVB	and wire is WVB	and tool is TB	then resistance is RS

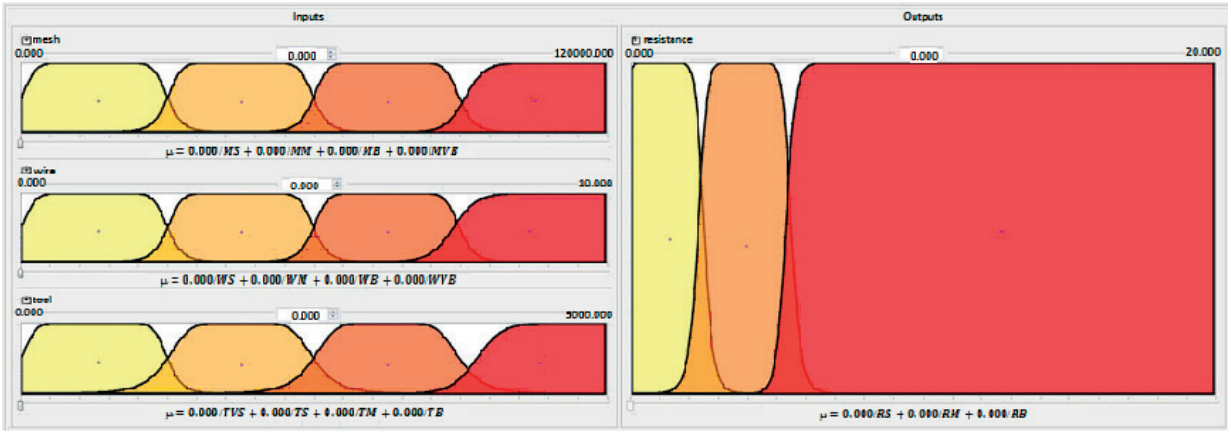


Fig. 3 Distribution of range of values into qualitative groups

Using the general rule set out in relation 9, the knowledge base was created. Based on a combination of number of input variables, 64 rules are needed to be able to create the model. According to the result of the measurement the model was created using 16 fundamental rules. The list of rules, which make the knowledge base is shown in Table 4.

The software tool „qtfuzzylite-4.0b1401 fuzzylite-4.0b1401" was used for processing rules and model creation [7]. There is a print screen of the software desktop in Fig. 3. On the left side are the input variables and on the right side are deducted values of the dependent variable.

The resulting model allows qualified determination of the time resistance level for a wire fences on the strength from 2.5 mm to 8 mm, the mesh size from 2 574 mm^2 to 11 000 mm^2 and when using a defined set of tools. The results show the information about the level of result in qualitative resistance groups.

The accuracy of the fuzzy model is evaluated as the ratio of the values assigned to the resistance classes from measurements and values included in resistance classes in the model. Due to the nonlinearity of values, as is apparent from Fig. 1, the theoretical accuracy of the model is 92%. The accuracy of the model with respect to the values of the measurement is 88%. The accuracy of the model for different types of tested fencing samples is for type A = 80%, type B = 93% type C = 80% type D = 100%.

For example, for a fence, wherein the mesh size is 50x80 mm, wire thickness is 6 mm and the test is done with the tools from group 3, it is possible, when using the model described, to obtain the objectivized values of breakthrough resistance. Case study results are presented in Table 5.

The evaluated sample, due to its characteristics, belongs to the fence group "C". The obtained results are accurate to within 80% to 88%. In the color-coded columns are values of membership function of the results to the group of breakthrough resistance.

The proposed procedure described in this article enables to designers of security systems to refine the calculations relating attacker´s delay, for example, by using the instrument EASI (Estimate of Adversary Sequence Interruption) [8] and [9]. EASI method evaluates the probability of interruption of attack depending on the level and range of perimeter, sheathing and object protection, place of using detection systems, the quality of communication means and the ability of fast-deployment unit to take up defensive positions.

4. Acknowledgements

This paper is a part of the Methodology for physical protection assessment of critical infrastructure elements against terrorist attack and other types of attacks. The project has been co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and Other Security-related Risks Programme of the European Union. This document reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Case study results

Table 5

	Test sample	*c*	Estimated time [min]	Degree of membership to the set		
Group	Tool			<2	2-5	5<
3	Handsaw	4 429	1.34	1.00	0.01	0.00
	Pair of pliers	4 446	1.33	1.00	0.01	0.00
	Hand gas incisor/cutter	4 692	1.30	1.00	0.01	0.00

References

[1] KITTEL, L., LOVECEK, T.: Passive Protection Elements Breach Resistance Modeling, *Communications - Scientific Letters of the University of Zilina*, 2011, ISSN 1335-4205.

[2] CSN EN 1627 *Pedestrian Door sets, Windows, Curtain Walling, Grilles and Shutters - Burglar Resistance - Requirements and Classification (in Czech)*, Praha, 2012

[3] LOVECEK, T., REITSPIS, J.: *Design and Evaluation of Objects System Protection – Ist ed. (in Slovak)*, Zilinska univerzita, 281 p., 2011, ISBN 978-80-554-0457-8.

[4] HADACEK, L. et al: *Methodology for Testing Passive Barriers Resistance*, F.S.C. BEZPECTNOSTNI PORADENSTVI, a.s., Ostrava, 2013

[5] ZADEH, L. A.: *The Concept of a Linguistic Variable and its Application to Approximate Reasoning - I.* 1975. On-line: http://www.cs.berkeley.edu/~zadeh/ papers/ The%20 Concept% 20of 20a%20Linguistic%20Variable%20and%20its%20Applications% 20to%20 Approximate%20Reasoning%20I-1975.pdf

[6] NOVAK, V., KNYBEL, J.: *Fuzzy Modeling (in Czech)*, Ostravska univerzita, Ostrava, 2005

[7] RADA-VILELA, J.: *Fuzzylite: A Fuzzy Logic Control Library,* 2014. On-line: http://www.fuzzylite.com.

[8] GARCIA, M. L.: *The Design and Evaluation of Physical Protection Systems*, 2nd ed., Sandia National Laboratories, 2007, ISBN 10: 0-7506-8352.

[9] LOVECEK, T., RISTVEJ, J., SIMAK, L.: Critical Infrastructure Protection Systems Effectiveness Evaluation. *J. of Homeland Security and Emergency Management,* 2010, vol. 7, No. 1, 2010, ISSN 1547-7355.

Kamil Boc - Dagmar Vidrikova - Zoran Cekerevac - Jan Misik *

PROPOSAL FOR INCREASE OF BURGLAR RESISTANCE OF COMMERCIALLY MANUFACTURED MOTOR VEHICLE DOORS

In many cases the level of personal protection especially during transportation by personal motor vehicles is dependent on burglar resistance of used car body materials. Currently commercially manufactured personal motor vehicles are modified by insertion offiller materials of high density (steel plates inserted into doors, steel reinforcements of vehicle floors). This approach causes not only increase in financial costs for procurement of such modified (armoured) vehicle, but also changes its driving characteristics. Particularly its financial cost affects its accessibility to wide public. Several cases of use of small firearms against the occupants of commercially manufactured personal motor vehicles have been investigated in recent years. The results of such attacks were casualties or grievous bodily harm. Considered materials were experimentally tested for the purpose of increasing burglar resistance mainly of commercially manufactured motor vehicle doors and increase of their burglar resistance against shots from small firearms. The result of experiments that were carried out was the recommendation for reinforcement of car body doors of personal motor vehicles using molten polycarbonate materials. The thickness of 24 mm resulted in such increase of door burglar resistance that used small firearm ammunition could not penetrate this barrier.

Keywords: *Person and property protection, security, burglar resistance, bullet, ammunition, reinforced, personal motor vehicle, self-loading firearm.*

1. Introduction

State of protection of persons and property level follows development of external and internal security environment in which they operate. An important indicator of security or risk level is criminality, especially the violent crime. Democratization of firearm ownership created relatively new phenomenon of security risk which until now correlated mainly with contracted attacks focused on lives and health of risk groups of persons (e.g. important political officials, members of the Government or Justice, ambassadors, members of criminal organizations, etc.). In recent period, relatives of risk group members, transporters of cash or valuables and ordinary citizens have also become targets of contracted violent attacks. Potential victims of assaults with weapon become most vulnerable mainly during transportation by motor vehicles. This status results from the nature of utilization of motor vehicle transportation. Potential victims are limited then not only by road infrastructure, but also by internal space of the vehicle which impedes their defense. Relying on passive protection elements of vehicles is possible only in vehicles in which special modifications were carried out, enhancing their burglar resistance against attacks utilizing firearms. Vehicles reinforced, for example by armor, provide high level of protection to their crew. Commercially produced vehicles are reinforced [1]. These are able to maintain the original technical and driving characteristics after modification. High cost of said types of personal motor vehicles, as well as the modifications, significantly lowers their availability to wider public (average price of reinforced personal motor vehicle moves around 200 000 €). For this reason, the target customers of modified (armoured) vehicles are mainly politicians, ambassadors, entrepreneurs or bosses of criminal organizations. Other concerned groups of persons are insufficiently protected against attacks with firearms from the viewpoint of burglar resistance of commercially used vehicles.

2. Problem description

Currently most of providers of personal motor vehicles reinforcement prefer steel sheets which provide high level

* [1]Kamil Boc, [2]Dagmar Vidrikova, [3]Zoran Cekerevac, [4]Jan Misik
[1]Department of Security Management, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Technical Sciences and Informatics, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Faculty of Business and Industrial Management, Union University Belgrade, Serbia
[4]Department of Security Management, Faculty of Security Engineering, University of Zilina, Slovakia
E-mail: Kamil.Boc@fbi.uniza.sk

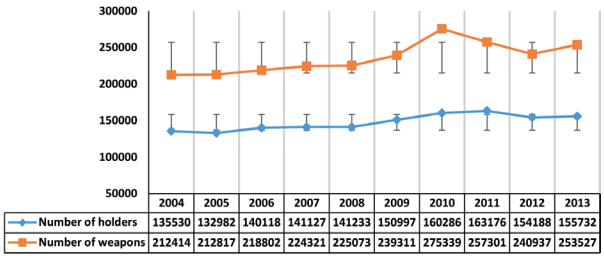
Euronorm Standard For Security Glazing [6] Table 1

Euronorm Standard For Security Glazing								
Class	***Weapon***	***Calibre***	***Type***	***Weight (g)***	***Range (m)***	***Velocity (m/s)***	***Impact Energy***	***Shots***
BR1	Handgun/Rifle	.22 LR	LB/RN	2.6 ± 0.1	10.00 ± 0.5	360 ± 10	170 J	3
BR2	Handgun	9x19mm Parabellum	FJ/RN/SC	8,0 ± 0.1	5.00 ± 0.5	400 ± 10	640 J	3
BR3	Handgun	.357 Magnum	FJ/CB/SC	10.2 ± 0.1	5.00 ± 0.5	430 ± 10	940 J	3
BR4	Handgun	.44 Magnum	FJ/FN/SC	15.6 ± 0.1	5.00 ± 0.5	440 ± 10	1510 J	3
BR5	Rifle	5.56x45mm NATO	FJ/PB/SCP	4,0 ± 0.1	10.00 ± 0.5	950 ± 10	1800 J	3
BR6	Rifle	7.62x51mm NATO	FJ/PB/SC	9.5 ± 0.1	10.00 ± 0.5	830 ± 10	3270 J	3
BR7	Rifle	7.62x51mm NATO	FJ/PB/HC	9.8 ± 0.1	10.00 ± 0.5	820 ± 10	3290 J	3

LB - Lead Bullet *FJ - Full Metal Jacket* *FN - Flat Nose*
RN - Round Nose *CB - Cone Bullet* *PB - Pointed Bullet*
SC - Soft Core (lead) *SCP - Soft Core (lead) & Steel Penetrator* *HC - Hard core*

of burglar resistance against effects of firearms due to their characteristics. Disadvantages of their use lie in increased mass of vehicle and related modification of its construction (necessary above limit modifications of motor unit, construction of vehicle, suspension setup, etc.). International ballistic standards (e. g., EN 1063 - Glass in building. Security glazing. Testing and classification of resistance against bullet attack, EN 1522 - Windows, doors, shutters and blinds. Bullet resistance. Requirements and classification, EN 1523 - Windows, doors, shutters and blinds. Bullet resistance. Test method, German ballistic standard DIN 52 290) are applied to increase burglar resistance of commercially produced vehicles. These norms set seven classes of vehicle resistance against attacks mounted by different types of weapons (Table 1) [2 - 5].

Burglar resistance of commercially produced personal motor vehicles available in Slovakia became object of our experimental examination within VEGA project No. 1/098/11 Model of Integrated Security System Optimization Framework for Protection of Specific Objects Realised by Means of Expert System. The goal was to ascertain level of burglar resistance especially of vehicle doors which belong to critical parts of chassis, and propose means for its improvement [7]. Criteria of the proposal were affordability of the proposed modifications, minimal interference with vehicle construction and maintaining of its mass to exclude negative change of its technical and driving characteristics (e. g. mass changes up to 65% of original vehicle mass after modification). A self-loading handgun was selected for the experiment according to ballistic standards. Its s selection was based on availability and legality of its ownership. Dynamic development of number of holders and registered weapons in SR in recent years was taken into account (Fig. 1) [8 and 9].



	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Number of holders	135530	132982	140118	141127	141233	150997	160286	163176	154188	155732
Number of weapons	212414	212817	218802	224321	225073	239311	275339	257301	240937	253527

Fig. 1 Development of holders and registered weapons count in the Slovak Republic in the years 2004-2013 including standard deviation, trend line and reliability equation R^2 [10].

According to statements of experts from Police Force and firearm dealers, the prevailing interest of holders of firearm licences lies mainly in self-loading handguns.

3. Methodology of experiment

Input data necessary for performance of the experiment were acquired within the pilot project. During its performance, burglar resistance of chassis of commercially produced motor vehicles was tested, specifically the door of personal motor vehicle (hereinafter "test sample") available at Slovak market. All accessories (glass, locking mechanism, electronics, etc.) were removed from the test sample before the main testing. Methods

of the examination within the pilot project, as well as the main experiment, were compliant with norm EN 1063 [2].

3.1 Pilot project

The pilot project was carried out in two stages. During the first stage, the burglar resistance of non-reinforced door was tested. During the second stage the door was reinforced by rock wool filling.

The test device consisted of a solid wooden frame on which the test sample (automobile door) was mounted. The mounting of test sample in frame:

- matches the standard car door mounting,
- distance from wall stopping the shots was 260 mm,
- distance from muzzle was 10 000 mm,
- height from ground level was 690 mm,
- perpendicular to the direction of shots,
- total target area was at minimum 440 mm x 440 mm,
- selection of necessary mounting pressure to ensure the door edges did not move during the test, but also not to cause tension which could influence the test results [2].

Fragments of the shots or sheet metal loose from the test sample were stopped by the wall placed behind the test sample. The wall consisted of masonry blocks made of autoclaved aerated concrete (compliant with norm EN 771-4, category 1) [11] arranged in two rows, each four pieces high. The masonry blocks were set in distance of 260 mm from the test sample. Height of the wall for stopping of shots and their fragments was 996 mm, width from the front side 599 mm, width from the side 750 mm. The scattering of shots or sheet metal fragments was mapped by the control paper. Control paper consisted of white paper with density of 110 g/m2. It was attached to the wall for stopping shots in vertical position, 320 mm behind the test sample. Its free surface was at least 440 mm x 440 mm, matching the target surface [3].

Ballistic testing device

Ballistic testing device was a self-loading firearm from Glock which belongs to the most widespread and most used types. Based on the selected type of weapon we focused on resistance class BR2. Technical parameters of used firearm and ammunition are listed in Table 2.

Rock wool Nobasil, type MPN of dimensions 1000 x 500 x 50.615 mm was used to reinforce the test sample. Process according to standard EN AW 6106 was followed for measuring metal sheet characteristics (Table 3) [12].

Technical parameters of used types of ammunition and weapon in pilot project [6] Table 2

Brand		**Glock**
Model		19
Produced in		2006
Calibre		9x19 mm
Length (frame)		174 mm
Height with magazine		127 mm
Width		30 mm
Barrel	Sight	153 mm
	Length	102 mm
	Profile	Clockwise
	Grooves	6
Magazine capacity		15
Weight	no magazine	595 g
	empty magazine	70 g
	full magazine	225
Muzzle velocity V_0		350 ms^{-1}
Shot energy E_0		490 J
Trigger travel distance		12.5 mm
Trigger pull weight		2.0 kg

Pilot project		**9mm LUGER Magtech**	**9mm LUGER Lapua Cepp Super FMJ**	**RL 124 GRS FMJ**	**RL 124 GRS FMJ lead**
Producer		Magtech	Lapua	Not listed	
Type		FMC	FMJ		
Material	case	CuZn (brass)			
	bullet	Lead core covered by metal jacket			
Shot weight		7.45g (115grs)	7.80g (120grs)	7.95g (124 grs)	9.83g (150 grs)
Primer		Boxer		Not listed	
Shot speed v_0		346 ms^{-1}	360 ms^{-1}	350 ms^{-1}	
Shot energy E_0		446 J	506 J	487 J	602 J

Technical parameters of test sample metal sheet [6] Table 3

Thickness (mm)	Width (mm)	Length (mm)	Weight (g)	Force (kN)	Rigidity (Nmm^2)	Length		Ductility (%)
						before	after	
.9	49	500	139.2	12.31	279.1	400	476	19

Calculation of impact kinetic energy E_d was based on following formula

$$E_d = \frac{1}{2} m_q \cdot v_d^2 \quad [\mathrm{J}] \tag{1}$$

where vd – impact speed of shot [ms^{-1}] and mq – weight of shot [kg].

Mathematic model according to DeMarre was used for calculation of limit impact speed which applies to piercing of armour by armour-piercing shot [13]. It was assumed that all impact kinetic energy of the shot Ed should be consumed when piercing the sheet metal. Based on this assumption, the impact speed may be considered equal to limit speed (vd = vlim). For calculation of limit impact speed v_{lim} following empiric relationship was derived:

$$v_{\mathrm{lim}} = K \cdot \frac{d^{\alpha}}{m_q^{\beta}} \cdot s^{\gamma} \left[ms^{-1} \right] \tag{2}$$

where v_{lim} - limit impact speed of the shot [ms^{-1}], d - shot calibre [dm], m_q - shot weight [kg], K - penetration force constant and s - thickness of penetrated material [dm].

Based on shooting tests, several authors determined values of coefficients α, β, γ demonstrated in Table 4 [14 and 15].

Values of coefficients α, β, γ determined by experiments [6 and 16] Table 4

Coefficient	α	β	γ
Euler	1.0	1/2	1/2
Noble	1/2	1/2	1.0
Krupp laboratory	5/6	1/2	1/3
DeMarre	.75	1/2	.7

Following formula in DeMarre's form was used for determination of shot penetration:

$$v_{\mathrm{lim}} = K \cdot \frac{d^{0,75}}{m_q^{0,5}} \cdot s^{0,7\gamma} \left[ms^{-1} \right] \tag{3}$$

Characteristics of the penetration of the test sample material are determined by penetration force constant *K*. Its value was set by the authors for purpose of this project empirically at K=2400. Calculation of values of impact kinetic energy and limit impact speed of used shots for overcoming the resistance of the sheet metal (penetration) are listed in Table 5.

Calculated values of impact kinetic energy and limit impact speed of used shots for penetrating the test sample during pilot project [6] Table 5

Brand	Ed (J)	V_{lim} (ms^{-1})
MAGTECH	445.94	168.96
LAPUA CEPP SUPER	505.44	165.13
Reloaded RL 124 GRS	486.93	163.56

3.2 Main experiment

Main experiment followed upon the results of the pilot project. Its goal was to verify the burglar resistance of test sample which was reinforced by cast polycarbonate. Testing device was similar to the one used in the pilot project. Ballistic testing device was replaced by handheld self-reloading Glock, model 19, made in 2012. Relevant technical parameters are similar to the technical parameters of weapon listed in Table 2. For the purpose of reaching higher penetration of the shot, 4 types of ammunition were used. Their technical parameters are listed in Table 6. The shooting distance was decreased to 5 m [17].

Technical parameters of used ammunition [6] Table 6

Main experiment		9mm LUGER ZVS	9mm LUGER Subsonic	9mm LUGER	Blazer 9mm LUGER
Producer		ZVS Holding	Sellier & Bellot ČR		FCC USA
Type		FMJ RN	FMJ	JHP	AL
Material	case	CuZn	CuZn 30	CuZn 10	AL
	bullet	Lead core, full metal		Lead core, half metal	Lead core, full metal
Bullet weight		7.45g (115grs)	9.70g (150grs)	7.50g (115grs)	7.45g (115grs)
Primer		Boxer, without Hg	Berdan 4.5mm		xxxx
Speed v_0		360 ms^{-1}	305 ms^{-1}	377 ms^{-1}	349 ms^{-1}
Energy E_0		518 J	451 J	533 J	454 J

Cast polycarbonate of 4 mm thickness was used for reinforcement of the test sample. Reinforcement of the test sample was done by connecting six polycarbonate boards of dimensions 510 mm x 510 mm x 24 mm. Impact kinetic energy of shot E_d was calculated according to equation (1). For calculation of limit impact speed of shot v_{lim}, calculation according to equation (2) was used. To determine the penetration force of shot, the formula in DeMarre's form was applied. Calculation of values of kinetic energy and limit impact speed of used shots for overcoming of sheet metal resistance is listed in Table 7 [17].

Calculation of values of impact kinetic energy and limit impact speed of used shots for penetration of reinforced test sample [6] Table 7

Brand	E_d *(J)*	V_{lim} *(ms^{-1})*
9mm LUGER ZVS	482.76	1666.05
9mm LUGER Subsonic	451.17	1513.03
9mm LUGER	532.98	1346.37
Blazer 9mm LUGER	453.71	1726.45

The theoretical results imply that the limit impact speed necessary for penetration of the reinforced test sample (of thickness s = 0.249 dm) is several times higher than the muzzle velocity V_0 of used ammunition.

4. Results of experimental testing

Results of burglar resistance (with and without reinforcement by rock wool) which were measured by perpendicular shooting of the test sample from 10 m by different types of ammunition within the pilot project are listed in Table 8 [6].

Using rock wool, no verifiable or relevant results were acquired which could be utilized to increase burglar resistance of the test sample. For this purpose, the reinforcement was resolved using a set of six 24mm thick polycarbonate boards within the main experiment. During the main experiment a shortening of distance between the muzzle and test sample in direction of shot to 5m occured. Measured results are listed in Table 9.

Results of burglar resistance after reinforcement of test sample by set of 24mm thick polycarbonate boards [6] Table 9

Ammunition	*Distance (mm)*	*Depth of penetration channel in polycarbonate board (mm)*
9mm LUGER ZVS	5.10^3	13.4
9mm LUGER Subsonic		7.5
9mm LUGER		13.6
Blazer 9mm LUGER		penetration

Table 9 implies that the polycarbonate boards reinforced the test sample and prevented its penetration by all bullets except Blazer 9mm LUGER which was able to penetrate it. Mathematical model was ineffective in this case. The reason of penetration is presumably the composition of shot core. Figure 2 displays the shot in polycarbonate board. Bullet Sellier&Bellot 9mm Luger Subsonic penetrated only the first layer. The second layer was disrupted, but all other four layers remained almost intact.

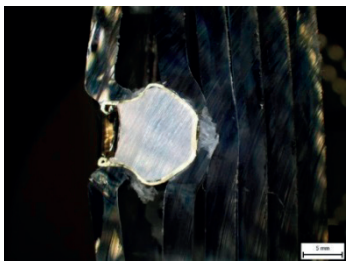


Fig.2 Cross-section of bullet in polycarbonate board [6]

5. Conclusion

The experiment performed with a set of 24mm thick polycarbonate boards proved significant increase of burglar resistance of the examined parts of chassis in a commercially produced personal motor vehicle (door). Only in one case, when using Blazer 9mm LUGER bullet, penetration occurred.

Results of burglar resistance (with and without reinforcement by rock wool) measured by perpendicular shooting of test sample within pilot project [6] Table 8

Ammunition	**Distance (mm)**	**Depth of penetration in wall stopping the shots (depth + length of bullet)**		
		Shot into test sample		**Difference**
		not reinforced	**reinforced**	
		(mm)		
RL 124 GRS FMJ	10^4	107.743	162.369	**54.626**
Lapua Cepp		104.104	138.629	**34.525**
RL 124 GRS FMJ lead		89.755	18.717	**-71.038**
Magtech		164.103	75.817	**-88.286**

These bullets are characteristic by their high penetration force. Further reinforcement is possible by adding another 4mm thick polycarbonate board. For the purpose of passive protection of the motor vehicle crew it is not necessary to use material from armored boards, but also other materials, such as polycarbonate board can be used. Financial costs of both polycarbonate boards and of technical modifications of a vehicle are significantly lower than the previous costs of armor reinforcement. In the next period, possibilities of increasing burglar resistance of motor vehicles using ceramic materials and carbon fabrics shall be experimentally verified.

References

[1] PLANKA, B. et al.: *Criminalistic Ballistics,* Prague: Ales Cenek, 2009, 672 p., ISBN: 9788073800369.

[2] BS EN 1063:2000 - *Glass in Building. Security Glazing. Testing and Classification of Resistance Against Bullet Attack*. BSI. 2000.

[3] BS EN 1522:1999 - *Windows, Doors, Shutters and Blinds. Bullet resistance. Requirements and Classification,* BSI, 1999.

[4] STN EN 1523 - *Windows, Doors, Shutters and Blinds. Bullet Resistance. Test Method (in Slovak)*, 2000.

[5] *German DIN ballistic standard.* German: DIN 52 290 - Part 2, Nov. 1988.

[6] Own experiment: *Exploration Burglar Resistance of Extracted Elements of Motor Vehicles*, 2012 - 2014.

[7] VEGA project No. 1/098/11 *Model of Integrated Security System Optimization Framework for Protection of Specific Objects Realised by Means of Expert System.*

[8] MARTINCOVA, P., GRONDZAK, K., VACLAVKOVA, M.: *Information System for Security Evaluation - Design and Implementation (in Slovak),* Proc. of intern. conference on technics, technologies and education ICTTE 2013: October, 2013, Yambol, ISSN 1314-9474. - [S.l: s.n], 2013, pp. 251-256.

[9] KITTEL, L., LOVECEK, T.: Passive Protection Elements Breach Resistance Modeling, *Communications - Scientific Letters of the University of Zilina,* vol. 13, No. 2, 2011, pp. 53-58, ISSN 1335-4205.

[10] Ministry of Interior of the Slovak Republic, Number of registred weapons in the Slovak Republic, [on-line] http://www.minv.sk/?statisticke-prehlady-evidencie-zbrani.

[11] STN EN 771-4 - *Specification for Masonry Units. Part 4: Autoclaved Aerated Concrete Masonry Units (AAC)*, 2013.

[12] EN AW 6106/ISO: *Al MgSiMn. Aluminium and Aluminium Alloys - Chemical Composition and Form of wrought Products* - Part 3: *Chemical Composition*; German version EN 573-3:1994.

[13] JURICEK, L., NOVOTNY, P.: Modeling of Small Arm Projectile Penetration Through a Steel Plate (in Czech). *Vojenske zdravotnicke listy*, vol. LXXIII, No. 1, 2004, ISSN 0372-7025.

[14] HALLQUIST, J., LS-DYNA: Keyword User's Manual. Nonlinear Dynamic Analyses of Structures. *Livermore Software Technology Corporation*, digital manual, May, 1999.

[15] IMAOKA, S.: *Implicit vs. Explicit Dynamics*. ANSYS, Inc. on 6.28.2001. www.ansys.net/ tnt_sheldon13.htm.

[16] SELLIER, K., KNEUBUHL, B.: *Wundballistik und ihre ballistischen Grundlagen. 2. vollig uberarbeitete und erganzte Auflage*. Berlin: Springer-Verlag, 2001, 526 p., ISBN 3-540-66604-4.

[17] MRAZ, J.: *Practical Research for Design of Passenger Car´s Body Increased Resilience (in Slovak)*. Diplomova praca, 2014, p. 91, odborny konzultant: Kamil Boc.

Adelaida Fanfarova - Ladislav Maris - Anton Osvald - Esko Mikkola *

THE REACTION TO FIRE TESTS FOR NATURAL THERMAL INSULATION OF HEMP MATERIAL MODIFIED BY FIRE RETARDANT OHNOSTOP SPECIAL

The scope of the paper is the experiment focused on testing and evaluating the fire protection of fire retardant modification of combustible material by means of experimental scientific method of the reaction to fire test. We tested the specimens of natural thermal insulation made of hempen fibre provided by the company Profi air color s.r.o. Zilina. These tested specimens were impregnated with retardation technology by soaking in the fire retardant Ohnostop special, provided by the company Bakra s.r.o. Rimavska Sobota. The experiment was performed by two experimental methods - the single-flame source test and the test of limited flame spread with the test devices under laboratory conditions. The main aim of the experiment was the assessment and possible improvement of fire-technical properties of thermal insulation material made of hemp by the application of fire retardant modification.

Keywords: *Reaction to fire tests, thermal hemp insulation, fire retardant, Ohnostop special.*

1. Introduction

Fire retardants are chemical impregnating substances which can in chemical, physical or combined way protect and prevent the ignition, slow down the process of combustion and eliminate the inception of fire and conflagration. The principle of the retardation process is the continuation of the specific retardation element to the surface and structure of combustible materials. Fire retardants have the ability to improve the fire-technical characteristics and fire resistance of the impregnated material and they also protect materials and products against direct flame contact, spontaneous combustion, flameless combustion (smouldering) and higher temperatures of fire (see [1]).

Classification of fire retardants depending on the principle of retardation (see [2]):

- fire retardants that release and emit non-combustible gases in the heat interval when the combustible gases are generated by thermal decomposition of the combustible material, which leads to dilution and decompression of concentration of flammable gases and, in this way, their ignition is impeded.
- fire retardants that accumulate heat from the source of heat, which leads to cooling the source of heat and slowing down the combustion process,
- fire retardants that create a protective intumescent foam layer (a few centimetres thick) on the surface of impregnated combustible material. This layer separates the surface of combustible material from the heat source and, simultaneously with the chemical reactions, slows down the combustion process,
- fire retardants that represent the mechanical type (for example, various building films and claddings made of non-combustible materials).

Classification of fire retardants depending on the way of application:

- coating (building constructions, metals),
- impregnation (wood, wood products),
- soaking (plastics, thermal insulation).

We experimentally tested the tangible fire retardant named Ohnostop special invented to decrease the combustibility and to improve the fire resistance of building products in interior spaces. This fire retardant can achieve the class of reaction to fire in accordance with standard EN 13501-1+A1:2010 : B-s1, d0. The Ohnostop special is a colourless watery substance of inorganic salts, 100% ecological, naturally recyclable, environmental and health friendly (see [3]). The composition of the product:

* [1]Adelaida Fanfarova, [2]Ladislav Maris, [1]Anton Osvald, [3]Esko Mikkola
[1]Department of Fire Engineering, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Security Management, University of Zilina, Slovakia
[3]KK-Palokonsultti Oy, KK-Fire Consult s.r.o., Espoo, Finland
E-mail: Adelaida.Fanfarova@fbi.uniza.sk

ammonium hydrogenorthophosphate technical - ($(NH_4)_2HPO_4$), ammonium sulphate technical ($(NH_4)_2SO_4$) and water (H_2O). Physical and chemical properties : liquid state, transparent colour, odour after urea, completely mixable, the density of 1180 - 1200 g/m^3, a boiling point of 100 °C, the decomposition temperature of 400 °C, flash point is not, is not self-igniting and is not dangerous explosion. It is one of fire retardants that release the non-combustible gases at the same time the combustible gases are produced. During the long-term affecting of open-direct flame this fire retardant prevents the fire spread. We can apply it by soaking, coating, spray application or by the vacuum – pressure method.

The careful choice of a fire retardant, the correct way of application and professional assessment of conditions and environment which will affect combustible material - all of these factors represent the functional and qualitative system of retardation process (see [4]). The mechanism of action of fire retardants usually depends on their chemical properties of material that we want to protect against the negative effects of fire. Fire retardants can be applied to various types of materials, for example, wood, plastics, metals, textiles, furniture, toys, cable bundles, electrical appliances, the construction and design elements, coverings of wall and ceilings, flooring, indoor and outdoor paints, thermal insulation.

Due to environmental aspects, the use of natural insulation materials made of plant materials, namely hempen fibre, is becoming more popular. There are two basic hemp species: Cannabis indica (containing psychoactive substances) which is not used in the construction industry and Cannabis sative (without psychoactive substances) which is used widely in various industries. As a building material, hemp represents a material that is difficult to replace by industrially manufactured insulation products due to its natural and unique properties. In addition, it is also produced from a renewable and sustainable source.

Hemp fibre insulation can be characterized by specific properties such as: high moisture resistance, ability to dry quickly, insulation stability in extreme conditions and creation of natural microclimate. Due to the natural content of bitter substances, it does not support fungal growth and has a certain resistance against rodents. Another advantage of hemp is its short vegetation period (harvesting is possible twice a year) and from a production point of view, fast renewal (3m growth in 3 months). The hemp insulation materials have good heat- and sound-insulation properties, owing to the sturdiness of the hemp fibres which are sufficiently flexible and can return to the original shape after a short compression. The hemp fibre is also able to maintain its shape and is not prone to material compaction and creation of unwanted cavities in places where insulation is required. Manipulation with this material is without health risks, such as skin damage, eye and airways irritation (see [5]).

Thanks to the above mentioned properties hemp insulation achieves higher qualitative standards in comparison to styrofoam, mineral or glass wool. It is also important to point out that hemp as a pure natural material is environmentally friendly, with no adverse health effects, recyclable and renewable.

2. Reaction to fire tests

The experiment consists of two different tests of reaction to fire performed under laboratory conditions:

1. *Reaction to fire test - Ignitability of building products subjected to direct impingement of flame, part 2 - the single-flame source test - in accordance with Slovak technical standard STN EN ISO 11925-2: 2011*. This method has been developed for determining the reaction of building materials to fire and it specifies the fire test for testing ignitability of combustible materials exposed to direct small flame with zero radiation, using vertically mounted specimens. Although this method is intended for determining the ignitability, it is based on the small flame spread on the vertical specimen surface after the application of small flame (match size) either to the surface or edge of the specimen for a period of 15 or 30 s. The duration of the test begins to elapse after the specimen is exposed to the flame. If the duration of the flame exposure is 30 s, then the entire test duration is 60 s (see [6]);
2. *Reaction to fire test - Methodology for testing the fire retardants and retardant modifications of material - the test of limited flame spread*. This method was developed in the Fire-chemical laboratory of the Department of Fire Engineering, Faculty of Security Engineering, University of Zilina as an internal document with the aim of becoming an STN standard. The methodology was created with the purpose of evaluating the specimen combustion behaviour when exposed to a direct mid-height flame for a longer time period. It describes and specifies the fire test for testing retardant treatments of combustible materials exposed to a mid-height flame, with the surface exposure angle of 45° to the vertical axis (see [7]).

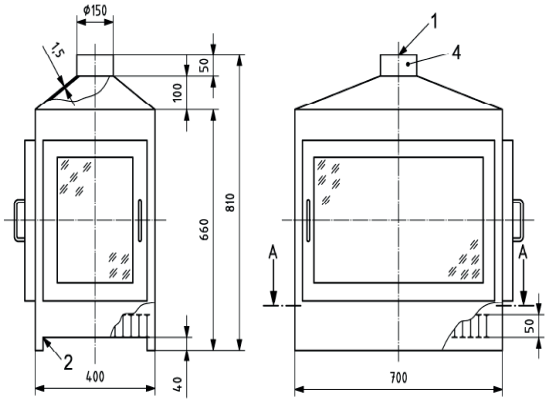


Fig. 1 The scheme of the test device
(1 - measured area of air circulation speed, 2 - metallic grating, 3 - horizontal board, 4 - chimney) (see [6])

It is necessary to maintain the ambient temperature of 23 °C (± 5 °C), relative humidity of 50 % (± 20 %) for the correct test procedure. Both test devices are located in such laboratory ambient conditions. A stainless steel combustion chamber with a fire-resistant glass door on the front face and one side is designated for the single-flame source test (see Figs. 1 and 2).

Fig. 2 The test device - combustion chamber located in the fire-chemical laboratory of KPI FBI ZU

The holder for the test specimen consists of two stainless steel U-shaped frames. The frame is fixed to a stand to which the specimen holder is fixed in such a way that it is not suspended too low and its open edge with the test specimen is exposed to the flame of the propane burner. The gas burner as the ignition source is designed for the use in a vertical orientation or under the angle of 45° (see Figs. 3 and 5). It is equipped with a valve for the exact flame height regulation. The device for flame height measurement is capable of identification of the prescribed flame height of 20 mm (± 0.1 mm) (see Fig. 4). The height of the flame is measured from the top edge of the burner to the yellow flame top (see Fig. 10). This check must be carried out prior to the test of each specimen, just before the test starts.

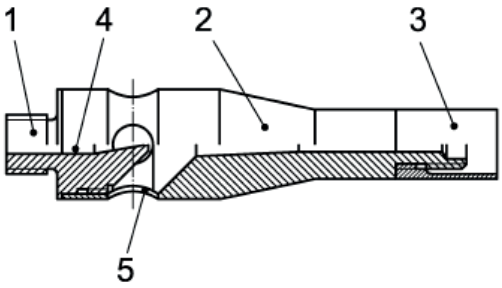


Fig. 3 The scheme of gas burner (1 - gas jet, 2 - pipe, 3 - flame stabilizer, 4 - mixing tube, 5 - construction rabbet) (see [6])

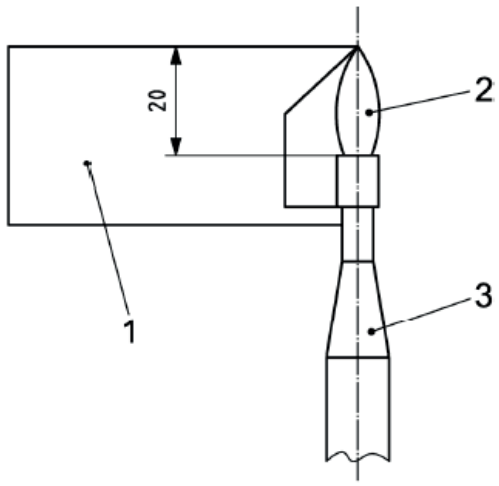


Fig. 4 The equipment for flame height measurement (1 - metallic board, 2 - flame, 3 - gas burner) (see [6])

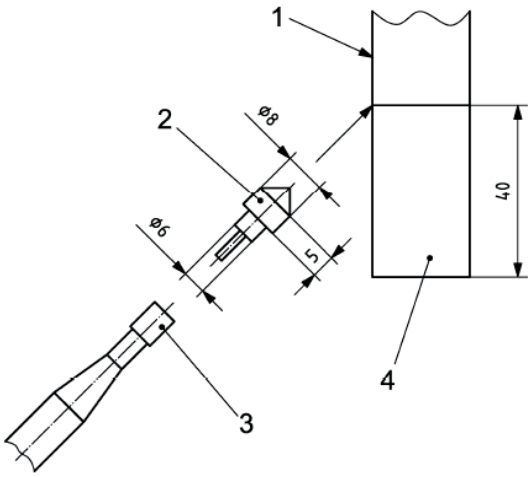


Fig. 5 The scheme of the flame impact on the surface of test specimen (1 - specimen surface, 2 - spacer, 3 - gas burner, 4 - test specimen) (see [6])

The test device for testing the limited flame spread determination is made of materials resistant to heat and combustion products released during the test. This device (see Fig. 7) consists of a test specimen holder of non-combustible material, gas burner, flow meter with fuel flow regulation and the fuel source – technical propane butane mixture cylinder and is constructed according to the scheme (see Fig. 6) adopted from an older standard (STN 73 0862 - supplement b). The ignition source is the gas burner designed and constructed (see Fig. 3) so that it can be firmly and securely fixed in the test apparatus and is controlled by a valve, ensuring the correct flame height 100 mm (± 2 mm).

The fuel source in both tests is a pressure cylinder with a technical propane-butane mixture with purity of at least 95 %. Other devices required for the tests are calibrated scales (with a precision of at least two hundreds of a gram) used for mass measurement of the specimens and time measurement devices for the measurement of the flame exposure duration.

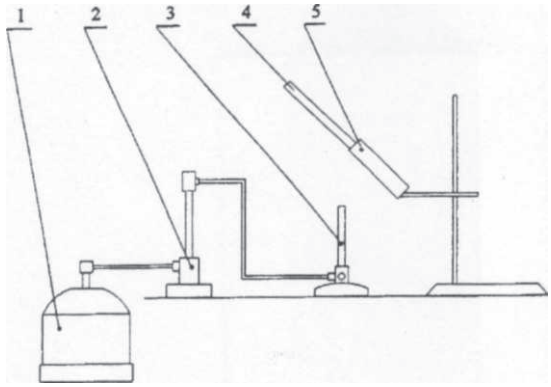


Fig. 6 The scheme of the test device (1 - gas cylinder, 2 - flow meter, 3 - gas burner, 4 - test specimen, 5 - holder for the test specimen) (see [7])

Fig. 7 The test device designed and located in the fire-chemical laboratory of KPI FBI ZU

The tests specimens for the experiment comprised six sets of specimens which were cut from a representative specimen of thermal hemp insulation (see Fig. 8). Each specimen had dimensions of 200 x 100 x 40 mm (± 1 mm). One set of test specimens comprised six specimens of natural material of the above stated dimensions (see Fig. 9).

For both reactions to fire tests three sets of test specimens were prepared:

- the first set of specimens (marked 1 » 6) was impregnated by soaking in the fire retardant Ohnostop special,
- the second set of specimens (7 » 12) was similarly impregnated by soaking in the fire retardant Ohnostop special but with addition of another effective chemical element in order to increase its fire protection,
- the third set of specimens (X1 » X6) was not impregnated in any way and was used as a fire retardant efficacy benchmark.

Fig. 8 The representative test specimen of thermal hemp insulation

Fig. 9 Two sets of test specimens soaked in the fire retardant

The preparation for both reactions to fire tests included mixing the Ohnostop special fire retardant solutions in compliance with the producer's instructions. The specimens of hemp insulation were impregnated by soaking for 5 minutes, whereas 350 ml of fire retardant solution was used for each two specimens. Subsequently, the specimens were weighed in regular intervals until completely dry, which meant complete evaporation of water bound during the retardation process. When the weight of all test specimens became stable (with 1g deviation), the test devices were prepared and the required laboratory conditions arranged. The methodology for the single-flame source test: each test specimen was fixed into the holder which was placed into the test device (see Fig. 10). The burner was lit in the vertical orientation and the flame was left to stabilise for a few minutes to achieve the prescribed height. Subsequently, the gas burner was adjusted

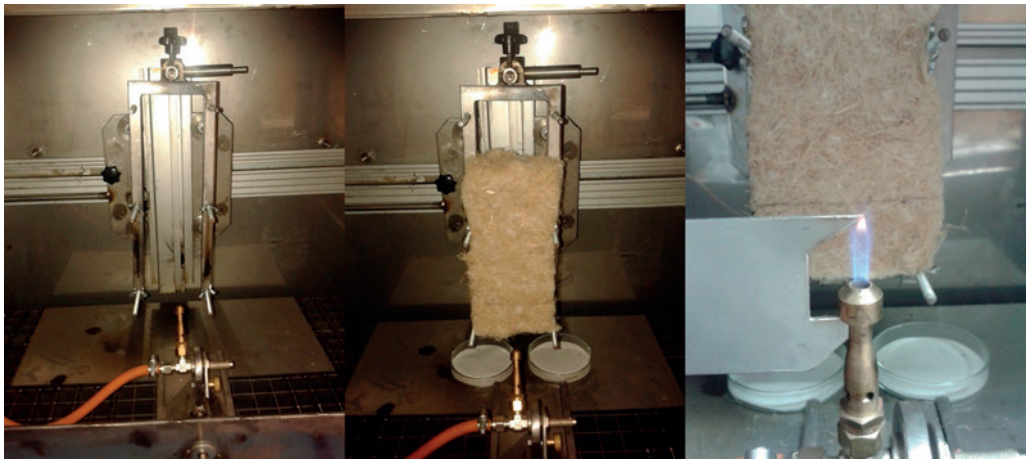


Fig. 10 The holder for the test specimen, consolidation of the test specimen to the holder, flame height measurement (left to right)

Fig. 11 The test specimen consolidation in holder, flame height measurement, testing (left to right)

to 45° and was moved horizontally until the point of contact with the specimen (40 mm above bottom edge of specimen) was reached. The duration of the flame exposure was 30 seconds and was measured from the moment of the flame contact with the specimen. The methodology for the test of the limited flame spread: each test specimen was placed in the test device holder under the angle of 45° and was exposed to the effects of an open mid-height flame for 5 minutes. For each individual test the height of the flame was exactly defined. Similarly, each test adhered to the unified test methodology (see Fig. 11).

3. The results of reaction to fire tests

All the test specimens were evaluated by the fire-technical characteristics specified for the process of combustion and fire development (time of ignition, time of spontaneous combustion and time of smoulder). The behaviour of the tested material during the testing procedure was also observed. The results of the tests of reaction to fire are summarized according to the sets of the test specimens as follows:

STN EN ISO 11925-2:2011 - Single-flame source test:

- the first set of the tested specimens soaked in the fire retardant Ohnostop special did not participate in the process of combustion in any way, there was no ignition, no sustained flaming, the test specimens did not spread the flame on the outer surface, there was no smoke, no smouldering, no dripping of flaming debris and no ignition of filter paper,
- the second set of the tested specimens also impregnated with the fire retardant Ohnostop special (but supplemented with one unnamed chemical element to improve the fire-fighting properties and qualities of the fire retardant) behaved in the same way as the first set of the tested specimens,
- the third set of tested specimens which was not modified in any way at all during the testing procedure significantly participated in the process of combustion, the tested specimens were ignited and the material spread the flame on

the outer surface, there was no sustained flaming, but high time of smouldering, tested specimens smoked visibly, there was no dripping of flaming debris and no ignition of filter paper was observed.

Methodology for testing the fire retardants - The test of limited flame spread:

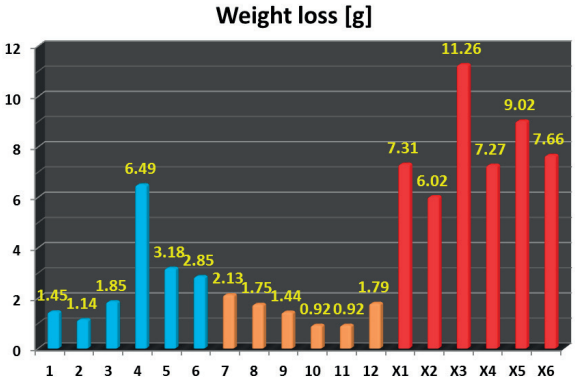


Fig. 12 The graph of values of weight loss of the test specimens

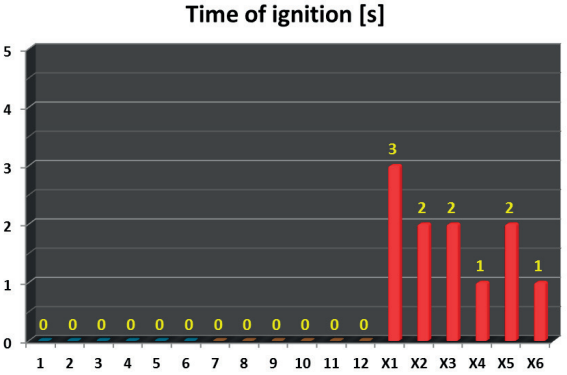


Fig. 13 The graph of values of time of ignition of the test specimens

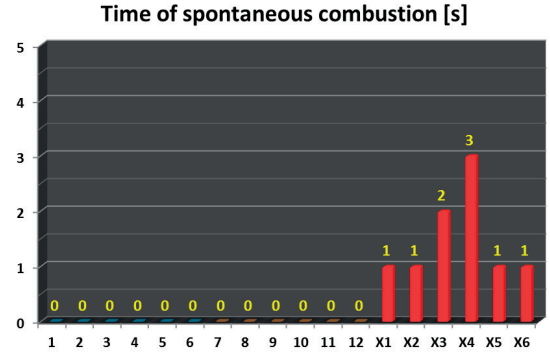


Fig. 14 The graph of values of time of spontaneous combustion of the test specimens

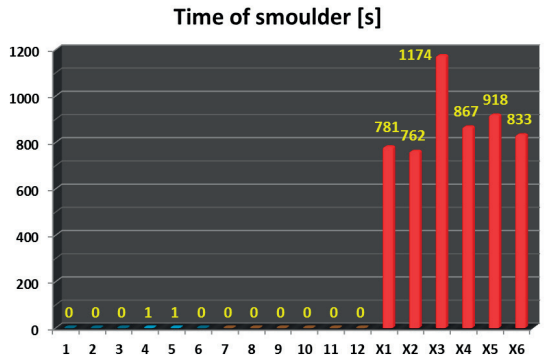


Fig. 15 The graph of values of time of smoulder of the test specimens

4. Conclusion

Based on the measured data from both tests of reaction to fire of combustible thermal insulation product made of natural hemp material, it is obvious that to improve the fire-technical characteristics of this material, it is advisable to impregnate it properly with a selected fire retardant. The suitable fire retardant can prevent the thermal hemp insulation to participate actively in the process of combustion. The fire retardant applied in our experiment was apparently able to slow down the combustion process. This phenomenon happens thanks to chemical composition and properly selected way of application of our fire retardant. During the retardation process the individual components of chemical composition strengthened effectively the structure of the combustible material and this slowed down the combustion cycle. All that almost completely eliminated the ignition, spontaneous combustion and smouldering of the tested material during the testing procedure. It is obvious from the above mentioned graphical representations of the results (see Figs. 12 - 15).

In standard practice these findings can be used, for example, in the possible deceleration of complete burnout time in the case of building fire, which can help save human lives, reduce property damages or mitigate negative environmental impacts. The team of authors aim to point out the use of fire retardants in standard practice and underline the importance of fire protection and fire-fighting qualities of retardant modifications of combustible materials and products.

Acknowledgements

The authors of the paper would like to express their gratitude to Mr. Arpad Krausz, the managing director of company BAKRA s. r. o., producer of the fire retardant OHNOSTOP special and to Mr. Zdeno Duris, the managing director of company PROFI AIR-COLOR, s. r. o., producer of natural thermal insulation made of hempen fibre CANABEST.

Special thanks also belong to FBI ZU for supporting the institutional grant of the project – IGP 201406.

References

[1] DRYSDALE, D.: *An Introduction to Fire Dynamics.* University of Edinburgh, West Sussex : John Wiley & Sons Ltd., 2nd ed., 1999, 576 p. ISBN 0 471 97290 8.

[2] OSVALD, A.: *Evaluation of Fire Safety Materials and Products of Wood*. Textbook. Zvolen : Technical university in Zvolen, 1997, 104 p. ISBN 80-228-0595-5.

[3] BAKRA, s. r. o.: *Product Ohnostop special*. 2013. [on line]. [cit. 2014-09-15]. Available at: http://www.ohnostop.com/ohnostop-special.html.

[4] MIKKOLA, E.: Fire Retardants and Product Behaviour in Fire Tests. *Polymer International*. Special Issue: Fire Retardant Polymers, vol. 49, No. 10, pp. 1222-1225, October 2000. Online ISSN: 1097-0126.

[5] PROFIAIRCOLOR, s. r. o.: *Natural Thermal Insulation Materials.* 2014. [on line]. [cit. 2014-09-15]. Available at: http://www.proficolor.sk/drevostavby8.html.

[6] STN EN ISO 11925-2: *Reaction to Fire Tests*. Ignitability of building products subjected to direct impingement of flame - Part 2: Single-flame source test. (ISO 11925-2: 2010). Bratislava : Slovak institute of technical normalization, 2011.

[7] FANFAROVA, A.: *Methodology for Testing the Fire Retardants and Retardant Modifications of Materials - Reaction to Fire Tests.* Internal document with suggestion of enact as STN, Zilina : Department of Fire Engineering, 2014. Verified by: Stefan Galla, managing director of The Fire-fighting, technical and expertise institute of The Ministry of Interior seat in Bratislava, Slovak Republic.

Pavla Gomba - Isabela Bradacova *

CRITICAL SYSTEMS AND PROCESSES AFFECTING THE RESILIENCE OF SUBWAY SYSTEMS TO TERRORISM RISKS

Terrorist attack on the urban transport systems with high concentration of people (such as the subway), depending on its mode, can cause different levels of damage including the elimination of sub-components of fire safety equipment or destruction of passive fire protection. To mitigate the effects of an attack, the resilience of vehicles, as well as efficiency of evacuation of the survivors affected mainly by the availability of adequate emergency exits, the number of evacuees and the local conditions of the process are critical. Based on the experience of previous attacks on the metro systems (Tokyo, London and other incidents), this paper identifies critical systems and processes for management of the emergency situation following a potential terrorist attack, ensuring safe and rapid evacuation and rescue to passengers.

Keywords: *Subway resilience and security, terrorism, critical infrastructure protection.*

1. Introduction

The risk of a terrorist attack in the developed countries remains consistently high. Based on research of case studies of both succeeded and failed terrorist attacks, the subway systems seem to be a popular target for terrorism because of the specific features and consequences related to an attack in the subway system´s environment: potentially substantial material and human damage, high media visibility and coverage causing general panic and long-term negative effects on the capacity of the whole transport infrastructure at a given place.

The state authorities as well as defense and security agencies are aware of these risks and implement special technological and organizational measures to improve the safety of subway transport systems, such as passenger clearance screening, increased depot security, on-going detection of explosives or integrating the emergency preparedness plans and approaches.

There have also been a number of studies and research projects aiming to increase the resilience of metro vehicles, to improve the effectiveness of preventive measures and to mitigate the potentially devastating impact of a terrorist attack in the subway system, such as the European FP7 SecureMetro project, the SECUR-ED and Protectrail projects to name but a few. In this regard, it is also worth noting the current MODsafe project (Modular Urban Transport Safety and Security Analysis) that integrates approaches to the safety and security measures in order to reduce barriers within the European Union so that a common European strategy can be established.

All these different initiatives and strategies have one common objective: to reduce material damage as well as potential causalities and injuries caused by a potential terrorist attack, to increase resilience and ensure fast recovery so that the metro transport systems are a less attractive target for terrorism.

2. Specifics of the terrorist attacks in the subway system

The physical features of the subway transport systems (underground location, construction technologies, ventilation, egress routes, alternative accessibility, integration with other public transport systems etc.) are rather specific and therefore require special measures with respect to the protection of passengers, ability to resume normal operation in an emergency situation and the crisis management in general.

It is critical to define most probable scenarios of a terrorist attack, analyze related risks, evaluate the current infrastructure under these threats and design both technological and organizational solutions for the high-impact types of attacks.

* [1]**Pavla Gomba,** [2]**Isabela Bradacova**
[1]Faculty of Safety Engineering, VSB - Technical University Ostrava, Ostrava, Czech Republic
[2]Faculty of Safety Engineering, VSB - Technical University Ostrava, Ostrava, Czech Republic
E-mail: pavla.gomba.st@vsb.cz

Research of the terrorist attacks in the rail-based systems in the last 50 years concludes that the number and severity of the attacks has grown substantially [1]. To be more specific, 833 recorded attacks killed about 3,500 persons and wounded more than 15,000. The sharpest increase in both number of attacks and their fatalities was identified in 1990s and 2000s [2], [3] and [4].

The scope and character of damage caused by a terrorist attack is mainly affected by the mode of perpetration and the tactics used. In the period of 2000 – 2010, bombing was used in 77% of the cases, followed by fire and firearms (both 4%) and firebomb and Molotov (3%). All other types of attacks are marginal (see Fig. 1). As the trends have the same characteristics over the period studied, it is reasonable to expect a continuing growth of attempted bomb attacks in the mid-term future [5].

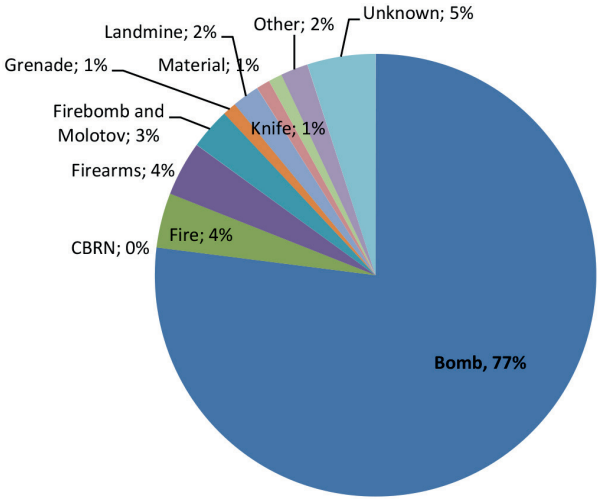


Fig. 1 Weapons used to carry out attacks in the rail-based infrastructure in 2000-2010[6]

The priority of security measures therefore needs to be given to the selection of vehicle materials and structural design that will increase the resilience of metro vehicles to the blast of explosives as well as measures increasing the security of passengers, staff and infrastructure through design of fire barriers and fire suppression technology that will reduce the impact of an attack. Special attention should be given to the situation when the metro train is blocked in a tunnel following a bomb blast as it represents the most challenging scenario for the survivability of the passengers, prevention of panic behavior and facilitation of rescue.

3. Case studies: major terrorist attacks on the subway systems

A mass-casualty terrorist attack at crowded, underground premises requires specialized response of the rescue agencies involved. The main inspiration for tailoring of the security plans and emergency response is the lessons learned from the major incidents targeting the subway infrastructure. Due to limited size of this paper, it focuses on the key findings only [7].

3.1 Tokyo subway sarin attack

The Tokyo subway attack was carried out on March 20, 1995 by a coordinated group of members of the religious movement Aum Shinrikyo (called Aleph since 2000 onwards), killing 13 and injuring over 5,000 people. It was the most serious incident in Japan since the World War II and noteworthy also for the use of a chemical agent (liquid sarin) instead of conventional explosives.

Nerve gas sarin is odourless, colourless and highly toxic (lethal even at very low concentrations). It is manufactured by the reaction of methylphosphonyl difluoride with isopropyl alcohol:

$$CH_3\,POF_2 + (CH_3)_2\,CHOH \rightarrow [(CH_3)_2\,CHO]\,CH_3\,POF + HF$$

Sarin affects the nervous system by interfering with the re-absorption of neurotransmitters. Death usually occurs as a result of asphyxia as the victim becomes comatose and suffocates due to the inability to control the muscles involved in breathing function.

The Tokyo subway, with its 9 lines, 179 stations and about the 195 km of route, is one of the busiest commuter transport systems in the world. The timing of the terrorist attack was not coincidental: around 8 a.m., at the peak of the morning rush hour when the concentration of commuters was the highest. Five men released liquid sarin from the plastic bags inside the trains at separate subway lines to maximize the impact and human damage. The trains continued on their routes with intoxicated passengers leaving the vehicles and others entering at each station. The gas further spread at each stop, either by vaporization or through contaminated passengers.

Following emergency response to the Tokyo subway attack revealed serious gaps in the security system and planning [8] and [9]:

- design of trains that did not allow to open the windows to support internal ventilation
- inability to identity the chemical agent until several hours later, thus exposing the passengers, subway staff as well as rescuers and causing secondary contamination of the whole subway infrastructure (e.g. on the Chiyoda line, employees cleaned two packages of liquid sarin on the train's floor by mopping them up with newspaper and bare hands, two of them died later on);
- more than an hour delay in problem recognition, not understanding that the emergency calls from different stations referred to the same mass incident, which led to the fact that the fire department sent all of their personnel to the first (Tsukiji) station, leaving minimal resources for other affected stations;

- unclear competencies and responsibilities of different authorities and lack of willingness to prioritize cooperation over interagency competition;
- serious failures in the organization of evacuation, data collection and transport of victims to the health facilities;
- withholding of information and miscommunication to the passengers and the public following the attack, based on the reluctance to provide information that might be incomplete or uncertain.

3.2 7/7 London subway bombings

The London bombings of 7 July 2005 were a series of multiple coordinated suicide attacks targeting civilians who commuted on the subway transport system during the morning rush hour. Between 8:50 and 9:47, four British jihadists detonated homemade organic peroxide–based devices in the London Underground trains across the city and another exposive was detonated inside a double-decker bus in Tavistock Square later on. In this country's first ever suicide terrorist attack, 52 civilians were killed, more than 700 injured and over 4000 people affected. Traffic in the city was paralyzed for a few hours and thousands of people remained closed in the metro stations and tunnels up to several hours [10].

The aftermath of the attacks were characterized by chaos and panic [11]: the lighting of trains and their immediate surroundings in the tunnel was destroyed, it was not possible to open the door, communication sets between the driver and passenger did not work and drivers could not communicate with the dispatchers either. There were power failures in some parts of the subway system and reports of blasts and smoke in the tunnels. In the first phase, the control center (London Underground Network Control Centre) evaluated the situation as a train derailment after hitting the tunnel wall at Edgware Road station.

Emergency health service was called to seven metro stations although some of them did not experience any incident. Serious incidents cause a large number of calls to the emergency helplines and the control center is usually able to evaluate the situation relatively quickly. However, in the case of London subway attacks, the situation was different because the subway stations and tunnels did not have sufficient cellular coverage meaning that people could not call for help and the drivers could not report to responsible dispatchers due to the damage of the communication system kits.

The most challenging situation occurred in the train that was damaged and blocked in the tunnel between King's Cross and Russell Square stations. After about half an hour after the attack, the evacuation of passengers was organized by the London Underground Emergency Response Unit with assistance of two police officers who helped passengers disembark through the driver's cabin and helped transport the wounded to the nearest station. Walking evacuation in an unlit tunnel lasted approximately 15 minutes.

The main method of evacuation developed then by the London Underground was through the end door in the last train. The side doors were designed so that they cannot be opened by passengers, only by trained subway staff as there is not enough space between the wall of the tunnel and side door, exposing the passengers to the risk of electric shock caused by high-voltage infrastructure in the tunnel.

Based on the severity of the injuries caused by bomb blasts and delayed arrival of qualified medical staff, another inadequacy revealed was the fact that the metro trains were not equipped with the first aid kits (available only to the drivers and in the stations).

Another important issue related to the evacuation in the urban environment is identification of large number of people, collection of their personal data and contact information for further police investigation, identification and return of personal property and notification of next of kin, as well as the establishment of appropriate reception centers to ensure that the people who have suffered mental or lighter physical trauma will not gather at locations around the disaster, thus preventing adequate and easy access of the rescue teams.

3.3 Moscow metro bombing and failed attacks

Subway systems have been a favorite terrorist target also in other parts of the world, particularly the Russian capital Moscow. In August 2000, a strong explosion of homemade bomb equivalent to 800 g of TNT occurred at Pushkinskaya metro station in the center of Moscow, killing 12 and injuring over 150 people. In February 2004, a suicide bombing inside the train between two stations on the Zamoskvoretskaya Line killed 10 and injured more than 50 people. The most recent terrorist attack occurred in the morning rush hours (7:56 and 8:38) in March 2010 when two bombs exploded on the Sokolnicheskaya Line, killing 40 and injuring 102 others. The two suicide female bombers who carried out the attacks wore explosive belts with a force of 1.5 kg of TNT and 2 kg of TNT respectively. Both devices were enhanced with metal nuts, bolts and screws to increase the destructive impact of the blasts. It is unfortunate that the Moscow authorities tend to release only limited information related to the attacks and emergency response which does not allow for more detailed study and analysis.

It is worth mentioning that there have been a number of terrorist attacks that foiled or failed, either as a result of efficient prevention and security measures or for other reasons related to the nature of the plot: four attempted attacks in the London Underground on 21 July 2005 (the bombs' detonator fired but did not ignite the main explosive charge), suicide bombings on the New York City subway system planned by al-Qaeda in 2009 and

a plot to bomb Washington Metro stations by another individual linked to the al-Qaeda ranks in 2010 to name but a few.

4. Key factors for the terrorism resilience and emergency response in the subway system

The above mentioned case studies, other incidents which could not be described here in detail as well as research projects focused on increased resilience and security of the subway systems identify a set of key survivability criteria based on the following functions:

- fast and accurate recognition of the problem, i.e. location, scope, character and impact of the terrorist attack
- minimization of the panic among survivors, allowing them to provide first aid to those wounded or suffering trauma and to understand their situation and possible next steps related to their rescue
- accessibility of the rescue teams to the place of incident
- organization of evacuation (if and when necessary)

The equipment and technical features of the subway trains need to be tested in realistic conditions simulating a bomb blast (currently the most usual mode of an attack), such as lack of lighting, smoke, secondary fire, panic and high concentration of people [12].

The designers and producers need to consider innovative approaches ensuring continuation of operation even in the most challenging conditions represented by the aftermath of a terrorist attack, e.g. self-powering of electrical equipment with internal ageing-prone batteries, protection of cables in shielded tubes, the closest possible location of antennae to the associated device while allowing easy operation and maintenance.

The overall crisis management is of utmost importance as the biggest challenges experienced after most of the attacks resulted from organizational and cultural, rather than technical deficiencies [13] and [14]. Following Table 1, Table 2 and Table 3 is an overview of the key criteria related to the subway resilience and security.

Key technical criteria for the subway trains — Table 1

Trains – technical criteria	
Windows	▪ Windows should be easily opened or closed manually as necessary for ventilation purposes. ▪ Unbreakable material and blast-proof design of windows is desirable to prevent injuries from the flying gass debris following a bomb blast. ▪ Use of windows as intuitive emergency exits needs to be considered (as seen in the 7/7 London bombings or the Kaprun funicular fire of 2000).
Door operating system	▪ Side doors represent a good emergency exit in a situation when the attack occurs while the train is in or close to the station. ▪ The door slides need to enable intuitive opening from the inside by passengers and the unlocking mechanism must be operational even without power. Luminiscent instructions next to the door are desirable. ▪ Doors connecting the trains need to be unlocked at all times allowing for evacuation by the end door of the last train.
Lighting	▪ Fire and blast-resistant lighting that secures visibility even in smoke, dust and soot conditions (e.g. LED-based lighting successfully tested under the SecureMetro project). ▪ Availability of flash-lights for the case when emergency lighting fails.
Intercom system	▪ Blast-proof device that allows mutual, both-direction communication between the driver and passengers should be installed in all trains, with special considerations for possible jamming with too many speakers on the same frequency. ▪ Train-to-ground communication system that allows both the driver to provide information about the attack and situation underground and the dispatcher/ rescue manager to give instructions for evacuation.
First aid equipment	▪ Easily accesible illuminated sets with the basic life-saving health supplies should be installed in every train.
Emergency instructions	▪ Easy-to-understand, illuminated emergency instructions located in each train may prevent the panic and help facilitate fast and effective rescue.
Evacuation guidance signs	▪ Luminescent exit and directional signs (similar to those used in airplanes and buildings) can help the passengers locate the exits. Considerations should be given to guidance for injured passengers crawling on the train ground.

Key technical criteria for the subway system Table 2

Subway system – technical criteria	
Surveillance system	▪ Fire and blast-resistant security cameras should be installed at all stations. Security can be further increased by regular parols, especially during moring and afternoon rush hours.
Lighting	▪ Tunnels, as well as stations and exits leading to the ground should be equipped with alternative emergency lighting independent of electric power supply (e.g. luminescent coating).
Ventilation	▪ Depending on the character of attack, ventilation shafts need to ensure fast supply of incontaminated air.
Design of rail track	▪ The tracks should be designed so that the trains in transit between stations can continue on to the nearest station without a power supply (gravity-driven).
Enhanced telecom infrastructure	▪ Full cellular coverage in the subway system, including the tunnels, can help facilitate communitation of passengers with the ground, thus allowing fast recognition of the incident, scope of the damage and efficient rescue of the survivors.

Key organizational criteria for the subway system Table 3

Subway system – operations	
Emergency response manual	▪ Adjustments/special considerations are needed to prepare the subway staff as well as the rescue agencies to handle multiple simultaneous incidents/ attacks.
	▪ In case of a major incident/ mass-casualty attack, additional rescue teams should be allocated to both neigboring stations.
Evacuation centers	▪ Based on agreements with local authorities and rescue agencies, identify at least two potential reception centers in the vicinity of the metro stations, negotiate with the owners / tenants of the premises and engage them in contingency planning and drills.
Division of responsibilities	▪ Clear allocation of decision rights and responsibilities among different divisions (both operational and technical) should be set-up to ensure timely and efficient rescue operations.
Training and emergency preparedness	▪ All subway staff should have professional training in the life-saving skills.
	▪ Regular drills involving subway staff and all rescue agencies need to be organized in order to identify and address potential inadequacies and areas for improvement.

5. Conclusion

Specifics of the subway infrastructure make it a particularly attractive target for the terrorists: an attack at a crowded space under the ground with limited alternatives for exit may not only cause potentially very high material as well as human damage but also paralyze the whole urban transportation system. A terrorist attack has some specific consequences (spread of fear and panic in the general public, typical lack of information in the immediate aftermath etc.) that distinguish it from natural or other man-made disasters and therefore requires special emergency response.

The case studies of the previous attacks carried out in the subway systems of different cities around the world provide valuable insight into what needs to improve so that the subway is more resilient to the attacks and the passengers are protected from the most serious effects. The threat of terrorism requires innovative approaches to the crisis planning.

The designers and manufacturers of the subway systems need to give a priority to the materials and technologies that ensure increased security in emergency situations: slide doors need to enable opening by passengers inside the trains, windows should allow for ventilation while not posing additional risks when broken, whereas adequate communications, together with emergency lighting in the train or tunnel and clear instructions and guidance by evacuation signs may reduce the chaos and panic that are associated with any emergency.

Professional crisis management system involving all stakeholders with well-established working relationships is just as important: it allows to recognize the problem without delays, deploy the rescue teams precisely when and where necessary and carry out effective recovery.

This paper presents a non-exhaustive checklist of key technical and organizational criteria against which any subway system can be assessed. More research and efforts are needed to implement the improved operating procedures and relevant safety standards of the subway systems into practice.

References

[1] Database of Worldwide Terrorism Incidents, downloadable at http://www.rand.org/nsrd/projects/terrorism-incidents/about/

[2] EU Terrorism Situation and Trend Report, TE-SAT 2011, ISBN 978-92-95018-86-0

[3] EU Terrorism Situation and Trend Report, TE-SAT 2012, ISBN:978-92-95078-23-9

[4] EU Terrorism Situation and Trend Report, TE-SAT 2013, ISBN: 978-92-95078-76-5

[5] LESLIE C. L,, KENNEDY, W., SHERLEY, A. J.: The Effectiveness of Counter-Terrorism Strategies, *Campbell Systematic Reviews*, No. 2, 2006, p. 8.

[6] Global Terrorism Database at http://www.start.umd.edu/gtd/

[7] SCHUURMAN, B., EIJKMAN, Q.: *Moving Terrorism Research Forward: The Crucial Role of Primary Sources,* ICCT Background Note, 2013, [online]: http://www.icct.nl/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf

[8] ROBYN, P.: *Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System.* BCSIA Discussion Paper 2002-4, ESDP Discussion Paper ESDP-2002-01, John F. Kennedy School of Government, Harvard University, February 2002

[9] FUNATO, T.: *Lessons Learned from Tokyo Subway Sarin Gas Attack and Countermeasures Against Terrorist Attacks,* Workshop on Implementing Sustainable Urban Travel Policies, March 2005, Tokyo

[10] BRUYELLE, J., O'NEILL, C., EL-KOURSI, E., HAMELIN, F., SARTORI, N., KHOUDOUR, L.: Improving the Resilience of Metro Vehicle and Passengers for an Effective Terrorism Response, *Safety Science* 62, 2014, pp. 37-45

[11] London Assembly: *Greater London Authority*, Report of the 7 July Review Committee, 2006, ISBN: 1 85261 878 7

[12] BRADACOVA, I.: *Fire Safety in Buildings. Non-production Objects - 2. ed. (in Czech)*, SPBI Ostrava 2010, ISBN 978-80-86111-77-3

[13] TITKO, M., ZAGORECKI, A.: Modelling Vulnerability of Transportation Network Using Influence Diagrams, *Communications - Scientific Letters of the University of Zilina*, No. 4, 2013, ISSN 1335-4205

[14] GOMBA, P.: *Alternatives for Modeling of Terrorism in Europe. Security, Risk and Crisis Situations in 2013 (in Czech)*, Proc. of X. Mezinarodni konference mladych vedeckych pracovniku, Ostrava, VSB - TU, 2013.

Milan Majernik - Petra Szaryszova - Martin Bosak - Lenka Stofova - Kani Kabdi *

INTEGRATED MANAGEMENT OF ENVIRONMENTAL-SAFETY AND TECHNICAL RISKS OF PLANTS PRODUCING AUTOMOBILES AND AUTOMOBILE COMPONENTS

The authors, as a result of their scientific and professional activities, present a concept of a future model for integrated management of risks in plants for production of automobiles and their components for contractors. They introduce the concept of a future standardized model of an integrated management system based on sub-aspects, impacts and risks according to the relevant current and upcoming new ISO standards of quality, environment, safety, including ISO 31000 Risks management and ISO/TS 16949. In this article the emphasis is placed on creation of a complex risks register (technical, environmental, safety), for this area of economic activity, their identification, analysis and evaluation within an integrated management system.

Keywords: *Automobile production, standardized management system, environmental and security risks, integrated management system, risks register, risk-assessment model.*

1. Introduction

Sustainable development in automobile manufacturing is now becoming strongly associated with its environmentalization and improvement of the quality from a complex point of view.

In this context, the organizations in the network of automobile industry suppliers are also forced to integrate environmental management, safety and technical aspects, impacts and risks of its production into their management systems. With increasing pressure from the whole society and intensifying pressure on the supply-chain, an evaluation of environmental, safety and technical risks represent an innovative approach by which an enterprise can effectively mitigate environmental-security threats, as well as create competitive advantages.

As a result of scientific research activities of the authors in the area of implementation, maintenance and authorization of integrated management systems (IMS), a suggestion and verification of the methodology for evaluation of environmental-safety and technical risks of products in automobile industry enterprises on selected products.

2. Integrated Management System based on ISO standards in plants for production of automobiles and their components

Ensuring the success of organizations by implementing various standardized management systems in today‘s difficult economic situation becomes increasingly common in general and in automobile manufacturing industry, primarily from the point of view of production complexity, quality and especially competitiveness. The best known and most frequently applied international standards include:

- Quality Management System (ISO 9001),
- Environmental Management System (ISO 14001, EMAS III),
- Occupational Health and Safety Management System (OHSAS 18001),
- Risk Management System (ISO 31000) and others.

Branch industry standards are increasingly used and an example for the investigated area is:

- Quality Management System. Particular requirements for application of ISO 9001:2008 in organizations for automobile production and their spare parts.

Currently, there is a unification of the standards structure on an internatonal level and their forthcoming revision (2015)

* [1]Milan Majernik, [1]Petra Szaryszova, [1]Martin Bosak, [1]Lenka Stofova, [2]Kani Kabdi
[1]Department of Management, Faculty of Business Economics in Kosice, University of Economics in Bratislava, Slovakia
[2]L. N. Gumilyov Eurasian National University Astana, Kazachstan
E-mail: milan.majernik@euke.sk

should bring unification in the form of 10 identical chapters in support of management systems integration. The concept of a standardized integrated management system model in the automobile plants industry (see Fig. 1) would create conditions for integrated management, environmental-safety and technical aspects, impacts and risks while fulfilling all requirements of sub-management systems. The basic prerequisite for the effectivity of such a system is the creation of an integrated risks register for continuous process improvement.

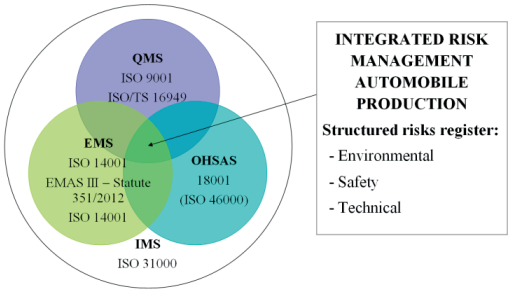


Fig. 1 Model of Integrated Management of risks in automobile industry operations

The basic guideline for the management of risks, regardless of their origin and character is the ISO 31000 standard with the only negative resulting from the fact that it is not a standard intended for certification purposes. Environmental risks will, therefore, be solved through implementation of ISO 14001 certification, or as part of the approaches of the EU, namely EMAS III. Until the Occupational Health and Safety Management ISO 46000 standard (2016) is published, it is possible to certify the system through the implementation of OHSAS 18001. The authentication of quality management according to ISO 9001 and ISO/TS 16949 remains the key element of IMS.

3. Risk analysis of the sustainability of automobile production products

Organizations in the network of automobile industry suppliers must continually improve the effectivity of their quality management system and manage their risks for development of sustainability. Improving of the production process must be continuously focused on management and reduction of product characteristics and manufacturing process parameters variance.

In every business, the management must decide which risks the company would be willing to accept in comparison to possible opportunities. This process can lead to a mixed strategy which everyone agrees with, and the organization is exposed face to face to uncertainty. Organization can work on reduction of their most vulnerable areas, while paying attention to their most important opportunities [1].

All approaches to risk management have a number of common basic points: to identify risks, determine the degree of hazard and to find ways to cope with them effectively. It is not important whether the concept of risk management in the enterprise is defined, but whether there are automatic tools leading to risk management control [2].

Risk management must be based on the management of the enterprise as a whole. „Effective risk management, identifying new events and changed circumstances, assists management in decision-making in the review of the company positions and its prospects“ [3].

In their work on the development and production of sustainable product, the authors emphasized the relevance of integration of environmental aspects into production of a new product and new decision-support tools to achieve it [4].

Other authors confirmed that achieving overall sustainability requires a focused look at the entire supply chain, including manufacturing systems and processes and a detailed life-cycle, which includes a better understanding of the impact of the product, predictive models of individual processes and optimized production processes, as well as optimization of all activities within a closed loop supply chain. In the development of advanced predictive models and optimization techniques for sustainable production, the authors also analyzed simplified scoring models for sustainable planning and production processes [5].

The authors of [6] proposed a new framework for assessing sustainability of business operations in the manufacturing sector, implementation of economic, environmental, safety and technical objectives into organizational operating procedures with an increasing focus on achieving sustainable business.

In their article [7], the authors presented how to compare companies with an appropriate level of sustainability using a model for designing the composite index of sustainable development, which determines efficiency and effectivity of businesses.

In comparison with different methods of integrated sustainability, the assessment methods of strategic environmental impact assessment results and, „triple-bottom-line approach“, concluded that the assessment of environmental aspects, impacts and risks requires a clear concept of sustainability as a social goal, defined criteria according to which assessments are realized and which effectively separates sustainable results from unsustainable ones [8].

4. Research methodology

Our research was realized on a selected production operation of the automobile industry. The risk management needs of the cable harnesses production life cycle were devided into the following 9 stages:

1. Receipt of material.
2. Transportation of the product to the warehouse.
3. Transportation by forklift.
4. Handling in the warehouse.

5. Cutting the cables.
6. Contact, welding, soldering, cutting contacts.
7. Stripping of cables.
8. Cable formation, repairs.
9. Electrical control, packaging.

4.1 Register of environmental-safety and technical risks

According to the impact probability and importance of each risk, certain value was given to each of the identified risks. From all of the identified risks – actual number 97 we chose those which reached the highest value. These risks had the value in the range of 0.033 to 2.256. Based on the prepared matrix of risk impact importance and probability (see Table 1), we deal with the risks of high importance and the relevant part of the register listing important environmental-safety and technical risks, as shown in Table 1.

From a review of literature, there is a clear need to use an assessment of environmental- safety and technological risks, but their results, as reflected in the stage of production cycle of existing products, failed to be expressed in many cases. To bridge the gap, this study aims to provide clearly set risks which have been identified and analyzed in the enterprise.

4.2 Evaluation of environmental-safety and technical risks of production of cable harnesses

For components or parts in finished products which meet specifications or customer expectations and are in accordance with ISO/TS 16949 (technical aspects) there is used the man – machine setting with division of labor in production and defined responsibility for the quality of the processes involved. This is the correct setting of material, resource and practise planning. Once the product reaches the employees (product handling)

Part of the register listing environmental-safety and technical risks of an operation for the production of automobile harnesses Table 1

Organizational unit / place of creation	Activity / process of creation	Environmental aspect	Environmental impact - pollution	Risks			Assessing the significance of			S/INS	PE/PO	D/IND
				ER	SR	TR	I	P1	P2			
Warehouse of logistics, warehouse of hazardous waste	Handling of hazardous waste in storage	Plastic containers containing residues of dangerous substances	Hazardous substances, waste	Toxicity Landfilling	Caustic burns	Potential damage of components of wiring harness	3	0.594	0.527	S	PE	D
		Metal packaging	Hazardous substances, waste	Oxidation Landfilling	Capture Cuts	Potential damage of components of wiring harness	3	0.403	0.384	S	PE	D
		Absorbents contaminated by pollutants	Hazardous substances, waste	Water contamination	Caustic burns	Technical failure of machinery	4	0.755	0.726	S	PE	D
		Hazardous substances, solvents	Water pollution hazardous substances	Water contamination Oxidation Toxicity	Inhalation, ingestion or absorption of hazardous substances by skin	Shorting or breakage of cable harnesses	5	0.839	0.913	S	PE	D
		Chemicals	Hazardous substances	Acid rains Greenhouse Effect Chemical spill	Fire Damage of the health of employees	Damage of machinery deformation of cable harnesses	5	0.871	0.885	S	PE	D

Explanation:

I - Importance
P1 - Probability of the impact on the environment
P2 - Probability of the impact on human health
ER - Environmental risk
TR - Technical risk
SR - Safety risk
S/INS - Significant / Insignificant aspect
PE/PO - Permanent / Potential aspect
D/IND - Direct / Indirect aspect

the stage which leads to different load cases and in various degrees to negative effects on health and safety of a person or the environment begins. In the stage of handling the product uses a lot of resources, either directly or indirectly. The final stage of production and packaging of the product also requires regular inspection or, maintenance, which must be determined on the basis of a designated production program of the enterprise. An important stage of the product life cycle is the production of waste which plays a crucial role in the dynamically changing modern world and developing environmental, safety and technical standards. On that basis, we need to have answers to the following concepts related to risks reduction, reuse, inspection and repair and recycling, which appear to be significant benefits in addressing the problem of continuous improvement and sustainability.

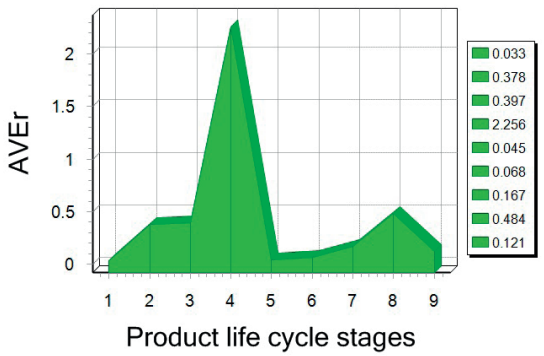
For the calculation of the risks for individual stages of a chosen product cycle, we used the basic formula and processed the Register of comprehensive integrated environmental-safety and technical aspects, impacts and risks of the enterprise.

$$Rp_n = \frac{\sum_{i=1}^{a} Ip_{n_i} \times P1p_{n_i} \times P2p_{n_i}}{a} \quad (1)$$

Explanation:

R - Risk of individual stage of production of the product
n - Number of stages, n=9
p_n - Probability of the n-th production stage of the product
Ip_n - Importance of the n-th production stage
$P1p_n$ - Probability of the environmental impact of the n-th production stage of the product
$P2p_n$ - Probability of the impact on human health of the n-th production stage of the product
a - Number of environmental-safety and technical aspects of the n-th stage production of the product

The greatest risk, as shown in Fig. 2, arises from handling of substances and materials in the warehouse because there are stored absorbents contaminated by pollutants, solvents, chemicals, plastic and metal containers, which, when handled improperly, can cause a risk of an adverse impact on the environment and human health.



Legend:
1. Receipt of material
2. Transportation of the product to the warehouse
3. Transportation by forklift
4. Handling in the warehouse
5. Cutting the cables
6. Contact, welding, soldering, cutting contacts
7. Stripping of cables
8. Cable formation, repairs
9. Electrical control, packaging

AVEr - Average risk of an individual production stage of the product

Fig. 2 Evaluation of total environmental-safety and technical risks lifecycle production of cable harnesses

5. Results and discussion on determination of the total value of environmental-safety and technical risks

The basic objective in determining or calculation was to identify and prioritize the key for addressing the risks of life-cycle production of cable harnesses (handling in the warehouse) and generalize a new, more precise approach for their reuse also of other products in the industry.

The nature of the risk assessment is in the decision whether we can take the risk (see Table 2) and, if not, what measures we have to implement to eliminate the risk or at least to minimize it to an acceptable level. The total value of environmental-safety and technical risks for the automobile wiring harnesses product was 48 %, while it is shown that it is necessary to make improvements to minimize the environmental impact in the stage of material handling in the production of cable harnesses.

Evaluation of environmental-safety and technical risks of the enterprise — Table 2

Range of environmental-safety and technical risk	Evaluation of environmental-safety and technical risk
R greater than 150 %	Requires immediate action
R in the range of 75 % - 150 %	Planned action according to the nature of danger
R to the extent of 15 % - 75 %	Requires increased attention
R smaller than 15 %	Acceptable level

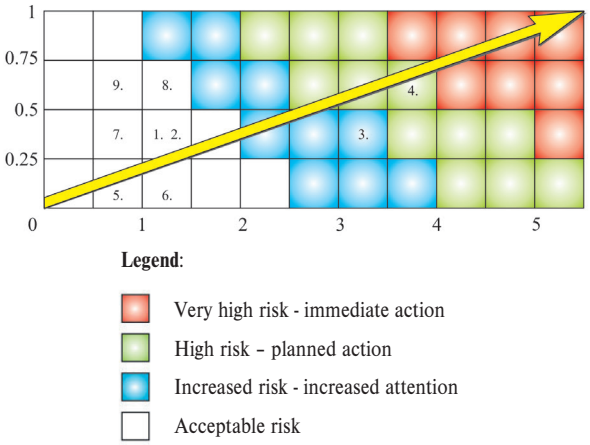


Fig. 3 Measurement of environmental-safety and technical risks

Environmental-safety and technical risks from various dangerous situations within the processes were transformed into a risk matrix (see Fig. 3). This way of formalization makes it easy to identify items which must be prioritized in the purposeful prevention of threats to life and working environment and workers‘ health. In the process of risk mapping as well as in the case of risk prioritization, two components will be used:

- probability of an impact,
- importance.

Probability of an impact will demonstrate a value determining uncertainty of occurrence of a specific event, phenomenon and severity, which will express a certain degree of deterioration. The prepared matrix, shown below, connects the seriousness of the risk and probability of the occurrence of environmental-safety and technical risks.

Effective prevention against damaging of health and the environment is based on the knowledge of the risk nature and their severity. The necessary condition of effective prevention is to meet all the requirements imposed by regulations and ISO standards OHSAS 18001 and/or ISO 14001. The determination of risk prevention measures is the result of all previous steps. The measures aim to eliminate the risks at the source of their origin or to mitigate them such that the risk to the environment and human health has been minimized.

The most effective method of prevention is to eliminate risks, for example, by a technological change and focus on the best available (BAT) changes in working practices, or increasing the distance from the source of a worker´s risk, alternatively, other organizational arrangements. However, it is important not to allow the risk to be transferred to another place where the consequences of new arrangements could be even more serious.

If you cannot eliminate the risk by technical or technical-organizational measures, or reduce it to an acceptable level at the source, technical collective protection measures are used. For example, there are installed safety devices which turn off the work equipment when a worker enters dangerous zones, a suction device removing pollutants from the breathing zone and others.

In cases when you cannot use the previous measure or despite its use some risk remains, we use PPE (Personal Protective Equipment). At the same time organizational measures, taken to minimize a worker´s exposure to that risk, are introduced.

A complex integrated assessment of relations between probable risk and its consequences on the environment and health of workers can also use a 3D diagram (see Fig. 4). This type of a diagram allows to put all three parameters into a mutual relation simultaneously.

The significance degree of a risk R is, in this case, determined by the product of the score of risk importance and probability of

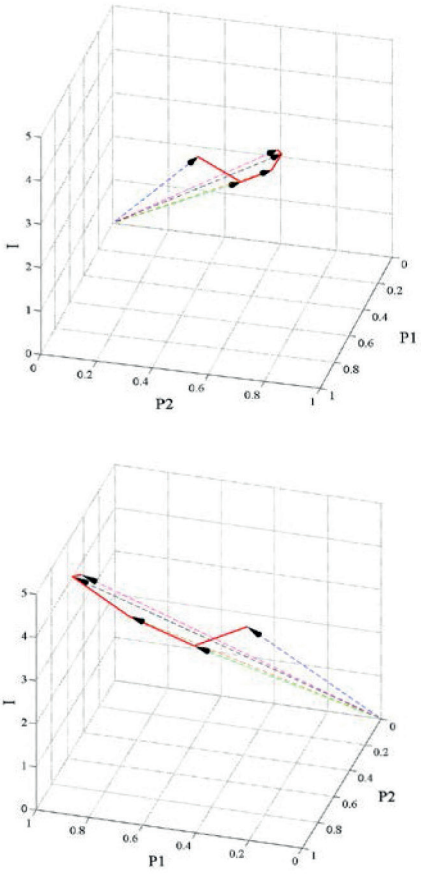


Fig. 4 Integrated assessments of environmental-safety and technical risks of production of cable harnesses

the impact on the environment and probability of the impact on human health. The relationship is as follows:

$$R = I \times P1 \times P2 \quad (2)$$

The value of the risk R importance degree may be in the range of 1 % to 150 %. Also, in this case, the resulting numerical risk assessment and determination of the degree is influenced by subjective opinions, while unacceptable risk can be considered values greater than 75 %.

The risk assessment is a process ongoing in most cases separately, but it cannot be understood in isolation. The risk assessment is a part of risk management and it is a process for the implementation and use of which there is currently high demand.

The analysis and management of environmental-safety and technical risks aim to eliminate risks, although, we have to realize that their complete elimination is not possible. It is important to reduce the level of risk to an acceptable level. This level is reflected in the residual risk which is acceptable for the company, individual, organization. The results of the analysis of environmental-safety and technical risks have, from this point of view, a very significant importance, especially for the adoption of reasonable preventive solutions which are very important for health and safety and protection of human lives and working environment.

6. Conclusion

A more exact procedure for integrated management of environmental-safety and technical risks in the automobile industry supply company, using a cubic matrix diagram, was suggested and verified on a case study. It allows to express the risk more exactly and explore significant connections and relationships of environmental, safety and technical aspects, impacts and risks of production sorted according to their relevance in the integrated register.

The proposed methodological approach allows not only identifying risks, but also prioritizing them according to their relevance and the implementation of results within environmental-safety management forming part of the integrated management system based on international standards and principles of a sustainable development.

Our research was primarily aimed on the identification of risks in an integrated 3D model which can be inspiring and helpful in identifying the main areas of risk occurrence and finding effective solutions to problematic issues. In further research methodology extended by examination of relevant socio-economic aspects, modified and implemented for a variety of products analyzed in the automotive industry and, ultimately, a methodology for the car as a whole may be proposed.

References

[1] JAYAL, A. D., BADURDEEN, F., DILLION, O. W. JR., JAWHIR, I. S.: Sustainable Manufacturing: Modelling and Optimization Challenges at the Product, Process and Systems Levels, *CIRP - J. of Manufacturing Science and Technology*, 2010, vol. 2, pp. 144-152.

[2] KAEBERNICK, H., KARA, S., SUN, M.: Sustainable Product Development and Manufacturing by Considering Environmental Requirements, *Robotics and Computer Integrated Manufacturing*, 2003, vol. 19, No. 6, pp. 461-468, DOI: 10.1016/S0736-5845(03)00056-5.

[3] KOTLER, P., CASLIONE, A. J.: *Chaotes*, Bratislava : Eastone Books, 2010, vol. 2, p. 168, ISBN 978-80-8109-114-8.

[4] KRAJNC, D., GLAVIC, P.: How to Compare Companies on Relevant Dimensions of Sustainability, *Ecological Economics*, 2005, vol. 55, No. 4, pp. 551-563.

[5] LABUSCHAGNE, C., BRENT, A. C., ERCK, R. P. G. V.: Assessing the Sustainability Performances of Industries, *J. of Cleaner Production*, 2005, vol.13, No. 4, pp. 373-385.

[6] LOVECEK, T.: *Security System - Security of Information System,* EDIS : University of Zilina, 2007, p. 246. ISBN 978-80-8070-767-5.

[7] POPE, J., ANNANDALE, D., SAUNDERS A. M.: Conceptualizing Sustainability Assessment, *Environmental Impact Assessment Review*, 2004, vol. 24, No. 6, pp. 595-616.

[8] RYBAROVA, D., GRISAKOVA, N.: *Business Risk 1st ed.,* Bratislava : Iura Edition, 2010, p.179. ISBN 978-80-8078-377-8.

Maria Hudakova - Katarina Buganova - Jan Dvorsky - Jaroslav Belas - Leo-Paul Dana *

ANALYSIS OF THE RISKS OF SMALL AND MEDIUM-SIZED ENTERPRISES IN THE ZILINA REGION

Small and medium-sized enterprises (SMEs) are very sensitive to changes in the business environment which after a certain time are always reflected into quantitative characteristics of this sector. In 2013, we accomplished a statistical survey on current trends in the field of business risks for SMEs in selected regions of the Czech Republic and Slovakia. In this article we want to analyze the effects of selected risks of the survey with respect to the length of the small and medium-sized business enterprises in the Zilina region. SMEs should be aware of their risks, mainly due to their importance in the economic system of the Slovak Republic, which mostly lies in their inconsiderable share to create job positions in the region.

Keywords: *Enterprise, risk, dependence, business environment.*

1. Introduction

Small and medium-sized enterprises (SMEs) have become an increasingly important component of economic development, representing a substantial proportion of national economies worldwide [1]. In this context, Henderson and Weiler indicate that SMEs can be characterized as a major engine of economic growth [2].

SMEs represent a strong economic potential for development in the Slovak Republic. The area of support of SMEs business is currently one of the key issues of further direction of our economy. Business in SMEs is mainly specific for its flexibility and possibility of faster adaptation to turbulent conditions of the market environment compared to large enterprises. From the quantitative point of view there are micro-enterprises, i.e., enterprises with the fewest employees (0 – 9) that are currently the most developed in Slovakia. Micro, small and medium-sized enterprises can be regarded as the driving force of national economies, as they create favorable conditions for increasing employment, the realization of innovative processes, but also create a suitable social environment in the regions [3]. Their flexibility predisposes to become a regional stabilization factor, even at the moment, at a time of increasing competitive pressures.

2. Defining the problem

2.1 Current state of the business environment in the Zilina region in Slovakia

In 2012, the economy of the Slovak Republic achieved growth in gross domestic product indicating the overall positive development in the economy. However, in the case of SMEs, the situation was different. Economic activity continued to decline and the trend towards marginalization of enterprises strengthened (business transfer from higher size categories into the category of micro-enterprises) resulting in a decrease in the number of enterprises with more than 10 employees to about half compared to 2008 [4].

In Slovakia, natural persons formed 70.2% and legal entities 29.8% out of a total number of SMEs in 2012 (551 608). Self-employed persons (92.8%) had the dominant representation in the context of natural persons. According to the data from the Register of Statistical Office SR [5] most of self-employed persons in 2012 worked in the Bratislava (15.2%), Zilina (15.1%) and Presov region (14.7%).

There were registered 15 167 active SMEs – legal entities (LE) in total in the Register of Statistical Office SR [6] in the Zilina region on 31.12.2012 which was more by 1 174 (8.4%) subjects year-on-year. In terms of size:

* [1]Maria Hudakova, [2]Katarina Buganova, [3]Jan Dvorsky, [4]Jaroslav Belas, [5]Leo-Paul Dana
[1]Faculty of Security Engineering, University of Zilina, Department of Crisis Management, Slovakia
[2]Faculty of Security Engineering, University of Zilina, Department of Crisis Management, Slovakia
[3]Faculty of Security Engineering, University of Zilina, Department of Crisis Management, Slovakia
[4]Faculty of Management and Economics, Tomas Bata University of Zlin, Department of Enterprise Economics, Czech Republic
[5]Faculty of Business and Economics, GSCM Montpelier Business School, France
E-mail: maria.hudakova@fbi.uniza.sk

- micro-enterprises represented share of 89.5%,
- small enterprises (10 – 49) represented share of 8.1%,
- medium-sized enterprises (50 – 249) represented share of 2.0%,
- large enterprises (250 – more) represented share of 0.4%.

In the structure of SMEs (LE) and according to the type of economic activity, there were business entities prevailing in the area of trade – 37.4% (about 7.5 p.b. more than SR in total), commercial services – 19.0 % (about 12.3 % less than SR in total) and industry – 11.4%.

2.2 Management of business risks in Slovakia

The need for more active and systematic engagement with risk rises in current changing business environment in Slovakia. Business risks arise from negative changes in internal and external business environment for SMEs. Currently, very wide range of business risks has effect on the SME which can not be clearly defined [7]. Every business is unique and so we must approach it in identifying potential risks that may endanger the business.

Small and medium-sized entrepreneur can create good conditions for risk management, as he is in close proximity to all aspects of individual operations and knows many strengths as well as the vulnerability of his business. On the other hand, even the owners of small and medium-sized enterprises are intuitively aware of common resources of risks that affect their daily lives [8]. Entrepreneurs are not always aware of such resources of risks as they do not have direct experience. Business experience in risk management often arises precisely of how long the entrepreneur carries out his business activities and thus sometimes can, sometimes cannot predict negative changes in the business environment [9].

SMEs are also much more closely tied to the region in which they implement their activities than large enterprises. In addition the enterprise is located in the region; its activity also participates in increasing regional employment and also brings other benefits to the region apart from economic benefits. Therefore, we focused on the quantitative analysis of selected risks of SMEs in this article from the point of view of their length of business in the Zilina region in Slovakia.

3. Objective and procedure of problem solving

In 2013, we accomplished a statistical survey of the business risks of SMEs in Zilina, within the project FaME/2013/MSPRISK: "Current trends in the area of business risks of small and medium-sized enterprises in selected regions of the Czech Republic and Slovakia." The project co-operated with Tomas Bata University in Zlin, Pan European University in Bratislava, University of Zilina and Trencin.

164 small and medium-sized enterprises in the region were surveyed. The structure of enterprises was as follows: 17% do business in production, 21% in commercial activities, 17% in construction enterprises, 6% in transport enterprises, 1% in agricultural enterprises and 38% formed the largest share of enterprises that do business in other sectors (trade, consulting, distribution, etc.).

In terms of the structure of SMEs and number of employees the results of the survey were as follows: 66% of micro-enterprises, 20% of small enterprises, 14% of medium-sized enterprises.

SMEs surveyed in the Zilina region: 38% do business more than 10 years, 32% do business from 5 to 10 years, 30% do business from 1 to 5 years.

The objective of article is based on data from a statistical survey to analyze the effect of selected risks to SMEs with regard to their length of business in the region. The length of business is an important factor affecting the perception of the business risks and their management style mostly. It is based on business experience of SME´s owners, managers and their attitude to risk and their ability to manage risk as well.

In order to meet the objective stated, we used empirical research methods (questionnaire, interviews with competent persons of SMEs), statistical methods, i.e., analysis of variance using quantitative tools of statistics (percentages, averages, homoscedasticity, Bartlett's Test, Kolmogorov-Smirnov Test, F-test, Kruskal-Wallis Test, Box-and-Whisker Plot) and statistical software Statgraphics Centurion XV [10].

In our research, we focused on the market, financial, personnel, operational (production), security, legal risks to SMEs. The percentage of identified key risks for SMEs in Zilina is shown in Fig. 1.

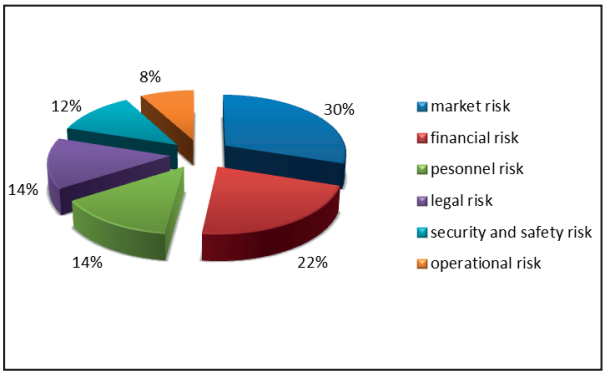


Fig. 1 Percentage of identified key risks for SMEs in the Zilina region

Subsequently were classified different intensities of identified key risks for SMEs, according to the length of their business in the region into three groups (Table 1).

Using statistical methods and tools we examined whether the average (mean) values of the key risks are dependent on the number of years of enterprise activities in the Zilina region or not. We used the quantitative method "*analysis of variance*". We

Classification of key risks to SMEs according to the length of their business Table 1

Key risks / SME groups according to length of business	Market risk	Financial risk	Personnel risk	Legal risk	Security risk	Operational risk
from 1 to 5 years	40	24	14	18	17	12
from 5 to 10 years	38	34	25	20	16	13
more than 10 years	56	39	26	22	20	9

Basic statistical characteristics of the key risks stated in three groups of SMEs according to the length of the business Table 2

Key risks	BSCs	SMEs from 1 to 5 years	SMEs from 5 to 10 years	SMEs more than 10 years
Market risk	μ	58.28	48.90	50.77
	σ	21.73	17.19	18.69
Financial risk	μ	31.67	32.79	33.77
	σ	15.44	12.92	14.02
Operational risk	μ	25.00	31.46	26.44
	σ	14.92	11.41	9.81
Personnel risk	μ	26.43	35.92	25.23
	σ	18.34	18.04	6.86
	σ^2	336.26	325.32	47.06
Legal risk	μ	31.28	29.75	30.22
	σ	22.73	11.06	12.86
	σ^2	516.45	122.30	165.43
Security risk	μ	28.00	25.63	23.05
	σ	24.43	12.89	8.36
	σ^2	597.0	166.2	59.8

determined the analysis of variance either by parametric or non-parametric tests [11]. Using the calculation of parametric tests two basic conditions had to be met: the resulting p-value of the intensity of the key risks of the homoscedasticity test (identity of variances) and normality test to verify intensities of risks must be higher than the level of significance 0.05 we have chosen.

The necessary information for the analysis of variance is given in Table 2. The basic statistical characteristics (BSCs) are as follows: μ - average intensity of risk to the enterprise, σ - standard deviation intensity of risk to the enterprise, σ^2 - variance intensity of risk to the enterprise.

4. Results and discussion

4.1 Analysis of variance of SMEs´ market risk

High competition, price battle, customer behavior, all of these can cause failure of SMEs and loss of market share. Up to 134 of SMEs selected market risk among the three key risks in the current business, representing 81.7% of SMEs surveyed. For the use of the parametric test of the mean values of market risk in the three groups of SMEs according to the length of business in Zilina, the following conditions are as follows:

1. *Homoscedasticity* was fulfilled. Resulting p-value using the Bartlett´s Test was 0.334.
2. *Normality of the risk intensity* was fulfilled. The values of Kolmogorov-Smirnov Test found were as follows: p-value of business from 1 to 5 years is 0.207, from 5 to 10 years is 0.534, more than 10 years is 0.213.

Table 3 shows that the resulting p-value of the analysis of the variance of market risk intensity for SMEs using parametric F-test is 0.071. The value is higher than the level of significance 0.05 which was chosen. We can confirm that there are no statistically significant differences among variances of the intensity of market risk in individual groups of SMEs according to their length of business in the Zilina region on the level of the reliability of 95.0%. The average values of the intensity of *market risk do not depend on the length of the business activity* on the market in the Zilina region. This fact corresponds well with the multiple Box-and-Whisker Plot in Fig. 2 where the red sign + represents the average intensity of market risk expressed as a percentage.

Analysis of the variance of market risk intensity using parametric F-test Table 3

Variance of SMEs according to the length of the business	Sum of squares	Df	Average of squares	F-ratio	P-value
Variance among groups of SMEs	1 995.9	2	997.948	2.69	0.0715
Variance within groups of SMEs	48 553.5	131	370.638		
Total variance	50 549.4	133			

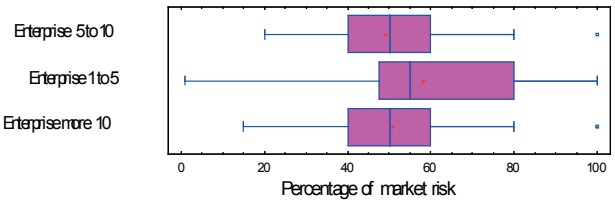


Fig. 2 Percentage of market risk using the Box-and-Whisker Plot

4.2 Analysis of the variance of financial risk for SMEs

The availability of financial resources, insolvency, enterprise debt and many other factors represent the financial risk for SMEs that was determined by 97% of the SMEs, 59.1% of SMEs surveyed. Considering the analysis of financial risk, parametric test of the mean values of financial risk in three groups of SMEs according to the length of the business in Zilina region could not be used, as all of the conditions were not fulfilled:

1. *Homoscedasticity* was fulfilled. Resulting p-value using the Bartlett´s Test was 0.650.
2. *Normality of the risk intensity* was not fulfilled. The p-value was lower in one group of enterprises than the level of significance of 0.05 we had chosen. Kolmogorov-Smirnov Test detected the following values: p-value of enterprises business from 1 to 5 years is 0.032, from 5 to 10 years is 0.487, more than 10 years is 0.101.

Subsequently, *non-parametric multi-selective Kruskal-Wallis Test of medians* of financial risk in defined groups of enterprises according to the length of the business in the region was performed. Since the calculated p-value of the analysis of intensity variance of financial risk from Table 4 is higher than 0.05, we can say that there are no statistically significant differences among intensities of the financial risk medians of enterprise groups according to the length of the business in the region of Zilina with reliability of 95.0%. *Intensity of financial risk medians does not depend on the length of the SMEs on the market.* This statement corresponds with multiple boxplot in Fig. 3 where the vertical blue lines represent the medians of the financial risk in the individual business groups expressed as a percentage.

Analysis of the variance of financial risk intensity using Kruskal-Wallis Test Table 4

	Number of groups	Financial risk median	P-value
Enterprise from 1 to 5 years	24	44.2083	0.590038
Enterprise from 5 to 10 years	34	49.4559	
Enterprise more than 10 years	39	51.5513	

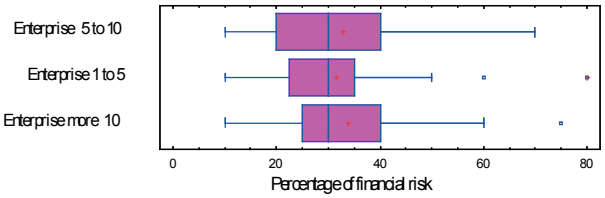


Fig. 3 Percentage of the financial risk using the Box-and-Whisker Plot

4.3 Analysis of the variance of personnel, legal and security risk of SMEs

The human factor has an indispensable role in SMEs, in terms of experience and knowledge in decision-making which may be benefit but also great risk for the enterprise. It is directly related to the risks arising from non-compliance with applicable legal standards, individual and public safety, as well as the safety of the products themselves, etc. When analyzing the personnel, legal and security risk, the course of calculating the analysis of variance was similar. Personnel risks were identified by 65 SMEs, representing 39.6% of the SMEs surveyed. Legal risk was identified by 60 SMEs, representing 36.6% and safety risk was identified by 53 SMEs, which is 32.3% of the SMEs surveyed. For the calculation of all these risks it was not possible to use parametric test of mean risk values in three risk groups of SMEs according to the length of the business in the Zilina region, since *the first condition of homoscedasticity was not met*. In all the cases, the resulting p-value was found by Bartlett's Test lower than the level of significance 0.05 which had been chosen:

- resulting p-value for the personnel risk was 0.00001,
- resulting p-value for the legal risk was 0.004,
- resulting p-value for the security risk was 0.0001.

Graphical display of the personnel risk of multiple boxplot in Fig. 4 shows that the length of the box (inner group variance) is for the enterprises with more than 10 years shorter than for other business groups. It is obvious even in the legal and security risk in Fig. 4 that the length of the box is for the enterprises with a length of business from 1 to 5 years longer than for other groups. Also the median of the group is about 7.5% smaller than the median of the remaining groups. On the basis of the graphical analysis and results of homoscedasticity test, we can say that the average (mean) values of the intensity of *personnel, legal and security risk depend on the length of the enterprise activity on the market* in the region and there are statistical differences among the groups of enterprises.

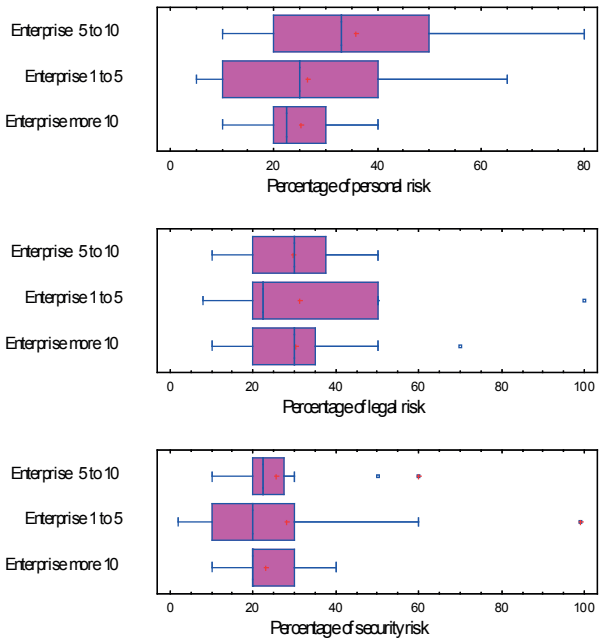


Fig. 4 Percentage of personnel, legal, security risks using Box-and-Whisker Plot

4.4 Analysis of variance of the operational risk of SMEs

The production processes themselves, or provision of services and the implementation of outcomes in practice constitute resources of operational risk. Operational risk was identified only by 34 SMEs, representing 20.7% of the SMEs surveyed. For the use of the parametric test of the mean values of the operational risk in the three groups of SMEs according to the length of business in the region, the following conditions were fulfilled:

1. *Homoscedasticity* was fulfilled. Resulting p-value using the Bartlett´s Test was 0.429.
2. *Normality of the risk intensity* was fulfilled. The values of Kolmogorov-Smirnov Test found were as follows: p-value of enterprises with the business length from 1 to 5 years is 0.710, from 5 to 10 years is 0.865, more than 10 years is 0.363.

The data from Table 5 shows that the resulting p-value of the analysis of the variance of operational risk intensity using parametric F-test is 0.408. The value is higher than the level of significance of 0.05 we chose. We can confirm that there are no statistically significant differences among the variances of operational risk intensity in the various groups of SMEs according to their length of business in the region on the level of reliability of 95.0%. The average values of the intensity of the operational risk *do not depend on the length of enterprise activity* on the market in the region. This statement corresponds with multiple boxplot in Fig. 5 where the red sign + represents the average intensity of market risk expressed as a percentage.

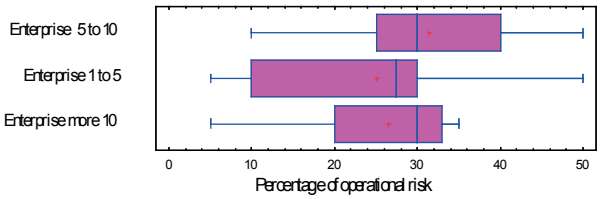


Fig. 5 Percentage of operational risk using the Box-and-Whisker Plot

5. Conclusion

The results from the analysis of the intensity of the key risks of SMEs identified with regard to their length of business in the Zilina region of Slovakia highlight the need to be prepared even more for unexpected changes to the current business environment. Using statistical methods and tools we were able to determine whether the average values of the key risks are dependent on the number of years of enterprise activities in the Zilina region or not. We applied quantitative method "ANOVA - analysis of variance". We calculated the analysis of variance either by parametric or non-parametric tests. Using the calculation of parametric tests two conditions had to be met:

Analysis of the variance of operational risk intensity using parametric F-test — Table 5

Variance according to the length of the business	Sum of squares	Df	Average of square	F-ratio	P-value
Variance among groups of SMEs	284.812	2	142.406	0.92	0.4080
Variance within groups of SMEs according to the length of business	4783.45	31	154.305		
Total variance	5 068.26	33			

the calculated p-value of the intensity of the key risks of the homoscedasticity test and normality test to verify intensities of risks must be higher than the level of significance 0.05 we have specified. The results of the above mentioned analysis of business risks for SMEs have confirmed that the intensity of market risk, financial risk, and operational risk is not dependent on the length of the enterprise activity on the market in the region. Therefore, many years of experience of managers often fail to protect SMEs before the unpredictable risks that the market economy and high competition can bring about.

The analysis and results of the tests showed that the personnel, legal and security risks depend on the length of the enterprise activity on the market in the Zilina region. In this case, the experience of the managers and owners prove beneficial. Assessing the risk, however, only on the basis of their own experience and feelings is currently inadequate. Therefore, the owners and managers of SMEs in Slovakia should rethink their approach to risk management.

It is necessary to increase the level of knowledge, in particular, enterprise owners (this is largely about micro-enterprises) about the possible causes and consequences of the risk, as well as on appropriate measures to be taken to reduce them. Improving the level of risk management in SMEs requires the acquisition of theoretical knowledge for the specific activities of the risk management process, methods and tools used in the management of risks. The absence of risk management can be one of the root causes of business failure and loss of competitive advantage especially in the highly unsettled business environment in Slovakia.

Acknowledgements

Publication of this paper was supported by the European Union within the project No. 26110230079 Innovation and internationalization of education – tools of quality enhancement of Zilina University in the European Education Area.

Reference:

[1] KARPAK, B., TOPCU, I.: Small Medium Manufacturing Enterprises in Turkey: An Analytic Network Process Framework for Prioritizing Factors Affecting Success. *Intern. J. of Production Economics,* 125: 60-70, ISSN 0925-5273.

[2] HENDERSON, J., WEILER, S.: Entrepreneurs and Job Growth: Probing the Boundaries of Time and Space, *Economic Development Quarterly*. 24(1): pp. 23-32, ISSN 0891-2424.

[3] HUTTMANOVA, E.: *The Present State, Possibilities of Support and Development of Small and Medium-Size Enterprises in the Slovakia*, [on line]. [cit. 2014-8-7], Available at: http://www.pulib.sk/elpub2/FM/Kotulic10/pdf_doc/11.pdf.

[4] SLOVAK BUSINESS AGENCY: *Analysis and Surveys of Business Environment,* [on line]. [cit. 2014-8-6], Available at: http://www.sbagency.sk/sba-0

[5] Statistical Office of the Slovak Republic: *Statistical Yearbook of the Regions of Slovakia 2013,* [on line]. [cit. 2014-7-18], Available at: http://slovak.statistics.sk/.

[6] SMSP: *Report on the State of Small and Medium-sized Enterprises in the Slovak Republic in the year 2012,* [on line]. [cit. 2014-8-4], Available at: http://www.sbagency.sk/sites /default/files/file/stav_msp_2012u.pdf.

[7] HOLLA, K. et al.: Complex Model of Risk Assessment of Industrial Processes MOPORI. *Communications - Scientific Letters of the University of Zilina,* vol. 15, No. 2, pp. 63- 68, 2013, ISSN 1335-4205.

[8] RISTVEJ, J., ZAGORECKI, A.: Information Systems for Crisis Management - Current Applications and Future Directions, *Communications - Scientific Letters of the University of Zilina*, vol. 13, No. 2, pp. 59-63, 2011, ISSN 1335-4205.

[9] HUDAKOVA, M., BUGANOVA, K., LUSKOVA, M.: *Small and Medium-Sized Enterprises Business Risks in Slovakia.* WMSCI 2014: The 18th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando : Florida, pp. 240-245, 2014, ISBN 13: 978-1-941763-05-6.

[10] STATGRAPHICS: *SoftverStatgraphics Centurion XV. 2014,* [on line]. [cit. 2014-7-11], Available at: http://www.statgraphics.com/support/download_center.aspx

[11] BETAKOVA, J., ONDERISINOVA, K., MICHALKO, J., SUPAK, M.: *Sustainable Development and Environmental Information Systems.* Multimedia w organizacjach gospodarczych i edukacji, Warszawa : Difin, pp. 46-50, 2006, ISBN 83-7251-673-1.

Ales Tulach - Miroslav Mynarz - Milada Kozubkova *

FORMATION OF CRITICAL CONCENTRATIONS OF NATURAL GAS AT ITS LEAKAGE

Spreading of natural gas during its leak from a domestic low pressure pipeline in a confined space is a complicated issue depending on many factors. In relation to possible explosion, created dangerous concentrations could be identified effectively by numerical simulations using mathematical CFD models. It is suitable to verify the results of numerical simulations by real experiment, even if it is a simplified one. Verified mathematical model could then offer detail picture of spreading of gas in a whole focused space. In executed numerical analysis, several mathematical models of gas flow were applied and they were compared to the results of experimental measurements. This paper deals also with formation and propagation of critical concentrations of natural gas in the whole observed space in the cubical experimental chamber. All above-mentioned matters could be applied in the fields dealing with safety of persons, technologies and objects, and it could be also used for explanation of accidents related to leakage and explosion of gas.

Keywords: *CFD models, leakage of gas, propagation of gas, natural gas, dangerous concentration, explosive concentration.*

1. Introduction

At present number of incidents, in which gas exploded in residential homes, increases. From the viewpoint of safety it is important to identify places where dangerous and explosive concentrations can be created. Determination of the amount of combustible gas leaked from a broken installation gas pipework is most often performed using simplified calculations [1]. The time required for creation of an explosive concentration is also determined in a similar manner.

CFD numerical simulations [2] are an appropriate means for more detailed determination of propagation parameters of dangerous gas. This paper is devoted to the mathematical modelling of leakage and diffusion of natural gas using the software ANSYS Fluent [3 and 4]. Emphasis is also placed on verification of the accuracy of calculation, which is ensured by comparison of the data obtained from numerical simulations with experimental measurements.

2. Description of measuring system and of calculation

For simulation of leakage and diffusion of gas throughout the enclosed space we created a measuring system consisting of a gas pipeline damaged in a defined manner, of partly closed container and of detectors. Leakage of gas occurred from the samples with leaks prepared in advance (circular and elongated hole, cut on the hose, etc.).

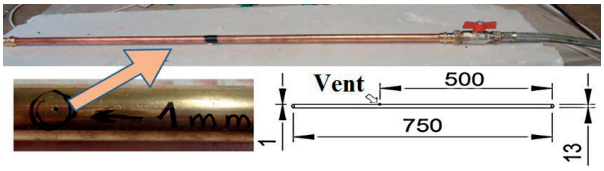


Fig. 1 Sample with a hole (mm)

Mathematical modelling considered a hole with diameter of 1 mm (Fig. 1) which was drilled into the copper gas pipe (sample). Area of the hole was 0.785 mm^2 and the pipe wall thickness was 1 mm. The sample (Fig. 1) with a hole was on one side blinded and from the other side it was connected to the installation low-pressure gas pipework.

The sample geometry (Fig. 2), designed with use of the software DesignModeler, consists only of inner volumes. The hole in gas pipeline was simulated by creation of a cylinder with the height and diameter of 1 mm on the inner volume of the sample.

* [1]Ales Tulach, [1]Miroslav Mynarz, [2]Milada Kozubkova
[1]Department of Fire Protection, Faculty of Safety Engineering, VSB - Technical University of Ostrava, Czech Republic
[2]Department of Hydromechanics and Hydraulic Equipment, Faculty of Mechanical Engineering, VSB - Technical University of Ostrava, Czech Republic
E-mail: ales.tulach@vsb.cz

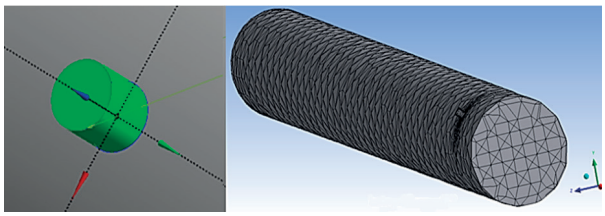


Fig. 2 Inner volume of the hole and calculation mesh of the sample

Mesh of the sample (Fig. 2), created in the software ANSYS Meshing, consists of 40 807 elements.

The gas leaked into an enclosed space (cubic vessel) with volume of approx. 1 m^3 [5]. A hole was cut into the vessel bottom in order to achieve during measurement a constant pressure in the vessel which would be identical to the pressure outside the vessel. Hardened polystyrene was used as construction material. Cubic vessel and location of the sample is shown in (Fig. 3).

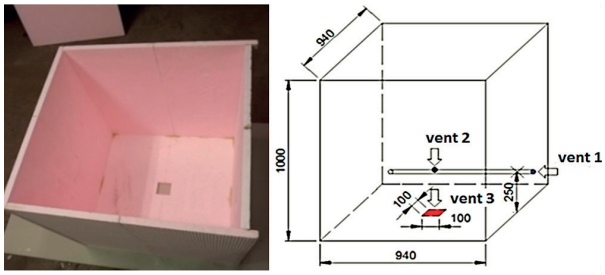


Fig. 3 Inner volume of the vessel and location of the sample (mm)

For easier creation of the calculation mesh the vessel geometry was formed from five connected volumes (Fig. 4).

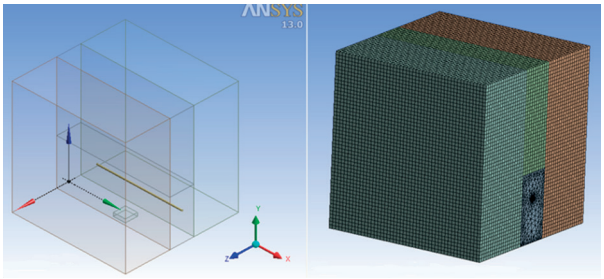


Fig. 4 Geometry of the whole system (on the left) and calculation mesh of the whole measuring system (on the right)

The whole computational mesh consists of 274 426 elements. The parameter for **determination of quality of a 3D cell** (degree of its deformation) is **0.748**. Limit value of the parameter is **0.9**. Quality of this computational mesh is therefore **satisfactory**.

Two stage detectors of inflammable gases CH4-GC20N, which were in-built into the walls of the created vessel, were used for detection of the flowing natural gas. Figure 5 illustrates position of detectors and tracepoints (dimensions are in millimetres).

During measurement we monitored times when 0.5% a 1% voluminal concentrations of methane were reached at the detectors' sensors. The measurement was finished after detection of 1% concentration by the last sensor. Each measurement was repeated three times. In the case of great difference of results the number of repeated measurements was increased as needed.

The function of six sensors used for experiment was ensured by six tracepoints created in the geometry of mathematical simulation. Position of points (black crosses) is the same as position of methane detectors in-built into the walls of the measuring system, which delimitates the space of gas leakage (Fig. 5). The program Fluent then evaluated on the basis of these points the dependence between the time of leakage and methane concentration in the mixture with air in voluminal percentages.

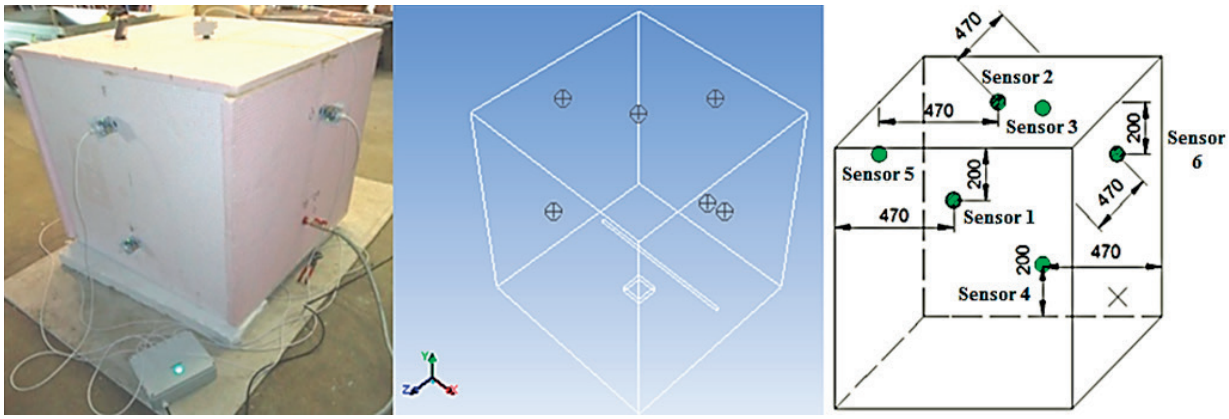


Fig. 5 Position of detectors and of tracepoints (mm)

3. Mathematical model of flow

The program ANSYS Fluent [3] for mathematical modelling of physical measurement was used. The basic relation used by the program for calculations is the **continuity equation** [4].

$$\frac{\partial(\rho)}{\partial} + \frac{\partial(\rho u_x)}{\partial x} + \frac{\partial(\rho u_y)}{\partial y} + \frac{\partial(\rho u_z)}{\partial z} = S_z$$

Simulation of methane flow through the space uses the **Navier-Stokes' equations** [4],

$$\frac{\partial \rho u_x}{\partial t} + \frac{\partial \rho u_x u_x}{\partial x} + \frac{\partial \rho u_y u_z}{\partial y} + \frac{\partial p u_z u_z}{\partial z} =$$
$$\rho a_x - \frac{\partial p}{\partial x} + \frac{\partial}{\partial x}\left(\mu \frac{\partial u_x}{\partial x}\right) + \frac{\partial}{\partial y}\left(\mu \frac{\partial u_x}{\partial y}\right) + \frac{\partial}{\partial z}\left(\mu \frac{\partial u_x}{\partial z}\right) + S_x$$
$$\frac{\partial \rho u_y}{\partial t} + \frac{\partial \rho u_x u_y}{\partial x} + \frac{\partial \rho u_y u_y}{\partial y} + \frac{\partial p u_z u_y}{\partial z} =$$
$$\rho a_y - \frac{\partial p}{\partial y} + \frac{\partial}{\partial x}\left(\mu \frac{\partial u_y}{\partial x}\right) + \frac{\partial}{\partial y}\left(\mu \frac{\partial u_y}{\partial y}\right) + \frac{\partial}{\partial z}\left(\mu \frac{\partial u_y}{\partial z}\right) + S_y$$
$$\frac{\partial \rho u_z}{\partial t} + \frac{\partial \rho u_x u_z}{\partial x} + \frac{\partial \rho u_y u_z}{\partial y} + \frac{\partial p u_z u_z}{\partial z} =$$
$$\rho a_z - \frac{\partial p}{\partial z} + \frac{\partial}{\partial x}\left(\mu \frac{\partial u_z}{\partial x}\right) + \frac{\partial}{\partial y}\left(\mu \frac{\partial u_z}{\partial y}\right) + \frac{\partial}{\partial z}\left(\mu \frac{\partial u_z}{\partial z}\right) + S_z$$

By combining the above mentioned relations it is possible to determine pressures and velocities depending on all three coordinates (x, y, z) in the whole calculation mesh for each time step.

At solution of propagation of admixtures it is necessary to resolve local mass fractions of admixtures "$Y_{i'}$" [-] in the mixture,

$$Y_{i'} = \frac{m_{i'}}{m} = \frac{\rho_{i'} V_{i'}}{\rho V} = \frac{\rho_{i'}}{\rho} \alpha_{i'},$$

where $m_{i'}$ [kg] is mass of the admixture i'; m [kg] is total mass of the mixture; $\alpha_{i'}$ [-] is voluminal fraction of the admixture i' in the mixture.

Transfer of admixtures (of mass fraction) is resolved by the **balance equation** [4] which in the changing time calculates with the values of mass fractions of the admixture "$Y_{i'}$" and with components of velocity of flow of present gases "u_i".

$$\frac{\partial}{\partial t}(\rho Y_{i'}) + \frac{\partial}{\partial x_j} \cdot (\rho u_j Y_{i'}) = -\frac{\partial}{\partial x_j} J_{i',j} + R_{i'} + S_{i'}$$

"$J_{i',j}$" is diffusion flow of the i^{th} component of the mixture, "$R_{i'}$" is the net rate of production of species i by chemical reaction and "$S_{i'}$" is the rate of creation by addition from the dispersed phase plus any user-defined sources.

In the solved task a transition occurs between laminar and turbulent flow. It is a transition region where flow in the pipeline is laminar (Re = 359), while in the zone of leaks the flow is, on the contrary, turbulent as a result of big increase in speed (Re = 4 640).

In order to achieve the best possible agreement of numerical simulation with the experimental measurement we used six mathematical models of flowing ("**Laminar**"; "**k-ε**"; "**k-ω**"). In the model"**k-ε**" we tested the variants **k-ε Standard; k-ε RNG** and **k**ε Realiz**able**. In the model "**k-ω**" we tested the variants **k-ω Standard and k-ω SST** [4].

For solution of above equations method of control volume was used.

4. Agreement of numerical simulation with physical experiment

Experimental part deals with propagation of natural gas into free space. It is, therefore, necessary to define in simulation that this is a mixture of natural gas with air. Database of the program Fluent contains only the mixture of air and methane [3]. It is possible to add other components of natural gas. This step would probably slow down the calculation due to higher number of unknown quantities and thus of calculated equations.

The used Transit natural gas contains 98.39 % of methane [6]. By comparison of densities of methane from the program database ($\rho_{27°C}$ = 0.6679 [kg/m^3]) and of Transit natural gas from literature [6] ($\rho_{20°C}$ = 0.680; $\rho_{30°C}$ = 0.658 [kg/m^3]) we can see a very good agreement. Thanks to these facts it is possible to consider this simplification to be acceptable.

Before describing propagation of gas in an enclosed space it was necessary to verify correctness of numerical simulation. The diagrams below present the results of six mathematical models with modifications approaching best the real flowing, which were compared with measurements. Diagrams in figures show dependence of the change of concentration on response time in the detectors Nos. 2 and 4 (Fig. 6 and Fig. 7).

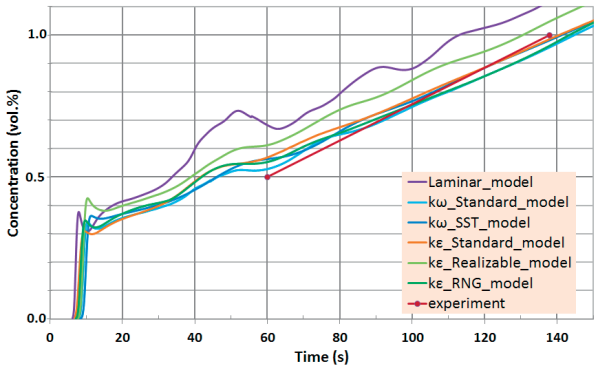


Fig. 6 Dependence of concentration change on response time of the sensor No. 2 [5]

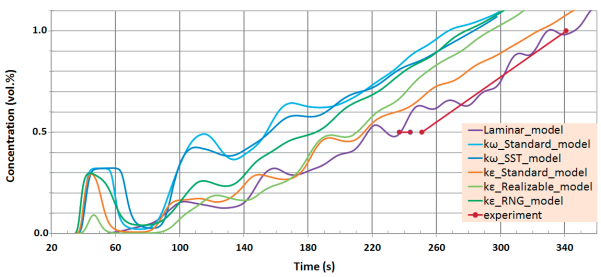


Fig. 7 Dependence of concentration change on response time of the sensor No. 4 [5]

It can be generally seen from the results that concentration first steeply increases and approximately at achievement of 0.3% to 0.5% of concentration the methane concentration further smoothly increases at tracepoints. Only at the fourth tracepoint the concentration steep increase again steeply decreased. After elapsing of several seconds it started again to increase smoothly. At the tracepoint No. 4 we can also observe a slight drop of concentration right before achievement of the 0.5% of concentration (model k-ε standard) and after it (laminar model). This phenomenon agrees with the measurement since at some measurements really only a glimmer took place and only after a while the diode signalling concentration of 0.5 % started to be lit permanently (Fig. 7).

5. Propagation of methane in an enclosed space

For the next evaluation of methane propagation through the space we took into account only the mathematical model „k-ε Standard“. This model was chosen due to its best agreement with the experiment.

Leakage of methane is visible on two created surface (sections through the whole calculation system). It is the surface on the axis ”z“ which passes through the centre of the pipeline, and surface on the axis ”x“ which intersects the centre of the hole from which methane leaks into the vessel. Range of the plotted contours, shown on created surfaces, is 0.5 to 1 vol. % concentration. The evaluation is, furthermore, completed with location of voluminal concentration 0.5% (blue) and 1% (red) in space.

Figure 8 shows direction of gas propagation during experiment. The hole was turned under the angle of 45°, that’s why methane propagated first to the detector No. 1 which signalled formation of 0.5% voluminal concentration. The gas then propagated along the wall to the top of the vessel. As soon as methane reached the top, it started to propagate to side walls, containing the detectors Nos. 5 and 6. Shortly after reaction of the first stage of the detector No. 2 (concentration of 0.5%), the velocity of gas propagation along the top of the vessel considerably dropped. On the rear wall (wall with detector No. 3) the flow of natural gas swirled. It is evident from the right bottom corner of the image (Fig. 9) that methane did not propagate along both side walls in a uniform manner. Methane flow, propagated along the right top part of the rear wall, reached the sensor No. 3 much more quickly than the gas flowing from the other side.

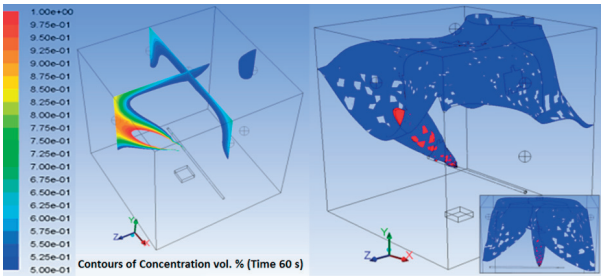


Fig. 9 Local concentrations during reaction of the sensor No. 3 (0.5 vol. %) [7]

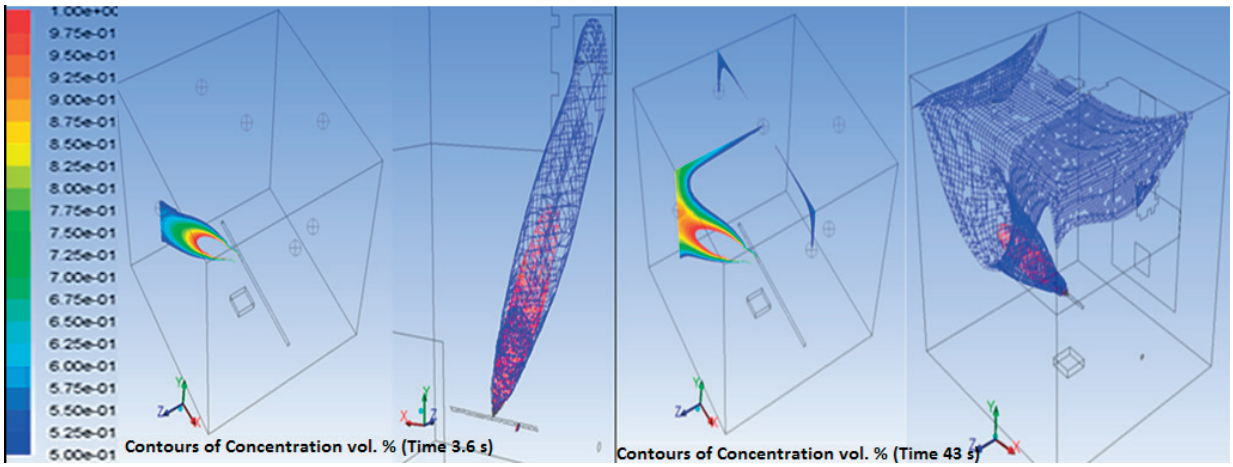


Fig. 8 Local concentrations (0.5 vol. %) during reaction of the sensors Nos. 1 (on the left) and 2, 5 and 6 (on the right)

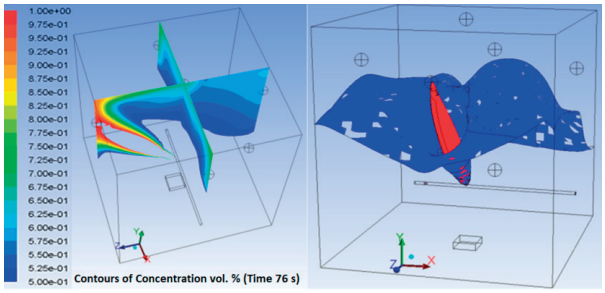


Fig. 10 Local concentrations during reaction of the sensor No. 1 (1 vol. %)

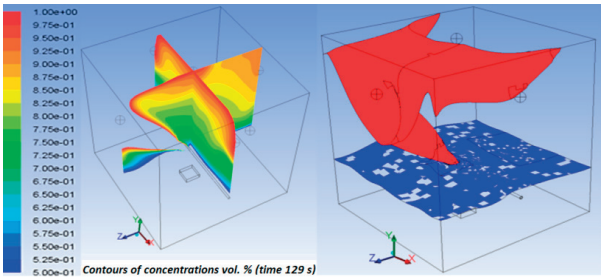


Fig. 11 Local concentrations during reaction of the sensors Nos. 2, 5 and 6 (1 vol. %) [7]

At the time after detection of the sensor No. 3 (0.5% of voluminal concentration) the gas propagated slowly along the rear wall downwards. Large swirl took place in the left part of the vessel (blue bulging on the right side, (Fig. 10). Figure 11 shows location of concentrations during the subsequent reaction of the sensors Nos. 2, 5 and 6 (1% of voluminal concentration). At that time the concentration of 0.5% already settled in one almost horizontal level. Drop of the level of 0.5% was already very slow, unlike the level of 1%.

During detection of the last detector (No. 4) both levels were almost horizontal and they slowly shifted downwards. The right top corner of the image (Fig. 12) shows that concentrations of 0.5% and 1% were created also in proximity of the hole from which the gas leaked, and that they were continuously connected with the levels by bended cones.

At the time of completion of the experiment both levels were under the pipeline which supplied methane (natural gas) into the vessel.

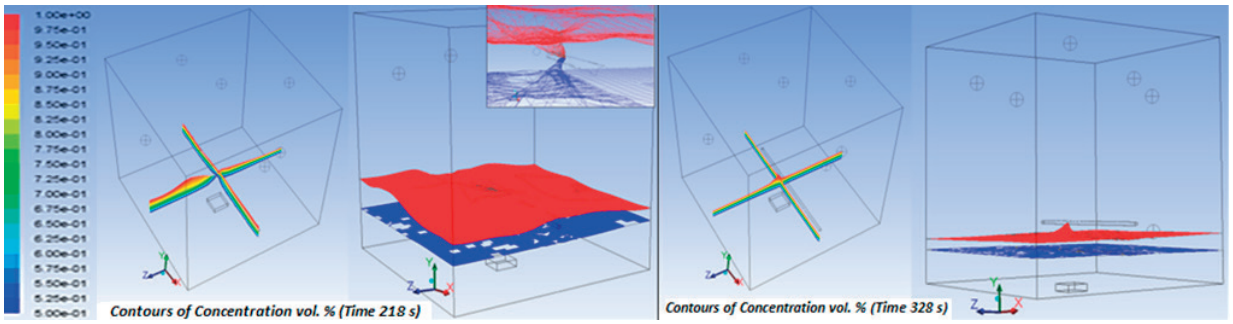


Fig. 12 Local concentrations during reaction of the sensor No. 4 (0.5 and 1 vol. %) [7]

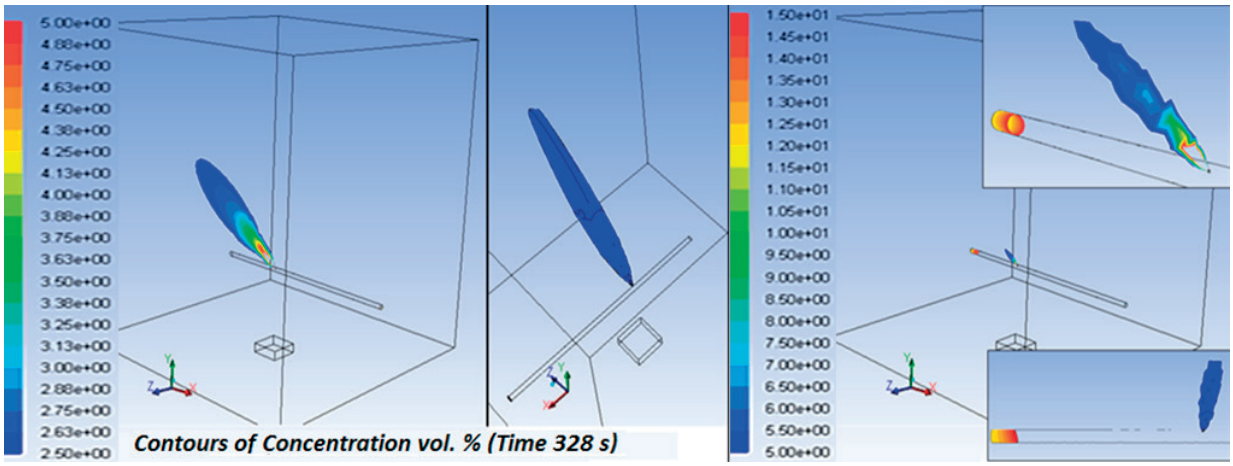


Fig. 13 Dangerous (on the left) and explosive (on the right) concentration right before the end of experiment

6. Formation of dangerous and explosive concentrations at gas escape

The question of safety of experimental measurements was a big issue. The first variant of safeguard consisted in replacement of natural gas by non-inflammable gas. This variant was rejected due to measurement of concentrations at maximum around 20% of the lower limit of explosiveness of natural gas and it was assumed that no explosive concentration should create. The vessel was moreover flushed after each measurement on open air in order to ensure safety during repeated measurements by venting the accumulated gas.

At the end of experiment (reaction of the last sensor) a question arose whether dangerous concentration (50 % of the lower limit of explosiveness) or even explosive concentration of methane was not already created in the measuring vessel, which would make the measurement dangerous for the persons near the vessel. For these reasons we monitored also formation of local dangerous and explosive concentrations. Natural gas is explosive when it reaches concentration of 5 to 15 voluminal percentage [6]. Two spatial levels were created in the program Fluent, which depicted dangerous concentration (2.5 vol. %) and lower limit of explosiveness (5 vol. %). The explosive concentration is moreover depicted in the plane intersecting the axis x. Its location is the same as in the case of evaluation, in chapter 6 ´Propagation of methane in an enclosed space´. Figure 13 shows distribution of contours with dangerous and explosive concentration.

Dangerous concentration was formed only as a paraboloid inclined under the angle of 45°. Figure 13 shows distribution of concentrations within the range of 2.5% to 5% of concentration (from the dangerous concentration to the concentration of the lower limit of explosiveness).

At the moment of termination of the experiment an explosive concentration was formed only in proximity of the leak (hole) from which the gas escaped, and in the pipeline at its blinded end.

7. Conclusions

Borders of local explosive and local dangerous concentrations were determined by mathematical CFD simulation. We obtained moreover a comprehensive image of manner of propagation and increase or decrease of concentrations of natural gas (methane) in the whole area of the given space. Correctness of the mathematical simulation was verified by experimental measurement during which voluminal concentrations of methane were measured at selected points.

So far the propagation of natural gas was investigated only in an enclosed space of simple shape, without internal structuring. Thanks to the good agreement of measurement with the simulation it is possible to move further and to investigate propagation of natural gas in larger spaces with much more complicated internal structure which would better correspond to real buildings or technologies.

The published procedures and results can be used for prediction at real accidents connected with gas leakage in production plants, in households, etc. It is, for example, possible to determine on the basis of numerical simulation the most probable places in which an initiation of explosive concentration could occur and at the same time also to estimate the strength of explosion.

Acknowledgements

This work was financially supported by the project of grant competition for students under the Reg. No. 030/2101/SV0304431, entitled “Quantification, propagation and distribution of inflammable gas-air mixture at explosion “.

References

[1] KOZA, V., CAPLA, L.: Determination of Leak Gas Amount from Damaged Gas Pipes, *Gas: Professional Periodical for Gas Manufacture*, vol. XC, No. 2, pp. 38-42, 2010.

[2] ZAVILA, O., BOJKO, M.; KOZUBKOVA, M.; DANIHELKA, MALEROVA, L.: *CFD Analysis of the Influence of Meteorological Conditions on Motion of Gas Ammonia in the Case of Emergency Release in Urban Development.* 11th Intern. Conference of Numerical Analysis and Applied Mathematics 2013 (ICNAAM 2013). 2127 September 2013, New York : AIP Publishing LLC, 2013. pp. 216-219. ISBN 978-0-7354-1185-2.

[3] Ansys, Inc. *ANSYS FLUENT 13.0 - Theory Guide,* 2010.

[4] KOZUBKOV, M.: Modelling of Fluid Flow, *FLUENT, CFX,* No. 1, Ostrava, 2008.

[5] TULACH, A., MYNARZ, M.: KOZUBKOVA, M.: *Study of Quantification and Distribution of Explosive Mixture in a Confined Space as a Result of Natural Gas Leak,* Intern. Conference Experimental Fluid Mechanics 2013, Liberec : Technical University, 2013, pp. 717-723, ISBN 978-80-260-5375-0.

[6] FIK, J.: *Natural Gas: Tables, Diagrams, Equations, Calculations,* Prague : Agency SSTZ, 355 p., 2006.

[7] TULACH, A., MYNARZ, M., KOZUBKOVA, M.: *Study of Distribution and Quantification of Flammable Gas in Confined Space,* Applied Mechanics and Materials. Switzerland: Trans Tech Publications, 2014, ISBN 978-3-03835-258-7.

Katarina Holla - Maria Simonova - Jan Kandrac - Stanislav Maly - Andrew Collins *

RESULTS AND CONCLUSIONS OF THE PROJECT "COMPLEX MODEL FOR RISK ASSESSMENT AND TREATMENT IN INDUSTRIAL PROCESSES" (MOPORI)

This article deals with selected results and conclusions which were achieved in the project APVV 0043-10 MOPORI during more than three years of its solution. The area of major industrial accidents prevention is very specific and concerns all EU member states. At the beginning we will describe the current state and bases of the project together with identification of the problem areas. In the next part we will aim at describing the algorithm created for assessing and managing the risks. Here we implemented suitable qualitative and quantitative methods and we will explain its applicability. Subsequently we will present software means for creating scenarios and assess the currently realised application of the model. This application is an inevitable part for verifying the procedures and schemes created.

Keywords: *Industrial Accidents Prevention, SEVESO, Complex Model, MOPORI.*

1. Introduction

The Slovak Republic with its area is relatively a small country compared with other European states. However, its small territory does not guarantee that major industrial accidents do not concern our country. The industrial production has a significant share of the Slovak economy and on 22nd August 2014 83 companies belonged to the SEVESO directive. Out of this, 38 companies is in the lower A category and 45 belong to the higher B category [1].

In the EU the area of the major industrial accidents prevention is adapted according to the SEVESO directive. The adaptations of the directive have followed the long-term development since its introduction in 1982 until now. Thanks to more and more sophisticated system of communication, information flows about accidents and also feedbacks from the industrial enterprises and citizens it has been possible to adapt the directive in the form we know today. Slovakia adopted the directive SEVESO II and implemented it to its legislation in 2002 when the law No 261/2002 Coll., about major industrial accidents prevention and implementing regulations were adopted. In this way the directive SEVESO II was implemented into the system. Currently in Slovakia there are working meetings which prepare a new law about accidents and this new law will transpose the directive SEVESO III to our national legislation – this new law will become effective on 1st June 2015. The new rules will strengthen the legal regulations in the area of major industrial accidents prevention and ensure the necessary high level of protecting lives and health of people as well as our environment [2].

The current time period creates space for implementing new approaches in the area of processing the safety and security documentation. One of the problem areas is also assessment and management of risks and this fact has been documented in several regulations and documents [3 and 4]. Based on the changes in process and problems in the area of assessing and treating risks the team at the Faculty of Security Engineering at the University of Zilina decided to submit a project under the name "Complex Model for Risk Assessment and Treatment in Industrial Processes" which is kept on file under the number APVV 0043-10 and abbreviation MOPORI.

2. Results and Outputs of the Project MOPORI

The first step after accepting the project was to carry out a deeper and more comprehensive analysis of the then current state in the area of major industrial accidents prevention for to specify or to change the partial project goals. The main aim was to create a model which would respect the requirements of

* [1]Katarina Holla, [2]Maria Simonova, [3]Jan Kandrac, [4]Stanislav Maly, [5]Andrew Collins
[1]Department of Crisis Management, University of Zilina, Slovakia
[2]Department of Fire engineering, University of Zilina, Slovakia
[3]Risk consult s.r.o., Bratislava, Slovakia
[4]Occupational Safety Research Institute, Praha, Czech Republic
[5]Department of Geography, Northumbria University, Newcastle, Great Britain
E-mail: Katarina.Holla@fsi.uniza.sk

the European directive SEVESO and the routine procedures in Slovakia in the area of major industrial accidents assessment and treatment.

To fulfil this goal it was necessary to establish cooperation with institutions which deal with this area not only in Slovakia but also in other EU member states. They are Ministry of Environment – Department of Environmental Risks and Biological Security, Bratislava; Slovak Environmental Agency, Banska Bystrica; Risk Consult, s.r.o., Bratislava; Mondi SCP a.s., Ruzomberok; Evonic Fermas, s.r.o., Slovenska Lupca; Vyskumny ustav bezpecnosti prace, Praha; Institut krizoveho manazmentu, Praha; Disaster and Development Centre, Newcastle, UK. Specialists from these institutions created the *"Board of Experts"* which met regularly and organised workshops for the goals of the project to be fulfilled through brainstorming and other methods.

A further inevitability was to complete the *qualification requirements* of individual investigation team members who participated in creating the model and its implementation in the companies. They were certificates of the safety and fire safety officers, specialists in the area of major industrial accidents prevention and safety and security advisor ADR.

As we have said already, the first step was to analyse the current state in the area of major industrial accidents prevention. Important information and bases not only for creating the complex model but also for other tasks were summarised in the *monograph „Prevencia zavaznych priemyselnych havarii"(Prevention of major industrial accidents)* [2].

A chapter under the name "Statistical Research of SEVESO Enterprises" is part of this book. This document was presented in the form of a research report reviewed by the *Board of Experts*. The document was subsequently revised. Its partial results served as a basic material for preparation of the new law which will become effective in 2015. A statistical questionnaire was sent to 81 companies and 44 pieces were returned. Figure 1 shows the representation of individual lines of business [3].

Based on research results we can ascertain a few facts as follows (these conclusions were stated in the case of questions answered minimally by 50 % of companies/responders):

- the level of collaboration of eligible and authorised safety persons with the company management is very good,
- the methods ETA, FTA and security and safety inspections are used in the framework of utilising the methods and techniques,
- almost unambiguously the companies require sending the safety documentation by electronic mail,
- Excel and Aloha are the software means/environments used by the companies,
- from the point of view of the costs for major industrial accidents prevention the companies spend 0 – 20,000 EUR,
- the majority of the companies involved has a company ranked in the risk area in its neighbourhood and collaboration between them is generally good,
- the companies evaluate the collaboration with state administration bodies as very good, etc. [3].

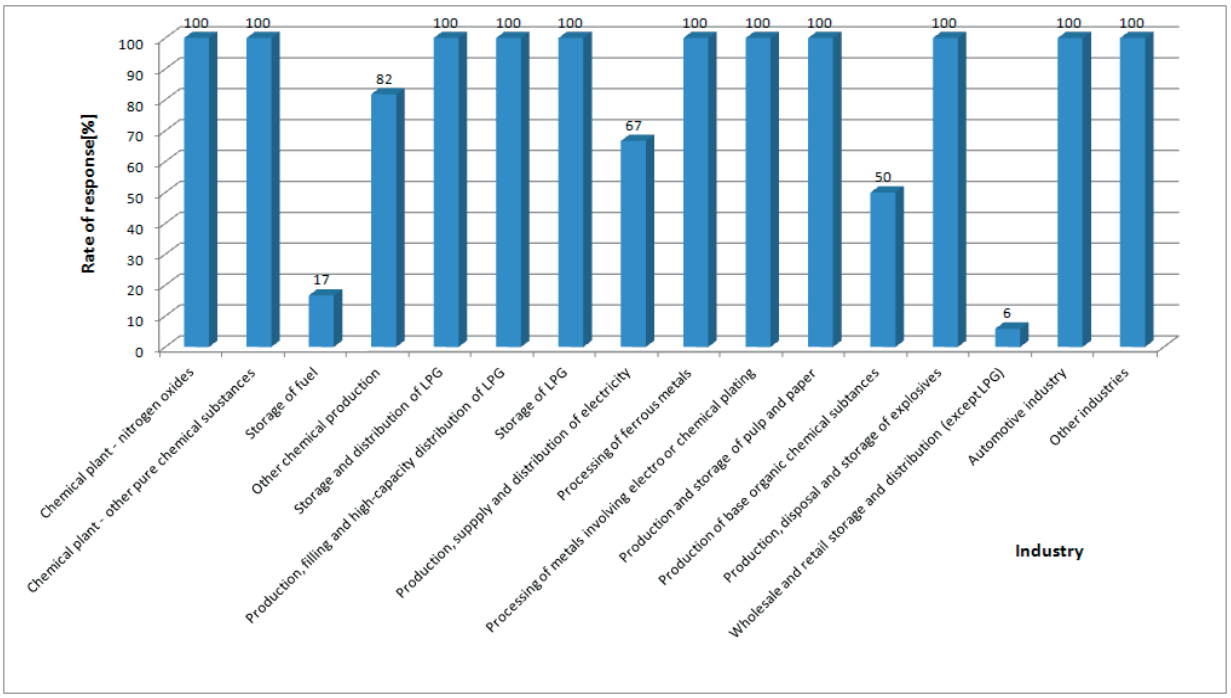


Fig. 1 Rate of return of the questionnaires according to lines of business [%] [3 and 10]

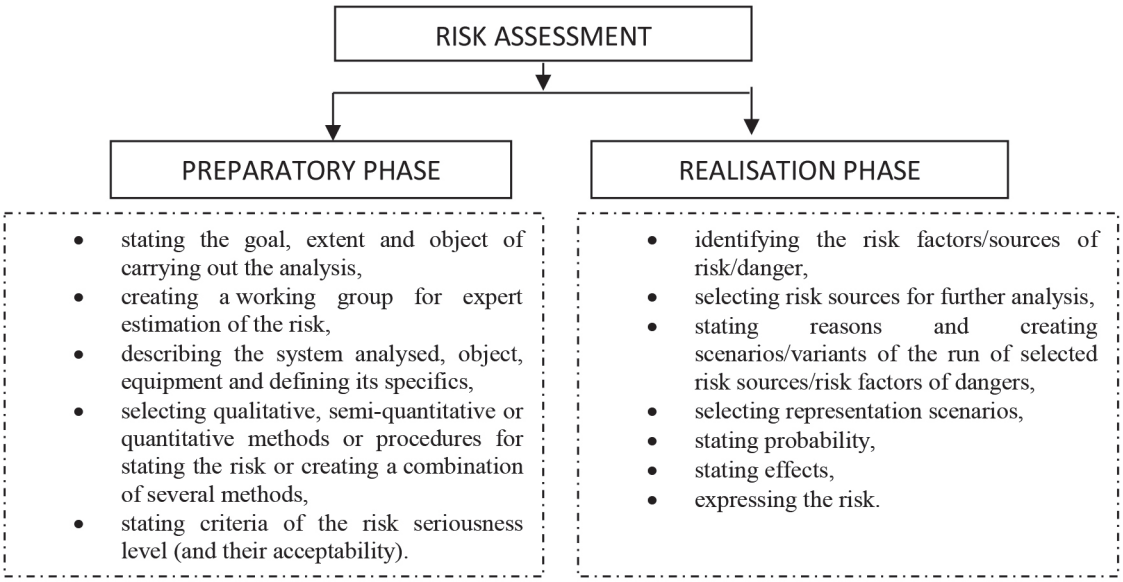


Fig. 2 A simplified model for risk management assessment

All results and conclusions of the current state analysis entered the second phase of the project solution, i.e. creation of the *Complex Model for Risk Assessment and Treatment*. At the beginning the individual model phases were defined and for each model phase steps of the model were determined. Procedural development diagrams for individual model phases were created. Methods/parts of systematic procedures were implemented into individual steps of the model and subsequently the functional dependences between individual phases and steps of the model were defined. Based on the detected assumptions and the analysis of the currently used reference but also modern approaches/methods a model for assessing the industrial processes risks which was verified on the basis of a practical application in two SEVESO companies was designed and created. This complex model is based on development diagrams and is too extensive; therefore, we introduce only its simplified version (see Fig. 2).

Methods and techniques which are utilised not only in the systematic procedure ARAMIS but also those which were assessed as suitable for usage in the model on the basis of the research were integrated into individual steps of the complex model [5]. The software programme ***iMotylik*** (iButterfly) was created in the framework of this step. It represents a new approach and connection of FTA and ETA which had pre-defined causes and effects in the ARAMIS approach. They were transferred to the

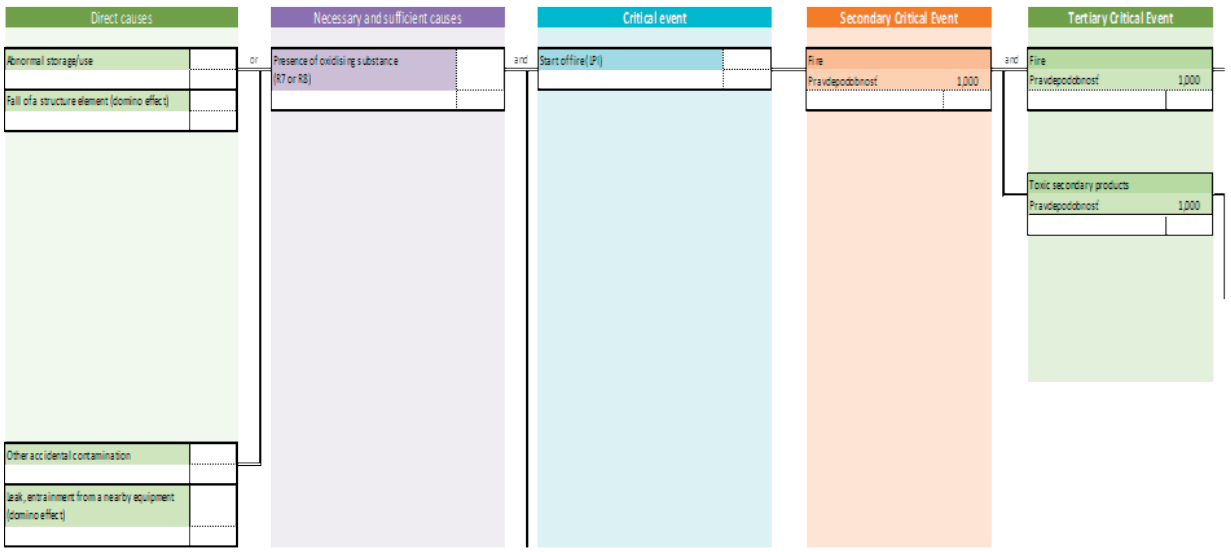


Fig. 3 Cut – out of A bow tie start of fire

software and the calculation relations based on Boolean algebra and other calculation relations were completed [6]. Innovative approaches to simplify the utilisation of the means by end users were introduced. This software was created on the basis of research activities of the MOPORI project where all generic trees were formed in the Excel environment (the environment chosen on the basis of statistical research 2013 – Holla et al., 2013) according to the causes, effects and impacts pre-defined in the ARAMIS approach and adapted according to currently used approaches in Slovakia. There are 47 of them. One of the simpler trees created in the MOPORI framework – iMotylik (the tree is part of the software iMotylik) is depicted in Fig. 3. It is a bow-tie with a critical event – "start of fire".

In the next step we will determine the development of leakage, explosion and fire of hazardous substances which is simulated by the software ALOHA and based on this it is possible to determine impacts on life, health, property and environment. After using the scenarios (bow-tie diagrams) only those branches which have a potential to develop to a major industrial accident are selected and they are then assessed (unacceptable risks) - Fig. 4. At the end measures for reducing the unacceptable risks are designed. In this risk matrix there are depicted frequencies (y axle) and impact categories (x axle).

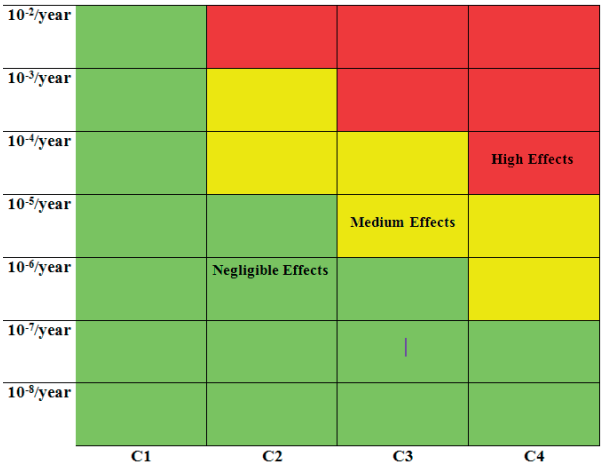


Fig. 4 Final risk matrix [5]

A complex model and its description are much more extensive and complex and a special document which will serve as a methodological aid for its implementation will be issued.

Implementation of the Complex Model and Software in SEVESO Companies

The model has been implemented in two SEVESO companies in Slovakia - EVONIC Fermas s.r.o (further only Evonic) and Mondi SCP Ruzomberok a.s. (further only Mondi). Both companies belong under the law about major industrial accidents prevention. The aim was to verify the operation of the complex model and software *iMotylik* in practice and to compare if the approach designed in the project is simpler and more systematic than that one which was used in the companies before. Two teams were created and each of them dealt with one application. The first results are ready and at the end of September there will be a meeting where the results will be compared and corresponding conclusions taken. Partial results are introduced in the further text. *Evonic* orients on producing bio-technological products, predominantly amino acids using fermentation processes. From the point of view of the directive SEVESO II/SEVESO III they work only with one hazardous substance in a greater amount – 28 – 31% solution of ammonia water. First of all it was necessary to carry out comparison tests in the lab of the Faculty of Security Engineering in Zilina concerning the speed of ammonia evaporation at a certain temperature (see Fig. 5).

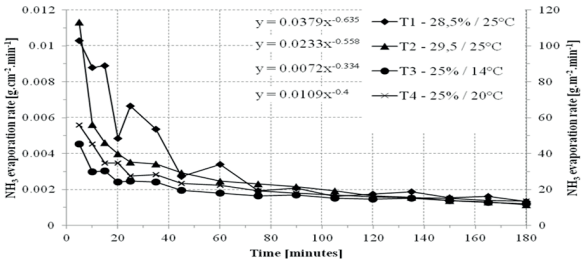


Fig. 5 NH_3 Evaporation rate as function of time [7]

The diagram confirms a strong dependence of the evaporation rate on the concentration of the ammonia solution as well as ambient temperature. Since T1 and T2 were both conducted with a higher concentration and at a higher ambient temperature, the rate of evaporation is greater (mainly in the first 10-20 minutes). Following the initial period the evaporation rate quickly drops down and the differences between the individual tests are much smaller. The effect of the higher concentration and ambient temperature is still observable. At 5 minutes the highest evaporation rate (T2/113 $g.m^{-2}.min^{-1}$) is approximately 150% higher than the lowest one (T3/45 $g.m^{-2}.min^{-1}$). For comparison, at 20 minutes the difference drops to 100% and at 45 minutes to 50%.This behaviour is most likely attributed to the self-cooling of the sample due to ammonia evaporation [7].

During the further phase we assessed the risk through the complex model and several conclusions were indicated. Although the company (when we assess the social acceptability) still does not belong to the socially acceptable risk, the implementation of the model and selected parts of the methodology of the complex model and taking into account the adopted organisational and technical measures (water screen in the store of the ammonia water) showed interest of the operator to take systematic

measures to suppress the risk of great leakages of the ammonia water and the gaseous ammonia. At the same time the creation of the barriers (water screen, emergency team of the operator and intervention of a professional fire brigade) has also reduced the occurrence frequency of emergency scenarios leading to the most serious threats.

The other company *Mondi a. s.* is a paper producer with headquarters in Ruzomberok. They work with several hazardous substances and therefore it was necessary already at the beginning to carry out a thorough selection for the implementation not to be too extensive. We agreed with the company representatives to work out a model application on the regeneration boiler EK2. We decided for this device because it is an operation where the processes require using several hazardous substances and also due to the fact that MONDI SCP currently builds another regeneration boiler, i.e. a current analysis of this equipment is necessary. In the framework of the overall analysis according to the designed analysis there were several consultations and meetings with specialists and MONDI SCP top management as well as process engineers of this enterprise. The implementation was realised according to the aforementioned procedure and without any complications. For the time being, the last implementation phase is running – we will have to define the consequences and their seriousness. After completing the implementation we will compare the original approach and the new designed one for us to be able to assess the effectiveness and benefits of the methodology designed by the MOPORI project.

Both applications are worked out in independent documents which have several tens of pages and it is impossible to describe them in this article in detail. However, it is possible, even now, to identify a few conclusions which have resulted from the analysis:

- the results of assessment by both approaches differed only minimally, however, they were different in the structure of the required inputs,
- different allocation of correct devices to typological machines in the framework of ARAMIS,
- the left side of the cause tree was not filled/developed due to availability of frequencies of critical events from generic databases,
- the complex model is more structured than the procedure utilised before,
- the complex model is less difficult and less time-demanding,
- the persisting problem of both approaches during final assessments of the effects of occurrence and impacts of major leakages on the inhabitants living in the surroundings.

4. Conclusion

At the end it is necessary to assess the results achieved by the project during three years of its solution. First of all it is necessary to point out that the monograph "Prevention of Major Industrial Accidents" will serve not only the enterprises which belong to the SEVESO companies in Slovakia, but especially the students of the Faculty of Security Engineering of the University of Zilina in the subject "Risks of Industrial Processes" which will be taught after its accreditation in 2015. The signed memoranda about collaboration which are based on real collaboration of the Faculty of Security Engineering of the University of Zilina with companies and creating space for student stays in these institutions will have further value added for the occupational growth of the students. The "Statistical Research of SEVESO Companies" served not only as a basic material in the project framework for processing individual phases and steps of the model, for applications of methods and parts of systematic procedures but also as a basic material for the Department of Environmental Risks and Biological Security at the Slovak Ministry of Environment. E.g. the newly-prepared law about major industrial accidents prevention which will become effective in 2015 will include sending/delivering the safety and security reports in electronic form – the companies declared this in the research unambiguously. A significant step was the creating of the complex model for assessing and managing risks which offers an alternative for the companies to process the problem part of the security and safety documentation [8]. Already today, after the implementation, it is possible to declare that the complex model offers an alternative which is more systematic and from the point of view of time less demanding (if we master the methodology) than the previous model – and this was at the same time the goal of the project. The management of crisis situations is undergoing rapid changes due to advances of Information Technology [9]. The software has also a value added. It contains generic tie-bow diagrams which demonstrate the causes, effects and impacts of a critical event which can lead to a major industrial accident. After removing errors and inaccuracies in the complex model this procedure could be utilised by several companies especially in connection with assessments of security reports and categorisation of companies in 2015.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-0043-10"

References

[1] Information system of PZPH [online]. [cit. 4.5.2012].Available at: http://www.enviroportal.sk/environmentalne-temy/starostlivost-o-zp/pzph-prevencia-zavaznych-priemyselnych-havarii/informacny-system-pzph

[2] HOLLA, K., KAMPOVA, K., SIMAK, L., SIMONOVA, M., MIKA, V. *Major Industrial Accident Prevention,* Zilina : University of Zilina, 2013, 147 p., ISBN 978-80-554-0786-9.

[3] HOLLA, K. et al.: *Statistical Survey of SEVESO Establishments in Slovak Republic: project APVV-0043-10 Complex Model for Risk Assessment and Treatment in Industrial Processes*, Faculty of Special Engineering: University of Zilina, 22 p., 2013.

[4] SALVI, O. et al: F – SEVESO, 2008. *Study of the Effectiveness of the Seveso II Directive,* Brussels : EU - Vri, 2008.

[5] *The Framework Programme Accidental Risk Assessment Methodology For Industries in the Context of the Seveso II Directive* [online]. 2004. [cit. 25.6.2012]. Available at: http://mahb.jrc.it/fileadmin/ARAMIS/downloads/ARAMIS_FINAL_USER_GUIDE.pdf

[6] KITTEL, L., LOVECEK, T.: Passive Protection Elements Breach Resistance Modeling. *Communications - Scientific Letters of the University of Zilina*, EDIS : University of Zilina, 2011, ISSN 1335-4205.

[7] MOZER, V., HOLLA, K., BUGANOVA, K.: Determination of Ammonia Evaporation Rates for MOPORI Project Model. *Advanced Materials Research,* vol. 1001, 2014, p. 458-462, ISSN 1022-6680.

[8] ZANICKA HOLLA, K., MORICOVA, V.: Human Factor Position in Rise and Demonstration of Accidents. *Communications - Scientific Letters of the University of Zilina,* vol. 13, No. 2, 2011, pp. 49-52, ISSN 1335-4205.

[9] RISTVEJ, J., ZAGORECKI, A.: Information Systems for Crisis Management - Current Applications and Future Directions, *Communications - Scientific Letters of the University of Zilina*, vol. 13, No. 2, 2011, pp. 59-63, ISSN 1335-4205. 2011.

Bohus Leitner - Maria Luskova - Alan O'Connor - Pieter van Gelder *

QUANTIFICATION OF IMPACTS ON THE TRANSPORT SERVICEABILITY AT THE LOSS OF FUNCTIONALITY OF SIGNIFICANT ROAD INFRASTURUCTURE OBJECTS

Incidents and unexpected phenomena occurrence in transport significantly affect the performance and capacity parameters of traffic infrastructure and its important objects. The objective of this article is to indicate possible uses of software tools to model the traffic at the loss of functionality of potential elements of critical road infrastructure and to demonstrate the possibility of their efficient use. The conducted case study applied the simulation models for quantification of the infrastructure traffic load under standard conditions as well as during the constraint of the transport system operation, i.e. after implementation of restrictive conditions (e.g. considering shutdown of an important bridge). The solution of the situation at the shutdown of an important element of infrastructure is possible to be designed, verified and modified using appropriately devised adequate virtual models. By this means, it is possible to predict the significance of the shutdown – criticality and influence of the loss of the functionality considering the transport serviceability parameters of the road infrastructure in the affected area.

Keywords: *Critical road infrastructure, loss of function, traffic modelling, traffic flow, transport serviceability, incident.*

1. Introduction

In Slovakia, the problem of complex risk management in the field of critical traffic infrastructure is quite new. In addition to the specific legislative framework [1], which defines the basic terminology and the necessary information base focused on the sectors and sub-sectors of critical infrastructure (CI), there is no singular methodological approach designed for objective identification of the elements of so-called critical infrastructures in defined areas so-called sectors. We notably absent the complex methodology, which would enable the conduction of the risk analyses and quantification of the impacts associated with the loss of functionality of important elements of traffic infrastructure, considered as "potentially critical".

Within the transport sector, in the field of threat identification and risk assessment of the potential elements of critical infrastructure, there is a methodology developed, which integrates main phases of the risk management of potential objects of CI in the road and rail transport.

The purpose of this methodology is to define the set of typological markers, criteria, approaches and methods suitable for implementation of the process of CI elements identification to the design of efficient systems of security measures, reducing the probability of the loss of infrastructure functionality to an acceptable level. The methodological approach generally comprises of three basic areas according to Fig. 1.

Phase 1: Identification of the species and types of traffic infrastructure objects, destruction of which would have a significant negative impact on the assurance of basic functions of the transport system.

Phase 2: Defining the most probable threats leading to the dysfunction of the potential objects of the road traffic

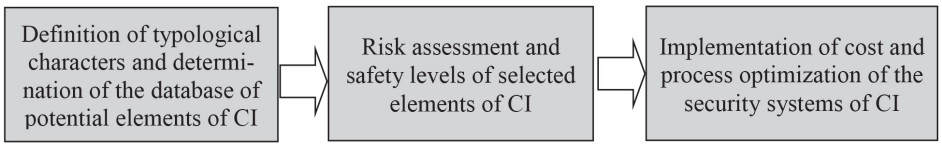


Fig. 1 Basic phases of applied methodology [authors]

* [1]Bohus Leitner, [1]Maria Luskova, [2]Alan O'Connor, [3]Pieter van Gelder
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]Department of Civil, Structural & Environmental Engineering, Trinity College Dublin, Ireland
[3]Safety and Security Science section, Delft University of Technology, The Netherlands
E-mail: Bohus.Leitner@fbi.uniza.sk

infrastructure [2], prediction of the risk exposure [3] and the assessment of the possibilities to minimize the threats of individual types of infrastructure objects [4].

Phase 3: Estimation of the time for recovery of the CI objects due to the loss of their functionality [5], assessment of their temporary replacement, alternatively their detour using traffic modelling [6]. An important task is to optimize the protection of important subject using existing traffic management systems, intelligent traffic systems [2] as well as new ways of object protection in order to reduce the impacts of the loss of functionality of a traffic system element.

The article presents the most important results of the conducted case study. Its objective is to demonstrate the possibilities and efficiency of using traffic flow modelling when assessing the importance of the road infrastructure object and quantification of the influence of the object's functionality loss on the traffic load of a part of road infrastructure. For comparison, we tracked the capacity and performance parameters of the road infrastructure under standard conditions and particularly in the situation when the operation of the traffic system is limited, i.e. after the introduction of restrictive conditions (e.g. shutdown of a bridge).

2. Traffic modelling and tools for analysis of the traffic flow models

Modelling traffic by the means of appropriate software represents an efficient method in the field of transport engineering. Their use not only involves the simulation of the traffic control itself, but it represents a set of tools from simple single-purpose application to complex systems for implementation of intricate analyses of the traffic networks and processes. Simulation models of the traffic flow were created as a tool for theoretical recognition of the influence of various factors on the analysed values of the basic traffic characteristics as well as for on-line identification of some parameters such as capacity of the flow movement in various conditions, investigation of the influence of an accident on the traffic flow behaviour, quantification of the length of column before the restriction of the network etc. [6].

Currently, specialized software products are being used for traffic problem solutions (e.g. *Getram/Aimsun, PTV Vissim, OmniTrans* and many others). These tools have vast possibilities of simulations, settings and other useful functions and, in a relatively short time, it is possible to simulate numerous scenarios of a traffic situation and run calculation of efficiency parameters of certain sections or individual objects of the traffic infrastructure. Using simulations makes it possible to model actual and prospective state of the traffic in selected traffic mode, as well as state of operational load of selected sections and elements of the road network. The mentioned software most frequently uses either microscopic dynamic simulation of the traffic which simulates behaviour of an individual vehicle in the flow or macroscopic principle which characterizes the traffic flow globally by the means of selected characteristics [7].

In the realization phase of the case study, the simulation tool *OmniTrans* [8] was used. This software tool is designed for macroscopic modelling of medium sized and large networks and involves all modes of the road traffic, i.e. so-called multimodal modelling tool. The software is suitable for prediction and solution of a traffic congestion and its impacts on the roads linking neighbouring agglomerations or impacts on individual areas – so-called *traffic districts*. Dynamic models enable us to create congestions in virtual environment in selected timescales and during modelling of several variants, they allow their cross comparison and assessment of solutions [9].

3. Impacts on the transport serviceability in adjacent areas due to the functionality loss of an important object of the road network

The form of the case study was selected to demonstrate efficiency of the use of software tools for traffic modelling when assessing the criticality of road infrastructure objects and expressing the impacts of their potential failure. The study was based on the assumption of the occurrence of a negative phenomenon and its influence on transport services and resulting changes in the capacity of the monitored road network sections. The first task solved was a model representing the normal operating conditions - traffic infrastructure without restrictions. The second tasks deals with a temporary restriction of the transit over a bridge and resulting traffic situation. The last problem analysed is a case of long-term breakdown of the bridge with defining the alternative proposal of redirection of the vehicle flow to a traffic detour.

3.1 Problem formulation, description of the object and chosen location

Within the traffic system, various unexpected phenomena can occur due to the change of climate conditions and human activities such as increasing number of vehicles in the road traffic. Their consequences are mostly traffic congestion and resulting speed limitation of the traffic flow, partial or complete obstruction of the area etc. The objective of the case study is to demonstrate the benefits of the use of software support for quantification of the traffic flow parameters during solution of partial or complete restriction of the traffic at certain spot of infrastructure, e.g. bridge, road junction or tunnel.

Fig. 2 Chosen bridge [authors]

Sub-objectives of the case study:

- Calculation of the road network load at the selected location in the normal state (working day, morning peak, times: 7:05, 8:30 and 8:55 am).
- Prediction of the traffic load at the occurrence of a restriction on the selected object (bridge structure according to Fig. 2).
- Design of the optimal variant of detour and prediction of the traffic load after the implementation of the measures so that the traffic would flow smoothly.

Expected outcome of the study is confirmation or negation of the assumption that during the restriction of the traffic flow (e.g. due to decrease in transitivity of the selected object), after the implementation of the designed alternative solution, the adjacent roads will be able to serve required traffic demand in the area.

The selected road section (3rd class road III/5181 with the length of 1.25 km – beginning of the section is on *Rondel*, the end of the section is the intersection to *Horky*) is a main connection between the town centre of Zilina and residential district *Hajik*, suburb *Banova* and neighbouring villages *Horky, Brezany, Bitarova* and *Ovciarsko*.

As the important infrastructure object in this area we selected the bridge which allows vehicles to pass over the river *Rajcianka*. The reason to choose this object was the flood in 2010 on the river *Rajcianka* in the suburb *Zilina - Zavodie* when after long rains a flood activity of 3rd degree was declared (serious consideration was given to the restriction of the traffic on this object). In the selected area, there is one circular and 8 level intersections.

3.2 Input data and data collection

The data necessary to define the traffic matrix were obtained from the traffic survey. The traffic survey was conducted at the time from 7:00 to 9:20 am (11th April 2014, Friday – as a critical day of the week), on the streets *Horecka* and *Osloboditeľov*. The total sum of vehicles includes personal cars, lorries and public transport vehicles too. For illustration, the results of the survey on *Horecka Street* are provided in Fig. 3.

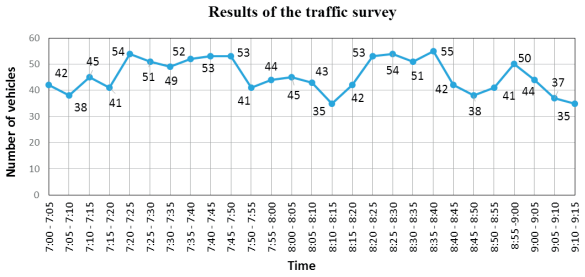


Fig. 3 The results of the traffic survey [authors]

In case there is no time to conduct the traffic survey, e.g. due to unexpected emergency situation, it is possible to obtain approximate information about the traffic flow from an older database. It is mainly the statistic data from the national census of traffic on the road network in Slovakia. The last traffic census monitoring the extend of the use of motorways, expressways, roads of 1st and 2nd class and some road sections of the 3rd class were conducted in 2010.

3.3 Preparation of the simulation model

Step 1. Inserting maps, plotting zones and defining districts

For more accurate plotting of the traffic network, it is useful to have a base map which would serve for drawing the transport network. As a base map, we used the map of the selected area from the portal Google maps. After inserting the base map, particular zones representing individual town districts were plotted in. After drawing the zones, we defined the so-called sectors, out of which the traffic flows will be directed. In total, 8 sectors were defined in the model (Fig. 4).

Step 2. Plotting traffic hubs, road network and defining intersections

After defining the zones and sectors, it was necessary to set so-called traffic hubs in order to create supporting traffic network. The traffic hub is usually placed on the base map at the road intersection. After defining the traffic hubs, it is necessary to define road sections between them which are usually named according to the actual street names.

When designing the road network and defining the performance and capacity parameters for particular road sections, we used the standard *STN 636110 Designing local roads* [10]. Equation for calculating the limit values of the traffic flow intensities is given as

$$\mathbf{l_p = l_z \times k_k \times k_s \times k_m \times k_b} \qquad (1)$$

when l_p is a value of admissible (design) traffic flow intensity in the vehicle per hour (veh/h), l_z is the basic value of admissible intensity of the traffic flow (veh/h), k_k is coefficient of the influence of the traffic-light controlled intersection, k_s is width

coefficient, k_m is manoeuvre coefficient and k_b is coefficient of very slow-moving vehicles.

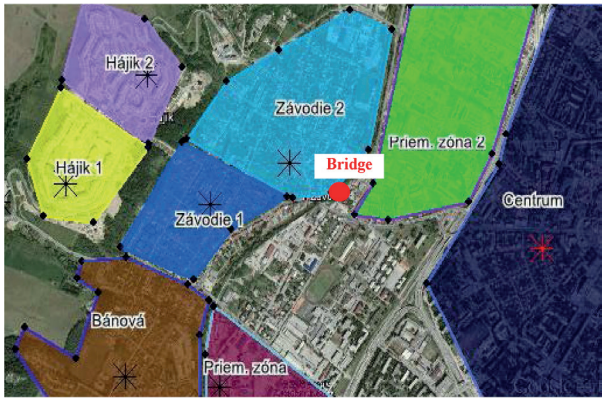


Fig. 4 Defining the zones and districts in the area [authors]

Coefficient values used at the designing of the simulation model:

l_z – v=50 km/h, longitudinal tilt 0-1.5%, 5% of slow vehicles is l_z*=1250 veh/h*,

k_k – when there is no traffic-light, therefore, the coefficient $k_k = 1.00$,

k_s – for one road lane, the width of the lane is 3.5 m, without the adjoining lane $k_s = 0.75$,

k_m – for one road lane in given direction we choose $k_m = 0.96$,

k_b – at 5% proportion of slow vehicles, the coefficient of the influence is $k_b = 0.9$ [3].

When we substitute these values into the equation (1) we get

$$l_p = 1250 \times 0.75 \times 0.96 \times 0.9 = \textbf{\textit{810 veh / h}} . \quad (2)$$

To be able to define the intersection in the traffic hubs, at least three road branches must interlink there. In the model of the road network in the area of interest, there were defined in total 8 intersections out of which one was a roundabout.

3.4 Defining the transport matrix and scripts

After the design of the road network model, transport links were defined into so-called *traffic matrix*. Typically, the input values, which were found or determined according to [11], give information about where the traffic flows begin and where they will direct. A very important part is to create a script of a programme task where *traffic network, input data* and *programme tasks* constitute basic elements for elaboration of the functional and adequate virtual model.

4. Simulation experiments with the traffic model of selected road network

Within our case study we created three simulation models, namely:

Model 1 = transitivity of the bridge without restrictions – normal state.

Model 2 = transit restriction over the bridge at the entry and exit from the sector *Zavodie*.

Model 3 = blocked bridge, detour suggestions and changes in traffic organisation.

All three models incorporated equations focused on the intensity of the traffic flow and density of vehicles on 1 km section at the maximum speed in the residential area *v=50 km/h*. For each simulation model, calculations were made in three timescales between 07:05 to 08:55 am. Due to limited extent of the article, only the outcomes of the analyses of Model 2 and Model 3 will be presented in more detail.

4.1 Simulation model 1 – cleared object without restrictions, normal state

The model is based on the assumption that the road sections considered are with no restriction. The most serious situation in the area usually occurs at about 8:30 (Fig. 5) when most of the roads surpassed the maximum intensity corresponding with the selected level of service for this type of road (approx. 810 veh/h).

According to the model, the worst situation occurs on the *Zavodska Street* in front of the roundabout where the traffic intensity reached the value of approx. 1650 veh/h. We note that all roads from the town districts and surrounding villages join there in the direction to the city centre.

4.2 Simulation model 2 – blocked bridge

The simulation model 2 deals with the blocked transit over the bridge which is on the entry and exit of the sector *Zavodie* and joins the *J. Zavodskeho Street* and *Zavodska Street*. By the modification of the model intersections we achieved that in the model, the bridge will be considered as impassable. The other conditions stay the same as in the simulation model 1. The simulation and the analysis showed that the situation is more complicated comparing to the conditions of the Model 1 (Fig. 6).

The intensity of the traffic in direction to the city centre is significantly higher. For example, the situation on *Zitna Street* reached twice as many vehicles as envisaged in the calculation. The intensity at 08:25 am comes to 1650 veh/h in direction to the centre and to the industrial zone. With very high probability, the predicted situation at that time would cause congestions. As in the case without restrictions (Model 1), even in the case of

Communi-cation	*J.Zavodskeho Street*	*Horecka Street*	*Zitná*	*Skultetyho*	*Priemyselna*
Density [veh / km]	106	83	72	56	56
Traffic load [veh / h]	924	1256	1096	436	959

Fig. 5 Model 1 – Traffic situation at 08:25 [authors]

Communi-cation	*J.Zavodskeho Street*	*Horecka Street*	*Zitná*	*Skultetyho*	*Priemyselna*
Density [veh / km]	0	132	55	44	46
Traffic load [veh / h]	0	659	1650	554	1217

Fig. 6 Model 2 – Situation at 08:25 with blocked bridge [authors]

Model 2, the worst situation is on the roundabout intersection. The worst conditions are on roads which connect the roundabout with *Rondel*. The traffic intensity is twice as high as the intensity intended for this road. The roads in *Banova* are below the established intensity, so there are not expected any significant problems in this area. At 8:55 am, the intensity on several main sections is even higher.

To compare the situation in the given sections, Fig. 7 shows certain parameters (density of the flow and traffic load of the road) during selected time sessions..

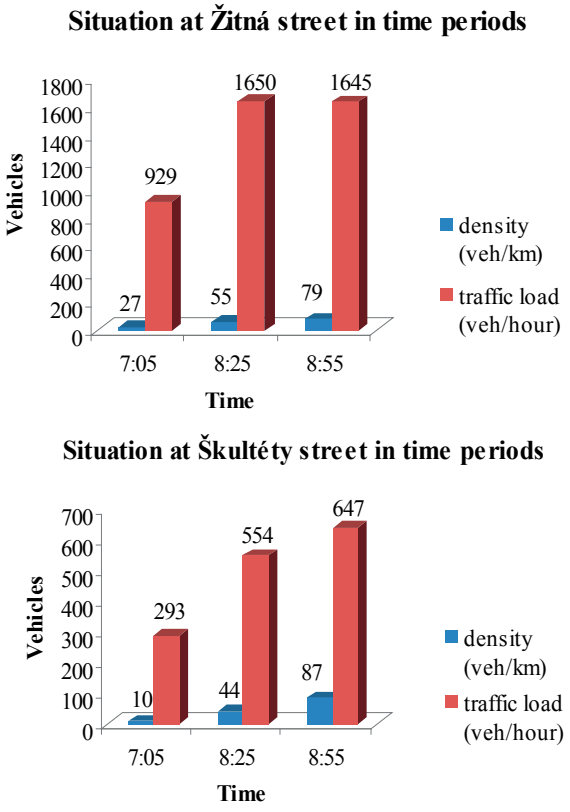


Fig. 7 Model 2 - situation on Zitna and Skultety [authors]

The values of the monitored parameters show that, in this case, the worst situation is on *Zitna* and *Skultetyho Street*. The situation is definitely caused by the breakdown of the bridge, with just these two roads being the only possible route to the city centre.

4.3 Simulation model 3 - blocked object, detour, change of traffic organization

A prediction resulted from the Model 2 showing how the situation would look like under restricted transit conditions over the bridge. Due to the blockage of the bridge, the traffic flow to the city centre from the direction of *Horky* and *Hajik 1*, *Banova* and *Zavodie* would pass through the *Zitna Street* and, consequently, through *Skultetyho Street*, alternatively through the street *Pri Rajcianke*. This natural solution would result into significant increase of the traffic load on these roads. It is based on the knowledge of the actual traffic behaviour. Usually, the most suitable solution used for the reduction of the traffic load is a diversion or distribution of the traffic load into other directions. One of the analysed solutions was to divert the traffic from *Hajik 1* through *Hajik 2* in direction towards *Priemyselna* to the roundabout (Fig. 8 blue). In the models 1 and 2, this route was not even considered, as it is twice as long and drivers, under normal conditions, often use the shortest routes (Fig. 8 red).

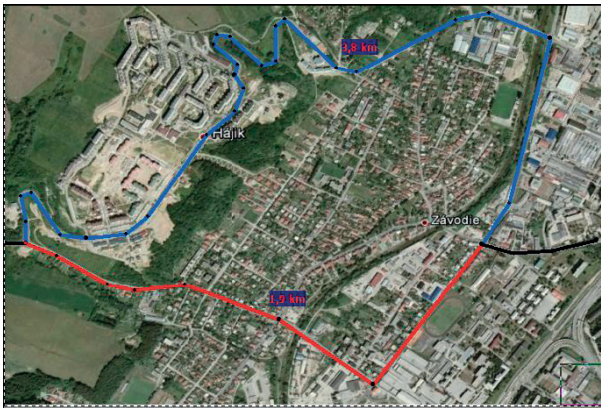


Fig. 8 Detours suggestion and routing of traffic flow [authors]

To avoid reduction of the planned traffic intensity in the area of interest, it was necessary to limit the transitivity of several roads. One of the modifications was a change of traffic organization on the roundabout junction of the *Skultety*, *Priemyselna* and *Zavodska* (Fig. 9).

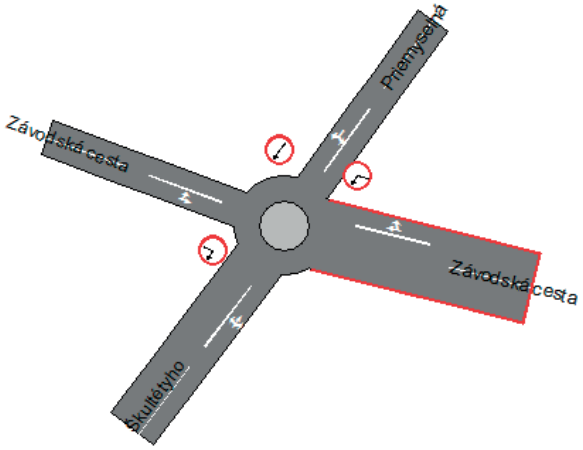
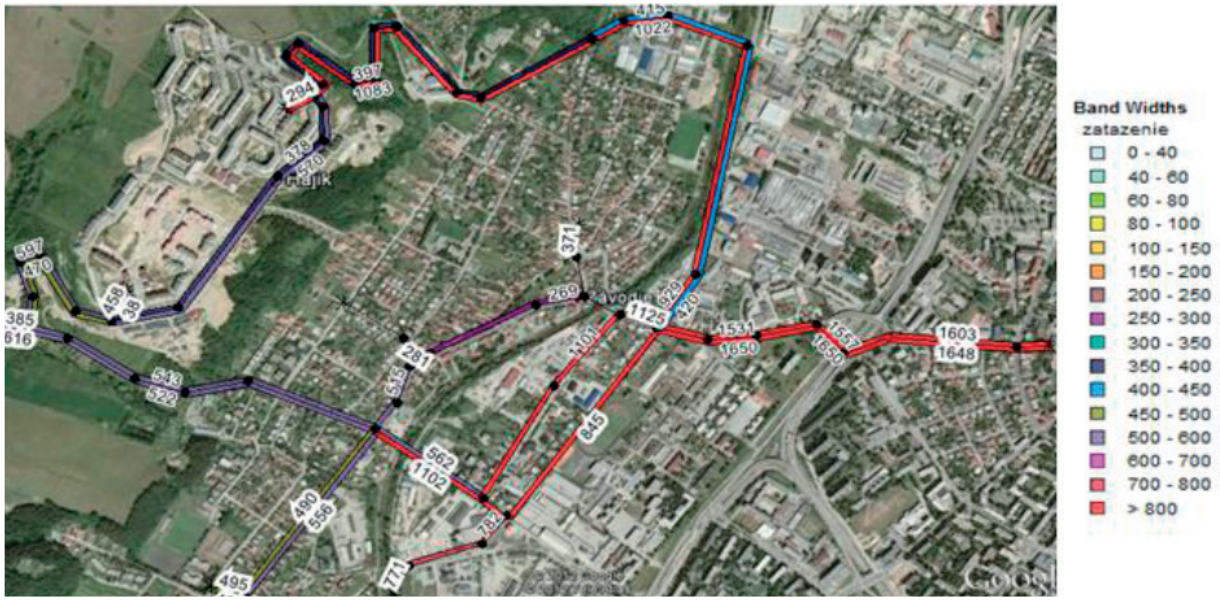


Fig. 9 Turn limitations on roundabout [authors]



Communi-cation	*Horecka Street*	*Zitná*	*Skultetyho*	*Priemyselna*
Density [veh / km]	185	179	118	132
Traffic load [veh / h]	522	1102	845	929

Fig. 10 Trafic situation at 8:25 using suggested detour [authors]

The proposed limitations and individual redirections in this case would be denoted by temporary vertical road signs, alternatively, during the first days, the traffic could be regulated by the traffic police. In case of implementation of these conditions in the Model 3, the traffic situation is stable. None of the roads is so overloaded to exceed the specified value of the traffic intensity. However, at 8:25 the estimated situation changes significantly.

As shown in Fig. 10, on *Zitna Street*, the traffic flow increased rapidly and the predicted intensity of vehicles rose to approx. 1100 veh/h. The traffic intensity between roundabout and *Rondel* is consistently high and, in this respect, it cannot be expected to reduce the traffic flow significantly. A slight increase occurred on *Priemyselna,* which could have been expected since the traffic from *Hajik* was redirected there.

4.4 Comparison of alternatives without (Model 2) and with the detour (Model 3)

In order to evaluate the impact of the proposed solution (inclusion of detours and change of two-way roads into one-way) it was necessary to compare the parameter values of the traffic flow. The results of the study lead to the assumption that the change in direction of the traffic flows and introduction of the alternative detour route had clearly positive effect on the transport services in the area and on the fluency of the traffic flow.

One of the most important results of the study was to demonstrate the possibilities to reduce the critical level of traffic load on *Zitna Street* and we can say that the detour and regulation of the direction of traffic flow had clearly positive influence on the traffic in the analysed part of the road network. Completion of the case study should involve experimentally verified characteristics of the traffic flow directly in real traffic. For example, if we implemented the considered blocking of the bridge and also all the regulatory and technical measures into practice and by the consequent survey determined the characteristics of the traffic flow and compared them with the predicted values.

5. Results summary and discussion

In case an emergency state with an impact on the transport system arises and it is possible to use simulation tools to verify or optimize the proposed solution, it is necessary to consider:

1. *How much time is needed to eliminate the consequences?* At situations, the effects of which are possible to be removed within several hours, max. days, it would be sufficient to plan a detour, divert traffic or reduce the transitivity of several roads, only on the ground of subjective assessment and

familiarity with the location. For longer lasting situation or before a planned reconstruction of the object, it is appropriate to use software in the phase of decision-making. This would enable us to define more variants of solution, experiment with the model and choose the most suitable variant [9].

2. *How much time is needed to obtain data and documents to design the most realistic model?* To create a traffic network we need maps. The most important are the values of transport links which define so-called transport matrix [12]. These data can be obtained from the traffic survey or certain sources from the field of transport [13]. However, it is necessary to compare the time needed to obtain it with the time dedicated to the problem solution. The more data has been collected, the more accurate and reliable the model will become.
3. *Possibilities and availability of a suitable simulation tool.* Software is not every suitable to simulate the situation. Therefore, it is appropriate to check the possibilities of its application as well as possibilities of realization and usability of the output format.
4. *Staffing the work with the model.* In order to consider the obtained result as relevant, it is necessary to have staff who will be able to perform design and analysis of solutions in as short time as possible and with the most precise outputs.
5. *Considering stochastic nature of internal - and external variables (such as human factor, weather conditions, traffic intensity, etc.) on transport.* In real traffic the state, parameters and dynamics of the traffic flow are influenced by other factors which are not taken into consideration by any simulation tool and any other intelligent traffic management system either [12]. The most important element affecting the overall flow of traffic is human behaviour as an element of the traffic system.
6. *Limited influence of random parameters of operating conditions in the road traffic.* Current state of meteorological conditions is another of the important factors influencing the traffic. Not always it is possible to consider such factors in the development of simulation model and, therefore, the results of the simulation experiments can be often doubted.

6. Conclusion

The risk of unexpected, mostly negative events in the traffic system is closely related to the increased intensity of the traffic as well as to the influence of meteorological, technological and social phenomena. The occurrence of these risks is conditioned by circumstances and phenomena usually of natural or technogenic character. However, the traffic infrastructure can be also influenced or restricted by planned reconstruction or repair of an important object or a section of the traffic infrastructure. The objective of our article was to demonstrate the possibilities of efficient use of software tools to model traffic when assessing the importance of an object of the road infrastructure.

The gist of determination of its criticality lies in the quantification of possible failure impacts on the traffic system functioning. In this case, the bridge structure near the centre of *Zilina* was selected. Based on the results of the application of simulation models to estimate the traffic load in standard but especially in specific conditions, it has been proven that the simulation methods have important place at the solution of the capacity problems of the traffic.

General solution of the problematic situation (particularly of long-term character) in the road infrastructure can be modified and verified according to the set requirements and restrictive conditions on adequate virtual models of the infrastructure and its important objects. Thus, it is possible to efficiently predict the importance and impact of the disengagement of important objects on transport services in the selected area of the road infrastructure. It is necessary to begin to promote the use of such tools. They streamline the work by fast and efficient suggestions and evaluations of more variants of solution are able to assist in choosing of the most suitable one.

Acknowledgements

The article was supported by the project APVV-0471-10 „Protection of critical infrastructure in the transport sector“, project „Centre of excellence for systems and services of intelligent transport II“, ITMS 26220120050, co-financed by the European Regional Development Fund and FP7 project „Risk analysis of infrastructure networks in response to extreme weather (RAIN)“.

References

[1] *Act 45/2011 of Coll. on Critical Infrastructure (in Slovak),* Bratislava : Slovak National Council.

[2] SIMAK, L., DVORAK, Z., GASPIERIK, L., KAMPOVA, K., REITSPIS, J., SEIDL, M., SVETLIK, J.: *Critical Infrastructure Protection in Sector Transport,* 1st ed., 180 p., University of Zilina, 2012, ISBN 978-80-554-0625-1.

[3] DVORAK, Z., RAZDIK, J., SOUSEK, R., SVENTEKOVA, E.: *Multi-agent System for Decreasing of Risk in Road Transport*. Proc. of the 14th Intern. Conference Transport means 2010, October 2010, Kaunas : University of Technology, ISSN 1822-296X. pp. 100-103.

[4] SVENTEKOVA, E., DVORAK, Z.: Theoretical Frame for Testing Critical Transport Infrastructure Elements. *J. of Engineering Management and Competitiveness (JEMC)* [electronic source], ISSN 2217-8147, vol. 3, No. 2, 2013, pp. 37-40. Available at: http://www.tfzr.uns.ac.rs/jemc/files/Vol3No2/V3N22013-01.pdf

[5] VIDRIKOVA, D., DVORAK, Z., KAPLAN, V.: *The Current State of Protection of Critical Infrastructure Elements of Road Transport in Conditions of the Slovak Republic*, Kaunas University of Technology, 2011.

[6] LEITNER, B., DVORAK, Z., SVENTEKOVA, E.: *Traffic Flow Modelling at Restrictive Conditions on Road Infrastructure (in Slovak)*. ITS 2013 [electronic source] = Intelligent transportation systems 2013: virtual conference: August 26-30, 2013. University of Zilina, 2013, ISBN 978-80-554-0763-0, pp. 104-111.

[7] GOGOLA, M.: *Transport Planning in OmniTRANS - Guide for Exercises (in Slovak),* PEDAS: University of Zilina, 2008, CD version.

[8] *OmniTRANS* [online] [cit. 2014-06-02]. Available at: http://www.pbaprague.cz/ download/omnitrans-cz.pdf.

[9] *Simulation Studies [on line]. Modelling in Transport: The process of Simulation Study (in Czech).* Available at: http://kds.vsb.cz/mkk/modelovani-10.htm.

[10] STN 63 6110 - *Designing Local Roads (in Slovak).*

[11] NOVAK, R.: *Analysis and Use of Software Tools to Traffic Conditions Simulation in Specific Crisis Situations (in Slovak),* Diploma work, University of Zilina : FSI, 2012, 79 p.

[12] *Transport Modelling, Chapter IV. Traffic Modelling on Roads (in Czech)*, [cit. 2014-01-10] Available at: http://projekt150.ha-vel.cz/node/94. *http://www.ioda.cz/*.

[13] RIHA, Z., SOUSEK, R., NEMEC, V.: *Transportation and Environment - Economic Research*, The 18th World Multi-conference on Systemics, Cybernetics and Informatics, Orlando : Florida, July 2014, ISBN 978-1-941763-05-6.

Jozef Klucka - Vladimir Mozer - Jan Dvorsky *

FIRE LOSSES IN THE SLOVAK REPUBLIC – THEIR CLASSIFICATION AND QUANTIFICATION

The paper deals with approaches to fire loss classification and quantification. Direct and indirect loss, total loss per fire and the relation of direct and indirect loss to the gross domestic product (GDP) are calculated. Furthermore, the Statgraphics Centurion XV package is used to express: total loss prediction for selected probabilities and probabilities for selected total fire loss values. The results are discussed and conclusions drawn in form of recommendations for the Fire & Rescue Services management in the Slovak Republic.

Keywords: *Fire, losses, modelling, probability, distribution.*

1. Introduction

This paper deals with the topic of fire loss classification and quantification. An analysis was carried out, using the available data which represent direct fire losses in the Slovak Republic. Direct loss was also supplemented by a quantitative expression of indirect loss. The aim of the paper is, based on statistical analysis, to offer managerial information on the probability of total loss in €, as well as the associated probabilities of loss occurrence. The outcomes of the analysis are then transformed into a set of recommendations for the Fire & Rescue Service management.

Loss may be analysed from the following points of view:

- trend,
- occurrence probability,
- interdependencies with other statistical descriptors and benchmark comparison (including international comparison).

The results of these analyses should have a positive impact on the realisation of the management process in the Fire & Rescue Service, as well as on the structure and process of statistical analysis (internal and external communication of processes and results).

2. Analysis

There is a number of approaches to incident loss classification; by an incident we understand, for the purposes of this paper, an event, the consequences of which lead to loss and potential system dysfunction (for more also see [1]).

Losses caused by emergencies are classified also [1] - Fig. 1.

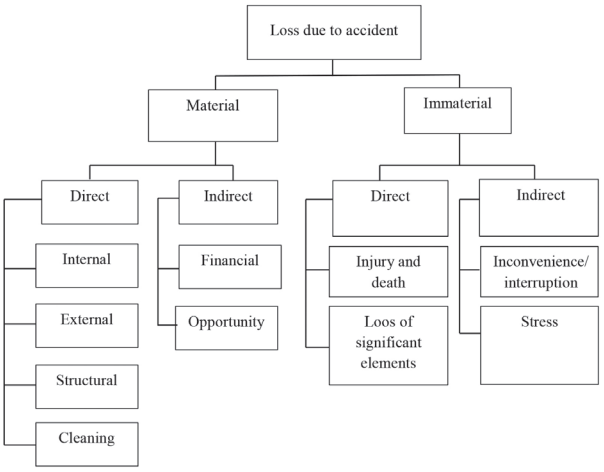


Fig. 1 Emergency-caused losses classification (for more also see [1])

From a fire-safety point of view Ramachandran [2] recognizes five levels in the management hierarchy, each having a different and specific view of topic of costs/losses and benefits. They are as follows: building owners, fire and rescue service, local authorities, government authorities, insurers and fire protection equipment manufacturers. Costs, such as installation of fire protection equipment, insurance premiums are real costs, however, the costs/losses associated with fire consequences are uncertain. Their height is tied to the probability of fire occurrence and the probable fire loss. The reduction of costs resulting from applied preventive measures is considered a benefit in this regard.

* [1]Jozef Klucka, [2]Vladimir Mozer, [1]Jan Dvorsky
[1]Department of Crisis Management, University of Zilina, Slovakia
[2]Department of Rescue Services, University of Zilina, Slovakia
E-mail: Jozef.Klucka@fbi.uniza.sk

Another view of costs results from their categorisation into direct – losses caused on the building and equipment due to a fire, and indirect – e.g. loss of production impacting profit, loss of customers, markets etc.

The direct loss on the building is expressed through an estimation of the expected replacement cost of the property damaged (for more also see [2]).

There is a number of approaches for fire loss quantification and they are organisation-specific. The insurance industry uses the following indicators (for more also see [3]):

Estimated maximum loss (EML): Usually expressed as percentage of value of unit under consideration. The fraction is likely to be charged in a serious conflagration.

Maximum possible loss: Financial loss that would occur under catastrophic or extremely unfavourable conditions (Failure of two or more protective systems – active and passive).

Maximum probable loss: Maximum financial loss under normal conditions, for example one protective system failing.

Normal loss expectancy: Financial loss under average operating conditions – all protective systems functional.

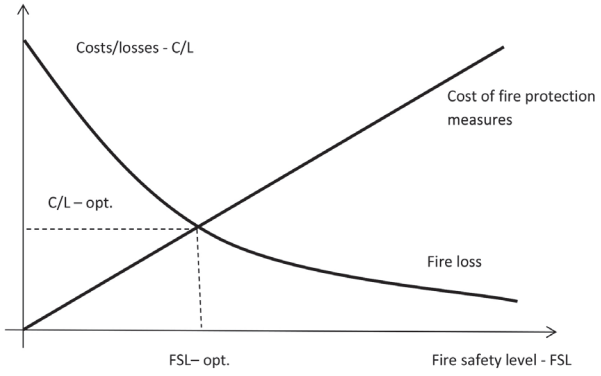


Fig. 2 Expression of optimisation conflict – fire losses vs fire safety level

Figure 2 illustrates the relationship between fire losses and the cost of fire protection measures. It is obvious, that for a given curve of costs and losses the (FLS – optimum C/L) point represent an optimum level – i.e. for the given level of costs, the losses are at their minimum value.

The extent of economic consequences of an accident is determined by the following elements:

- economic consequences are divided into direct and indirect,
- life loss and injuries represent specific forms of loss which are, although difficult, quantifiable
- economic consequences of an accident are driven by system's resilience,
- the ratio of direct and indirect loss is inconsistent among the sources (for more also see [1]), states that the indirect loss represent 25 – 40 % of direct loss,
- there is only a limited theoretic methodology basis and statistical data required for incident consequence quantification.

The current methodology of Slovak Fire & Rescue Service (FRS) recognizes only direct losses. They are recorded in accordance with internal guidelines of FRS (for more also see [4], [5] and [6]).

3. Results

The analysis included the following steps:

- total direct loss calculated from statistic report data was adjusted for inflation; direct loss was also used as the basis for the calculation of indirect loss for the analysed statistical set (see Table 1),
- based on the above total adjusted direct and indirect loss, direct and indirect loss per fire was calculated (see Table 2),

Direct and indirect loss in SR in 2003 – 2012 Table 1

Year	Inflation (%)	Direct losses-DL (€)	Direct losses with inflation (€)	Indirect losses IDL (€)	Total losses TL (€)	TL - (€)	Growth coef. TL
2003	8.5	18734874.0	20327338.3	6726573.0	27053911.3	8319037.3	-
2004	7.5	19539670.0	21005145.3	7006951.3	28012096.6	8472426.6	1.0
2005	2.7	27003084.0	27732167.3	9902582.3	37634749.6	10631665.6	1.3
2006	4.5	27121208.0	28341662.4	10174267.2	38515929.6	11394721.6	1.0
2007	2.8	46921954.0	48235768.7	19725511.6	67961280.3	21039326.3	1.8
2008	4.6	43493564.0	45494267.9	18339592.7	63833860.6	20340296.6	0.9
2009	1.6	38761305.0	39381485.9	15324004.8	54705490.7	15944185.7	0.9
2010	1.0	69148435.0	69839919.4	31271071.3	101110990.7	31962555.7	1.8
2011	3.9	33561130.0	34870014.1	13170022.3	48040036.4	14478906.4	0.5
2012	3.6	41394490.0	42884691.6	17039230.2	59923921.9	18529431.9	1.2

Where:

$TL = DL_{inf} + IDL$ *and* $ID = c \times (DL_{inf})^b$

where $c = 0.015$; $b = 1.245$ (due to missing data, calculation method form [2] was adopted).

- subsequently, the total adjusted direct and indirect loss was recalculated as a percentage ratio of GDP (see Table 3), and the results were compared with selected European countries (see Table 4 and Table 5),
- finally, the adjusted direct and indirect loss was fitted to an appropriate statistical distribution (see Table 7 and Table 8); these values were then analysed for a relationship between probability and total loss value (variably for each given probability of total loss occurrence and the given amount of total loss) (see Table 9 and Table 10).

Having calculated the direct and indirect losses, their values were divided by the number of fires which had occurred in SR during the monitored period. The outcomes are as follows:

- the average value of direct loss per fire adjusted for inflation is 3 200 € and the average indirect loss per fire is 1 263 €,
- the total loss per fire adjusted for inflation in the monitored period in the range of 1781 – 10 264 €; statistically, year 2010 is interesting due to the significant decrease of the number of fires, compared to preceding period, however, fire loss was extremely high; only a more detailed analysis of individual fires would provide explanation,
- by analysing the total loss per fire, it is possible to state that the development of its value has a significant variability; particularly the period of 2008 – 2012 would require further attention.

The further area of analysis was a comparison of direct and indirect loss in relation to GDP in the monitored period. The obtained results were compared with the published ones (see Table 3).

Direct and indirect loss per fire in SR during the period of 2003 – 2012 Table 2

Year	Sum of fires	Direct losses	/fire (€)	Indirect losses IDL (€)	IDL/fire (€)	TL/fire (€)	Growth coef. TL/ fire
2003	15189.0	20327338.3	1338.3	6726573.0	442.9	1781.2	-
2004	10118.0	21005145.3	2076.0	7006951.3	692.5	2768.5	1.6
2005	11294.0	27732167.3	2455.5	9902582.3	876.8	3332.3	1.2
2006	10260.0	28341662.4	2762.3	10174267.2	991.6	3754.0	1.1
2007	14366.0	48235768.7	3357.6	19725511.6	1373.1	4730.7	1.3
2008	11045.0	45494267.9	4119.0	18339592.7	1660.4	5779.4	1.2
2009	11991.0	39381485.9	3284.3	15324004.8	1278.0	4562.2	0.8
2010	9851.0	69839919.4	7089.6	31271071.3	3174.4	10264.0	2.2
2011	13677.0	34870014.1	2549.5	13170022.3	962.9	3512.5	0.3
2012	14413.0	42884691.6	2975.4	17039230.2	1182.2	4157.6	1.2

Relation of direct and indirect loss to GDP in monitored loss Table 3

Year	GDP (mil. €)	Direct losses with inflation- (€)	Indirect losses -IDL (€)	/GDP (%)	IDL/GDP (%)	IDL/
2003	40 612.00	20 327 338.29	6 726 572.98	0.050%	0.017%	0.331
2004	45 161.40	21 005 145.25	7 006 951.32	0.047%	0.016%	0.334
2005	49 314.20	27 732 167.27	9 902 582.34	0.056%	0.020%	0.357
2006	55 001.60	28 341 662.36	10 174 267.2	0.052%	0.018%	0.359
2007	61 449.70	48 235 768.71	19 725 511.6	0.078%	0.032%	0.409
2008	66 932.30	45 494 267.94	18 339 592.6	0.068%	0.027%	0.403
2009	62 895.50	39 381 485.88	15 324 004.8	0.063%	0.024%	0.389
2010	65 887.40	69 839 919.35	31 271 071.3	0.106%	0.047%	0.448
2011	69 058.20	34 870 014.07	13 170 022.3	0.050%	0.019%	0.378
2012	71 463.00	42 884 691.64	17 039 230.2	0.060%	0.024%	0.397

Direct and indirect loss in selected EU countries [2] Table 4

Country	Direct losses* (%)	Indirect losses* (%)
Austria	0.21 (79-80)	0.029
Belgium	0.4 (88-89)	N.A.**
Denmark	0.26	0.034
Finland	0.17(88-89)	0.021
France	0.23	0.037
Germany	0.2	0.037
Hungary	0.12 (86-88)	0.028
Netherlands	0.19	0.03
Norway	0.24	0.005
Spain	0.12 (84)	N.A.
Sweden	0.25	0.009
Switzerland	0.23 (89))	0.095
UK	0.19	0.019

*Average percentage of GDP

Direct and indirect loss in relation to GDP in selected EU countries [2] Table 5

Country	Indirect losses -ID (%GDP)	Direct losses - DL (%GDP)	Ratio IDL/DL
Norway	0.005 (58-60)	0.24	0.021
Sweden	0.009	0.25	0.036
The Netherlands	0.030 (87-88)	0.19 (87-88)	0.158
Austria	0.029 (79-80)	0.21 (79-80)	0.138
Germany	0.037 (87-89)	0.20 (89-90)	0.185
Denmark	0.034	0.26	0.131
Finland	0.021 (88-89)	0.17 (88-89)	0.124
UK	0.019	0.19	0.1
France	0.037 (80-81)	0.23 (81-82)	0.161
Switzerland	0.095 (89)	0.23 (89)	0.413

** N.A. – estimate not available

The following is evident from Table 4 and Table 5 (for more also see [7] and [8]):

- the ratio of direct loss to GDP is significantly lower than in other EU countries,
- the ratio of indirect loss to GDP in selected EU countries is in agreement with values (see Table 4 and Table 5),
- the ratio of indirect to direct loss is significantly higher in SR than in other EU countries; only a more in-depth analysis would provide reasons explaining this fact; it was not possible at the moment of writing this paper due to limited data availability.

The results of the above are determined by the following factors:

- from the available data, we presume that direct loss is not adjusted for inflation,
- the value of direct and indirect loss is determined by limited data; the presumed fact of different indirect loss for various building groups is simplified (see Table 5).

Statistical modelling of total fire loss comprised a number of stages, in which a number of distributions and calculation methods were tested and the most appropriate selected (for more also see [9] and [10]) The calculations were carried out in the STATGRAPHICS CENTURION XV package, due to the computational demands (for more also see [11], [12] and [13]). The basic selective characteristics (see Table 6) indicate that the selected group is characterised by a continuous probabilistic distribution due to a high coefficient of variation – 42.32 %.

Basic statistical characteristics of fire loss for the period of 2003 – 2012 Table 6

Average	5.26792 x
Standard deviation	2.22954 x
Coefficient of variation	42.323%
Kurtosis	1.01213
Skewness	1.37392

The estimated distribution parameters using the maximum likelihood method (see Table 7)

Parameter estimation for selected probabilistic distributions Table 7

Pareto distribution	Gamma distribution	Lognormal distribution	Weibull distribution	Normal distribution
α = 0.05649	α = 6.61954	μ = 53 131 800	δ =2.64796	μ =52 679 200
c = 22 587 800	β = 1.25663 x	= 23 014 300	c = 59 407 600	= 22 295 400

Kolmogorov-Smirnov test results Table 8

	Pareto distribution	Gamma distribution	Normal distribution	Weibull distribution	Lognormal distribution
DPLUS	0.17524	0.13652	0.11514	0.13981	0.14653
DMINUS	0.00163	0.08991	0.10939	0.11716	0.12520
DN	0.10163	0.13652	0.11514	0.13981	0.14653
P-value	0.94138	0.99225	0.99937	0.98970	0.98280

The tests were carried out on the 5 % significance levels. With 95 % level of confidence, the data fit the Lognormal distribution, since the P-value of Kolmogorov-Smirnov test is the highest for this distribution.

Having found that the total fire loss in SR for the period of 2003 – 2012 fits best to the Lognormal distribution, future extreme values for selected probabilities can be predicted.

Total fire loss prediction for selected probabilities Table 9

Probability of Total fire loss (%)	Total fire loss (€)
20	69 116 700
10	82 948 900
5	96 435 700
2	114 255 000
1	127 929 000

Probabilities for selected total fire loss Table 10

Total fire loss (€)	Probability of Total fire loss (%)
30 000 000	12.07
50 000 000	52.43
70 000 000	80.85
90 000 000	93.03
110 000 000	97.51

The results from Table 9 and Table 10 can be interpreted as follows:

- with 10 % probability, the expected loss in SR for the next year is 82 948 900 €,
- the probability that the total loss will not exceed 70 000 000 € is 80.81 %,
- analogically same interpretation applies to other values in Table 9 and Table 10.

Similar logic may be applied to other probabilities of total fire loss.

The analysis of the results yields the following outcomes:

- the average value of total direct loss in the monitored period is 36 568 000 €; the average value of adjusted total direct loss is 37 811 000 €; on average, inflation caused a 4 % increase of direct loss,
- the increase of total loss, when compared to the direct loss for the given year, is approximately 44 %,
- the average difference of the total and adjusted direct loss is 16 mil. € and the median of this item is 14.5 mil. €,
- the standard deviation value of the difference of total and direct loss is 7.2 mil. €, which suggests a significant variability of the analysed items,
- the average value of indirect loss is 14 868 000 €; the median of this item 13170 000 €,
- the growth coefficient of total lost has a significant variance; the periods of growth and decrease alternate, with extremes in 2003 – 2004 (4 % increase) and years 2010 – 2011 (137 % growth).

4. Conclusion

The analysis of fire risk is carried out with the aim of risk reduction in decision making which deals with fire source identification, determination of the probability of a fire starting and consequence quantification. The process of loss analysis is also part of the risk management process. Knowing the probable consequences and their quantification allows to take appropriate measures as part of risk management, which help the organisation (FRS) decrease the risk to an acceptable level. In other words, the realised measures decrease the level of risk from unacceptable to acceptable.

From the presented results it is possible draw the following application conclusions for FRS:

- formulate a methodology for direct fire loss calculation and decide on the way of inflation integration,
- extend the current methodology for indirect fire loss,
- compare direct and indirect loss as part of analyses and quantify loss per fire,
- categorise fires by sectors/industries, and based on these extend the analysis of direct and indirect fire loss for the individual categories,
- carry out a trend analysis for each sector/industry – development of direct an indirect loss in time,
- carry out an international comparison of the direct loss/GDP, indirect loss/GDP, and indirect and direct loss ratios,
- extend loss quantification for life loss and injury factors,
- analyse the methods currently used by the insurance industry for quantification (for more also see [3])

The above proposed measures have an ambition to include the results of statistical analyses into the FRS management more effectively.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under the contract No APVV-0727-12.

References

[1] *Critical Infrastructure Resilience Strategy.* Australian government, Canberra, 2010, (information on: www.ag.gov.au/cca)

[2] RAMACHANDRAN, G.: *Economics of FireP*. Published by E & FN Spon, 1998, ISBN 0-203-78436-7, p. 247.

[3] RASBASH, D. J., RAMACHANDRAN, G., KANDOLA, B., WATTS, J. M., LAW, M.: *Evaluation of Fire Safety*. Wiley, 2004, p. 479, ISBN 0-471-49382-1

[4] *Collection Instructions Presidium Fire and Rescue Service,* No. 25, 2005 Ministry of Interior of the Slovak Republic.

[5] BETAKOVA, J., LORKO, M., DVORSKY J.: *The Impact of the Potential Risks of the Implementation of Instruments for Environmental Area Management on the Development of Urban Settlement*, Environmental impact II, Ancona, 2014, ISBN 978-184564762-9, ISSN 17433541, pp. 91-101.

[6] BUTTON,K.: *Transport Economics*, Edward Elgar, 2010, p. 511

[7] CONTE, A. P. E. (ed.): *Fire Protection Handbook,* vol. I., NFTA, Quincy, 2008, ISBN-13:978-0-87765-758-3, p. 1584.

[8] DVORSKY, J., KLUCKA, J.: *Modelling of the Amount of Economic Losses Causes by Fires in the Region of Zilina*, Fire Protection 2014, Ostrava, ISBN 978-80-7385-148-4, pp. 48-51.

[9] *Keeping the Country Running: Natural Hazards and Infrastructure*, Cabinet Office, London, 2011 (information on: www.cabinetoffice.gov.uk/ukresilience)

[10] KELISEK, A., KLUCKA, J., ONDRUSEK, M., STRELCOVA, S.: Economic Security - A Principal Component of Multilevel Security Concept in Global Economy. *Communications - Scientific Letters of the University of Zilina,* 2011, ISSN 1335-4205, pp. 44-48.

[11] KLUCKA, J., MOZER, V., PANAKOVA, J.: *Development of Fires in Different Categories of Buildings for the Period 1993 - 2012*, The conference of Rescue Services, Proc. of intern. scientific conferences, Zilina, ISBN 978-80-554-0894-1, pp. 91-110.

[12] PANAKOVA, J., KLUCKA, J., MOZER, V.: *Model for Evaluation of Fire Protection Measures Economic Efficiency*. Fire protection 2014, Ostrava, ISBN 978-80-7385-148-4, ISSN 1803-1803 pp. 264-266.

[13] STATGRAPHICS: *Software Statgraphics Centurion XV. 2014*. [online]. [cit. 25 March 2014]. Available: http://www.statgraphics.com/support/download_center.aspx.

Vladimir Mozer - Jiri Pokorny - Petr Kucera - Lubica Vrablova - Peter Wilkinson *

UTILITY OF COMPUTER MODELLING IN DETERMINATION OF SAFE AVAILABLE EVACUATION TIME

The main aim of the paper is to evaluate the primary factors affecting the safe available evacuation time with the utility of computer modelling, namely Consolidated Model of Fire and Smoke Transport (CFAST) computer model by NIST. The traditionally accepted base value of 2.5 minutes, used in many design standards, may not be appropriate due to its very generalised nature. Hence, a multi-criteria analysis is carried out in which four standard fire scenarios (fire growth rates) are modelled in a set of compartments with varying geometry. The simulation results are assessed against a range of critical conditions, including visibility, toxicity and temperature. Obtained safe available evacuation times are then compared to the standardised values used in design. The results show that the standardised times derived from the 2.5-minutes base value are not as conservative as believed; both under- and overprediction have been identified. The outcomes indicate that a review of the standardised available safe evacuation times should be carried out.

Keywords: *Available safe evacuation time (ASET), t^2-fire, CFAST, layer height, toxicity.*

1. Introduction

Many of fire safety design standards prescribe the maximum allowed length and minimum clear width of escape routes. By adhering to these limits, evacuees are assumed not to be exposed to the harmful effects of fire and smoke and to exit the building prior to the onset of untenable conditions. So logically, the maximum length and minimum width must be calculated for a time period during which tenability is maintained. In fire safety engineering the term *Available Safe Evacuation Time (ASET)* is used to define this period, however, there is no direct equivalent in prescriptive fire design codes and various other terms may be used, e.g. *Maximum Allowed Evacuation Time (MAET)* [1]; for the purposes of this paper the term ASET is used, although it does not refer specifically to fire safety engineering design.

In prescriptive or other traditional codes, however, ASET is usually not stated directly as a time value but rather as the above mentioned length and width limits. This ASET value is usually based on the 2.5-minutes clearance time indicated in [2]. In light of the age, premise and significant generalisation of the 2.5-minutes value, forming critical part of fire design standards internationally, there is a need for a review of its validity and applicability.

This paper provides an introduction study of the effect of the most important parameters – compartment geometry and fire dynamics – on the Available Safe Evacuation Time. The selected geometries should demonstrate how the increasing area and height of a compartment and the rate of fire growth affect the onset of tenability limits. Computer modelling, namely CFAST and FDS, is used to calculate the development of the fire and its parameters.

2. Model description

A set of rectangular-geometry compartments of varying area and height was modelled in CFAST, a zone computer model. In each compartment, four differently growing fires were simulated in order to assess the impact of compartment geometry and fire properties on the available safe evacuation time.

* [1]Vladimir Mozer, [2]Jiri Pokorny, [3]Petr Kucera, [1]Lubica Vrablova, [4]Peter Wilkinson
[1]Department of Fire Engineering, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Fire & Rescue Service, Department of prevention and CNP, Ostrava, Czech Republic
[3]Department of Fire Protection, Faculty of Safety Engineering, Technical University of Ostrava, Czech Republic
[4]Civil Safety and Security Unit, University of Leicester, United Kingdom
E-mail: vladimir.mozer@fbi.uniza.sk

2.1 Consolidated Model of Fire and Smoke Transport (CFAST) and Fire Dynamics Simulator (FDS)

CFAST is a two-zone fire model used to calculate the evolving distribution of smoke, fire gases and temperature throughout compartments of a building during a fire. These can range from very small containment vessels on the order of 1 m^3 to large spaces on the order of 1000 m^3 [3].

The modelling equations used in CFAST take the mathematical form of an initial value problem for a system of ordinary differential equations (ODEs). These equations are derived using the conservation of mass, the conservation of energy (equivalently the first law of thermodynamics), the ideal gas law and relations for density and internal energy. These equations predict as functions of time quantities such as pressure, layer height and temperatures given the accumulation of mass and enthalpy in the two layers. The CFAST model then consists of a set of ODEs to compute the environment in each compartment and a collection of algorithms to compute the mass and enthalpy source terms required by the ODEs [4].

FDS version 6.1.1 (July 10, 2014) [5] and [6], a CFD model by NIST was used for validation in which results from CFAST and more advanced FDS were compared.

2.2 Compartment geometry and ventilation

Each simulated compartment comprised an undivided square room with side dimensions selected such that the floor area was 50, 100, 150 and 200 m^2, depending on the case. In addition, a 200 m^2 room divided into four identical 50 m^2 rooms was modelled. This scenario was introduced in order to evaluate the impact of partitions on the ASET, as it allows to observe three sizes of a compartment – 50, 150 and 200 m^2 – and compare them with their respective undivided counterparts. The layout the divided-compartment scenario is shown in Fig. 1.

Two compartment heights were simulated – 2.7 and 4.5 m; the first represents the clear construction height of a standard office storey, and the second is to represent higher spaces, such as auditoria, assembly halls, etc.

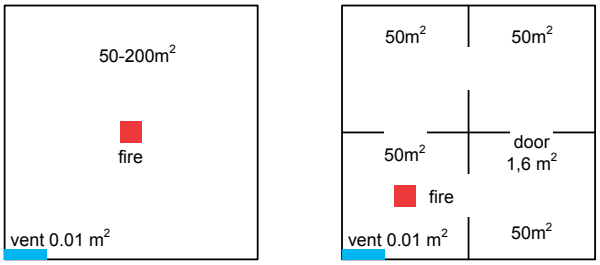


Fig.1 Geometric layout of simulated compartments (undivided left / divided right)

Ventilation was provided only via a slit of 0.01 m^2 cross-section area in each case. This way air leakage in and out of the compartment via gaps around doors and other similar paths was simulated. No open windows and doors to the exterior were included in the simulation. It was assumed that the selected temperature tenability limit (120°C) will not cause damage to the enclosing construction, doors and windows. This assumption was also confirmed in a previous study [7].

In the divided 200 m^2 case, additional ventilation between the individual rooms was through four doors. Each door was 2 m high and 0.8 m wide, resulting in a total open area of 1.6 m^2.Their layout is shown in Fig. 1. The doors remained open for the entire duration of the simulation.

2.3 Fire scenarios and fuel properties

Fires are usually described by the time-temperature relation or heat release rate [8]. The basic assumption employed in this study is that only the growth phase of a fire is considered relevant to evacuation. The tenability limits are far exceeded by the time the fire reaches flashover, therefore, it is not needed to consider the phase of fully developed fire when evaluating the safe available evacuation time in the room of fire origin.

During the growth phase, the fire is fuel-bed controlled (well ventilated) and its heat output grows with time. For this purpose the t^2 – fire model was used in this paper to prescribe the development of the heat release rate (HRR) with time. This model is well established widely used in the fire safety engineering field, see e.g. [9] and [10]. The basic principle of this model is that HRR grows exponentially with time and the intensity of the growth is defined through the fire-growth coefficient α_t. Four standard fire-growth regimes are defined, depending on the time a fire requires to reach a HRR of 1 MW; these are specified in Table 1.

Fire growth regimes for t^2-fire [9] Table 1

Fire growth regime	Time to reach 1 MW [s]	Coefficient α_t [kW.s^{-2}]	Example building use [11]
Slow	600	0.00293	Picture gallery
Medium	300	0.01172	Office
Fast	150	0.0469	Shop
Ultra-fast	75	0.1876	High rack storage

For each of the above described compartment geometries, all four fire-growth regimes were modelled. The fire itself had a fixed floor area of 10 m^2. Although, in a real fire, the burning area would increase with time, this is not possible to model in the current implementation of CFAST. For this reason, the McCaffrey plume model [4] was used, which is independent of the floor area of the fire. It was found to yield greater plume

entrainment rates (in agreement with [12]), therefore erring on the side of safety.

Since the incubation time – the period from ignition to sustained growth – is rather variable, ranging from 0 to 100's of seconds, it was not included in the simulation. The HRR grows from t = 0 s without any delay. Once again, this errs on the side of safety and allows for a wide application of the obtained results.

The fuel was specified as a mixture of wood and polyurethane foam, an approximation of common cellulosic-plastic fuel composition. The ratio was 70% wood and 30% polyurethane. Since CFAST and FDS allow specification of a single fuel, the chemical composition, product yields and other properties were calculated as a weighted mean of the respective fractions. All the original properties were taken from SFPE Handbook [10]. The resulting fuel specification is as follows:

Formula: $C_{4.94}H_{6.5}O_{2.4}N_{0.3}$
Heat of combustion: 20390 kJ.kg^{-1}
Soot yield: 0.05 kg/kg
CO yield: 0.007 kg/kg

2.4 Tenability criteria

When determining the available safe evacuation time, properly selected tenability criteria are of crucial importance. For this study the following quantities were monitored; the associated values represent critical tenability limits:

Critical layer height: 1.9 m [13]
Smoke OD: 0.15 m^{-1} [10]
Ambient temperature: 120°C [10]
Heat radiation: 2.5 kW.m^{-2} [10]
CO concentration: 500 ppm [14]
CO2 concentration: 3 % vol. [14]
O2 concentration: 15 % vol. [15]

The critical layer height (1.9 m) is based on the philosophy presented in CSN 73 0802 [13] which allows this limit for spaces with a smaller clear height. It also represents a height at which a large proportion of the general population will not be affected by the smoke layer.

Tenability was reviewed on the basis of exceeding at least one of the above listed critical values and simultaneous decrease of the smoke layer below 1.9 m. The only exception is the intensity of heat radiation which is monitored at ground level. If 2.5 kW.m^{-2} is exceeded, untenable conditions are reached regardless of the layer height.

3. Results

The following Tables 2 to 5 list the available safe evacuation times determined for the individual geometries and fire growth rates. In addition to the ASET values (seconds), each value is also assigned an acronym indicating which of the tenability criteria was exceeded. The acronyms are as follows:

Critical layer height (H); Smoke OD (OD); Ambient temperature (T); Heat radiation (R);

CO concentration (CO); CO_2 concentration (CO2); O_2 concentration (O2).

If (H) is listed, then one or more criteria were exceeded prior to the smoke layer decrease to 1.9 m. If other acronyms, except (R), are stated, then the smoke layer decreased below 1.9 m and the given criterion – (OD), (T), (CO), (CO2), (O2) – was exceeded afterwards. As mentioned previously, the heat radiation criterion (R) is independent of the smoke height, therefore, it states the time at which the critical intensity was exceeded.

Available safe evacuation times for undivided compartments - 2.7 m height Table 2

Floor area [m^2]	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
50	92 (OD)	55 (OD)	42 (H)	32 (H)
100	109 (H)	84 (H)	65 (H)	49 (H)
150	141 (H)	109 (H)	84 (H)	62 (H)
200	169 (H)	130 (H)	100 (H)	73 (H)

Available safe evacuation times for divided compartments - 2.7 m height Table 3

Room [m^2]	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
Room 1 – fire	91 (OD)	54 (H)	42 (H)	32 (H)
Room 2 – adjoining	186 (OD)	129 (H)	97 (H)	71 (H)
Room 3 – adjoining	186 (OD)	129 (H)	97 (H)	71 (H)
Room 4 – remote	281 (OD)	188 (H)	139 (H)	102 (H)

Available safe evacuation times for undivided compartments - 4.5 m height Table 4

Floor area [m^2]	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
50	133 (OD)	86 (H)	66 (H)	50 (H)
100	172 (H)	131 (H)	101 (H)	75 (H)
150	222 (H)	169 (H)	127 (H)	93 (H)
200	266 (H)	202 (H)	149 (H)	108 (H)

Available safe evacuation times for divided compartments - 4.5 m height Table 5

Room [m²]	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
Room 1 – fire	133 (OD)	86 (H)	66 (H)	50 (H)
Room 2 – adjoining	281 (OD)	180 (OD)	130 (H)	94 (H)
Room 3 – adjoining	281 (OD)	180 (OD)	130 (H)	94 (H)
Room 4 – remote	425 (OD)	282 (OD)	192 (OD)	134 (H)

The following Tables 6 and 7 list the available safe evacuation times determined for the smallest area of compartment (50 m²) and fire growth rates using two types of fire models (CFAST and FDS).

ASET results from CFAST and FDS - 50 m² area, 2.7 m height compartment Table 6

Type of model	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
CFAST	92 (OD)	55 (OD)	42 (H)	32 (H)
FDS	94 (OD)	56 (OD)	32 (H)	23 (H)

ASET results from CFAST and FDS – 50 m² area, 4.5 m height compartment Table 7

Type of model	Available Safe Evacuation Time (s)			
	Slow	Medium	Fast	Ultra-fast
CFAST	133 (OD)	86 (H)	66 (H)	50 (H)
FDS	125 (OD)	86 (OD)	51 (H)	29 (H)

Graphic visualisation of results is possible via SMOKEVIEW. Figure 2 shows a comparison of smoke layer heights and zone interfaces obtained from CFAST and FDS for the 50 m² compartment with 2.7m height and medium fire growth rate. The snapshots are taken at the time when critical conditions were exceeded.

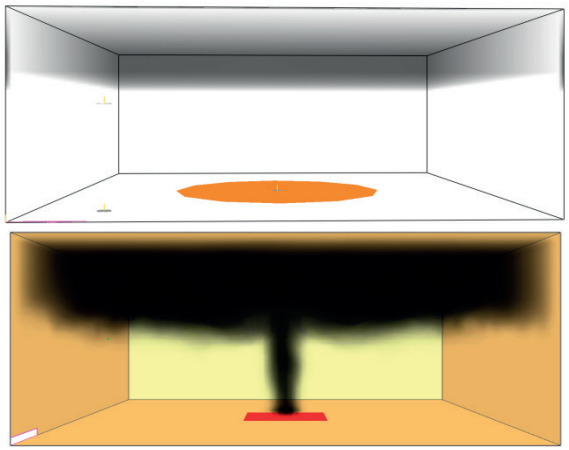


Fig. 2 Visualisation of smoke layer in CFAST (top) and FDS (bottom)

4. Discussion

The simulation results from CFAST are evaluated from two points of view – in general and in relation to the 2.5 min value which is considered as the base safe available evacuation time. Facts which are predictable even without simulation (e.g. shorter time to critical values for smaller compartments, lower ceiling height and greater fire growth rates), are not further discussed in detail.

Based on the simulations carried out, it is possible to make a general statement that, for the given simulation conditions, the layer height and optical density of smoke, were the major limiting criteria; the importance of optical density grew with the fire growth rate. The limiting temperature criterion was usually exceeded after the above criteria (OD and H).

The critical CO, CO_2 and O_2 concentrations were not the limiting factor in any of the cases. This result is closely tied to the specification of fuel chemistry and individual species assessment. The specification of fuel is arbitrary and was explained in Section 2.3. The Fractional Effective Dose (FED) could be used for a more detailed assessment of critical concentrations and toxic potential of the above gases. In general, the onset of the individual dangerous species concentrations was well after the OD, H and T criteria were exceeded.

In relation to the available safe evacuation time, it may be concluded that for the undivided compartments (50 - 200 m²), untenable conditions were attained in 32 s (0.53 min.) - 169 s (2.81 min.) for the 2.7 m compartment height and 50 s (0.83 min.) - 266 s (4.43 min.) for the 4.5 m compartment height. A very significant fact is that, for a given fire growth rate, the ASET does not grow linearly with the floor area of the compartment, but slower; for a four-fold increase in floor area the ASET is approximately doubled.

It is apparent that the critical conditions were achieved prior to the base 2.5 min ASET, mainly in the scenarios with smaller floor area and height and higher fire growth rates. ASETs exceeding 2.5 min were established for larger and taller compartments and slower growing fires. This is a logical and more or less expected outcome which confirms the doubts over the robustness of a "generic" ASET value (2.5 min). It is clear that the ASET is affected not only by the occupancy type (purpose group), determining the fire growth rate, but the compartment geometry – area and height – plays also a significant role. Nonetheless, the geometry factor has very little use in the traditional fire codes, both nationally and internationally.

For the divided compartments of 200 m² floor area, the ASET value intervals were 32 s (0.53 min.) - 281 s (4.68 min.) and 50 s (0.83 min.) - 425 s (7.08 min.), for 2.7 m and 4.5 m compartment heights, respectively. The spatial division of the compartment causes gradual smoke filling and greater ASET values. The fire location and room configuration plays a significant in this type of scenario. Although, a greater ASET is achieved in the most

distant room, when compared to an undivided compartment of the same floor area, if egress is available only via the fire room, the greater ASET is of little value. This confirms the importance of two-way escape and dangers associated with inner-room configurations. Essentially, if an inner-room configuration is present the ASET is the value for the entrance room and not that for the inner room. Inner-inner rooms should be avoided at all; a requirement which is not explicitly stated in the Slovak or Czech fire codes. British Approved document B, for example, prohibits such a room configuration.

The comparison of the results from the CFAST zone model and FDS CFD model for the undivided 50 m^2 revealed that there is a good agreement across all the monitored criteria. It is, therefore, safe to say that the zone model, although simpler and faster, offers a comparable result precision. For simpler compartment geometries, such as the above, this brings the advantage of reduced computational time, which in turn allows for more a detailed parametric analysis – more scenario variations.

5. Conclusion

The fact that the Available Safe Evacuation Time (ASET) is primarily affected by the dynamics of fire and compartment geometry is commonly acknowledged in the fire safety industry. It is, therefore, not in the interest of life safety that fire safety design codes do not incorporate these factors adequately, be it for historical or other reasons.

This study reveals, on a set of simple but representative scenarios, how significant an impact both of these factors have. Although the scenarios cover only a very limited range of areas and heights, 50 - 200 m^2 and 2.7/4.5 m, respectively, the difference in ASET for any given fire growth rate is around 300% and even greater for spatially divided geometries. This variation is not negligible and points out that the historical base ASET value of 2.5 min should be reviewed in light of these findings; as a minimum fire design codes should account for compartment area and height. At the moment, the Czech and Slovak codes adjust the 2.5 min base ASET for only the effect of purpose group, similarly to the British code [16]. It was also found that ASET does not grow linearly with the floor area of compartment but slower.

Spatial division was found to have a positive effect on ASET, however only when each room has two available directions of escape. It was confirmed that inner-room compartment geometries are not desirable from an escape point of view. Where unavoidable, ASET for the access room should be taken as limiting.

From a tenability point of view, it was found that the smoke layer height and optical density of smoke are the primary factors determining ASET. The results reveal that the smoke optical density criterion is usually the first one to have been exceeded, followed by smoke layer decrease to the critical height. Other tenability criteria were exceeded subsequently.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-0727-12.

This work was supported by the project of the Ministry of the Interior of the Czech Republic No. VG 20122014074 – "*Specific Assessment of High Risk Conditions for Fire Safety by Fire Engineering Procedures*".

References

[1] STN 92 0201-1: *Fire Safety of Buildings - Part 3. Escape Routes and Evacuation. B.m.*: SUTN, 2000.

[2] Post War Building Studies, No. 29: *Fire Grading of Buildings - Parts II., III. and IV.,* Her Majesty's Stationery Office, London, 1952.

[3] PEACOCK, R. D., RENEKE, P. A., FORNEY, G. P.: *CFAST - Consolidated Model of Fire Growth and Smoke Transport (Version 6) User's Guide*. NIST SP 1041r1. B.m.: National Institute of Standards and Technology, 2013.

[4] PEACOCK, R. D., RENEKE P. A., FORNEY G. P.: *CFAST – Consolidated Model of Fire Growth and Smoke Transport (Version 6) Technical Reference Guide*. NIST SP 1026r1. B.m.: National Institute of Standards and Technology, 2013.[5] McGRATTAN, K. et al: *Fire Dynamics Simulator Technical Reference Guide Vol. 1: Mathematical Model.* NIST SP 1018, Sixth Edition. B.m.: National Institute of Standards and Technology, 2014.

[6] McGRATTAN, K. et al: *Fire Dynamics Simulator User's Guide.* NIST SP 1019, Sixth Edition. B.m.: National Institute of Standards and Technology, 2014.[7] MOZER, V.: An Analysis of Factors Affecting Available Safe Escape Time. *Advanced Materials Research,* vol. 1001, 2014, pp. 267-271, ISSN 1662-8985.

[8] BLAGOJEVICH, M. D.: Time-temperature Curve Definition According to Fuel Type. *Communications - Scientific Letters of the University of Zilina,* No. 3, 2006, pp. 48-51, ISSN 1335-4205, 2006.

[9] MAYFIELD, C., HOPKIN, D.: *Design Fires for Use in Fire Safety Engineering*. Bracknell : IHS BRE Press : BRE Trust, ISBN 9781848061521, 2011.

[10] DINENNO, P. J.: *SFPE Handbook of Fire Protection Engineering,* 4th ed. Quincy, Mass. : Bethesda, Md: National Fire Protection Association : Society of Fire Protection Engineers, 2008, ISBN 9780877658214.
[11] PD 7974-1: *Part 1 Initiation and Development of Fire within the Enclosure of Origin*. London: BSI, 2003.
[12] KARLSSON, B., QUINTIERE, J.: *Enclosure Fire Dynamics,* Boca Raton : Taylor & Francis : Environmental & Energy Engineering, 2002, ISBN 9781420050219.
[13] CSN 73 0802: *Fire Safety of Buildings - Non-industrial Buildings*, Praha : Urad pro technickou normalizaci, metrologii a statni zkusebnictvi, 2009, 122 p.
[14] HOSSER, D. L.: *Ingenieurmethoden des Brandschutzes. Braunschweig: Vereinigung zur Forderung des Deutschen Brandschutzes* e.V., GFPA German Fire Protection Association, 2009, 386 p.
[15] Krajska hygienicka stanice se sidlem v Praze: *Reduced Oxygen Levels in Workplace and their Effect on Employees' Health (in Czech),* available online at: http://www.khsstc.cz/ Soubor.ashx?souborID=1104&typ=application/pdf&nazev=Sn%C3%AD%C5%BEen%C3%BD%20obsah%20kysl%C3%ADku%20v%20pracovn%C3%ADm%20prost%C5%99ed%C3%AD.pdf , accessed on 05/09/2014.
[16] CLG. *Approved Document B, vol. 1&2, 2006,* Communities and Local Government.

Roman Jasek *

SHA-1 AND MD5 CRYPTOGRAPHIC HASH FUNCTIONS: SECURITY OVERVIEW

Despite their obsolescence and recommendations they are phased out from production environment, MD5 and SHA-1 cryptographic hash functions remain defaults frequently offered in many applications, e.g., database managers. In the article, we present a security overview of both algorithms and demonstrate the necessity to abandon them in favor of more resilient alternatives due to low computational requirements necessary to reverse engineer the message digests, or to future proof security due to advances in hardware performance and scalability. Suitability procedures and their methods of use are part of this article.

Keywords: *Algorithm, bcypt, function, hashing, MD5, PBKDF2, security, SHA-1, scrypt.*

1. Introduction

Sensitive data protection has been in focus of security researchers for a long time. While extensive academic coverage analyzing existing and proposed cryptographic hash algorithms exists, organizations are slow to adopt them due to inertia, backward compatibility issues, increased hardware requirements, and deployment costs. When benefits of these changes are not clearly communicated, keeping cryptographic systems up-to-date is deprioritized due to lacking technical background.

Website frontends are frequently vulnerable to one or more techniques such as SQL injection, null byte injection, buffer overflow, directory traversal, and uncontrolled format strings. Relying solely on network perimeter security elements should not constitute basis for leaving critical portions of data storages unencrypted. However, some data encryption schemes do not guarantee adequate level of security. To detect changes in databases consisting millions of records, various mathematical fingerprinting techniques were devised titled cryptographic hash functions which provide computationally efficient way to generate, store, and manipulate (compare, move, delete) the control strings with marginal time requirements. They are also used for storing sensitive user data in scrambled form, thereby reducing the attack surface.

Definition of sensitive data varies. Legal incentives, namely Payment Card Industry Data Security Standard codify proper handling and storage of financial data [1]. European Union's Data Protection Directive 95/46/EC was enacted in 1995 [2] and in 2012, a major reform titled General Data Protection Regulation has commenced which plans to streamline protection and sharing of personally identifiable data of all member states' citizens. Unless noted, sensitive data will refer to any confidential electronic assets users willingly disclosed which may compromise their electronic identities or integrity if obtained by unauthorized third party. To preclude such situations, data may be converted to a fixed-size output using a hash function.

Advanced chip designs with high integration of transistors (whose power is growing according to Moore's law [3]) represent high computing power for malicious code from third parties. This risk will also increase over time.

For this reason, revisions must be made as to what cryptographic hash algorithms are sufficient and suitable to protect sensitive with respect to brute-force and dictionary attacks, allowing attackers to enumerate billions of combinations per unit of time, rendering the hash scheme inefficient if deployed incorrectly.

The article provides security overview of two popular but obsoleted hashing algorithms still used in production environment: MD5 and SHA-1. While they have been proven computationally insecure or incapable to future proof applications as per Moore's law mentioned above, they are nevertheless widely deployed as alternatives to comparably more secure schemes for backward compatibility or legacy reasons. It is structured as follows: Section 2 provides security overview of MD5 and SHA-1 cryptographic functions, outlining their design and describing timeline of significant attacks. Section 3 lists best practices applicable to hashing sensitive data, including cryptographic salts to thwart exhaustive searches and dictionary attacks, key strengthening

* **Roman Jasek**
Department of Applied Informatics, Tomas Bata University of Zlin, Czech Republic
E-mail: jasek@fai.utb.cz

which imposes computational penalty when reverse engineering hashes. Section 4 continues by describing key strengthening and mentions suitable alternatives to MD5 and SHA-1 designed specifically with key stretching and strengthening in mind, and brief concluding remarks.

Security in various forms, i.e., message authentication [4] and protecting data in transit [5] is imperative for data confidentiality, integrity, and availability. We believe the article will contribute to safer organizational environments by incentivizing system administrators and appropriate parties to migrate from insecure or weakened cryptographic hash functions to alternatives scrutinized by academia and security community.

2. Cryptographic hash functions

A cryptographic hash function, commonly abbreviated as a hash is a "...function, mathematical or otherwise, that takes a variable-length input string (called a pre-image) and converts it to a fixed-length (generally smaller) output string (called a hash value)" [6]. Hash is alternatively titled checksum, although checksums validate homogeneity and consistency of a data block while hashes serve multitude of functions apart from integrity checks, e.g., authentication, watermarking, digital signature schemes, or MACs (Message Authentication Codes) mentioned in Section 4.

Important properties of a hash are fixed bit length, irreversibility, and fast calculation. Once the input is processed into a digest, no operation is theoretically capable to produce the pre-image. However, as the hash is of fixed size, a brute-force attack can be mounted where all candidate pre-images are converted and compared to the original fingerprint. If a match is made, the hash constitutes either the original pre-image, or a different one which hashes to the same value, i.e., a collision. The attack is extremely time- and resource-intensive and was considered impractical when first cryptographic hash functions were devised.

Another feature is that a bit change in the pre-image results in at least 50% change in the hash, a phenomenon known as (strict) avalanche effect [7]. Avalanche effect ensures the data has not been tampered by a simple fingerprint check. Hashing is a lossy process and input source information content is not preserved. The functions are thus unusable as a storage solution but only to ensure pre-image validity through comparison. It is demonstrated in Fig. 1.

Hashes have become a widely-utilized means of validating any type of data with the only requirement being binary input form. Software libraries are usually provided by database vendors out of the box with the option of purchasing additional packages. As most corporations nowadays limit expenditures into information technology, it is not reasonable to assume database management systems (DBMSs) as well as other applications will be enhanced in such a way. Therefore, encryption modules included by default in many instances of DBMSs will be considered: MD5 and SHA-1.

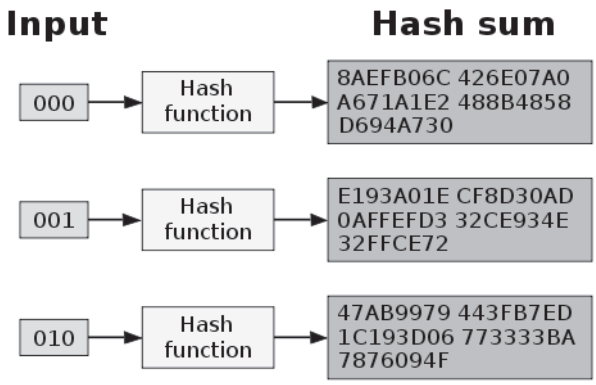


Fig. 1 Avalanche effect for SHA-1 [8]

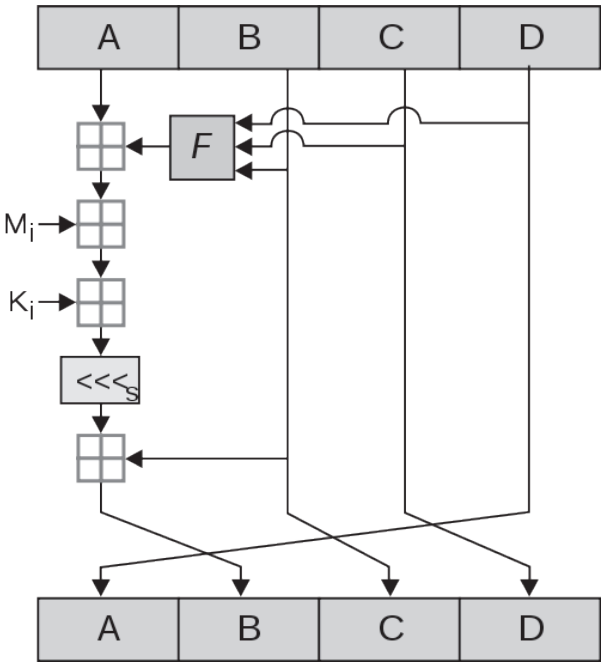


Fig. 2 An MD5 encryption round Source: [9]

A. MD5

The MD5 Message-Digest Algorithm is a 128-bit, 4-rounds function proposed by Ronald Rivest [10]. Successor to MD2 and MD4, it was designed as an industry standard and sanctioned by the Internet Engineering Task Force (IETF) to be a part of the Internet protocol suite. MD5 is represented by a 32-byte hexadecimal string.

As every encryption scheme seeing widespread adoption, MD5 was heavily scrutinized by both security researchers and academia. From the properties listed in Section 1, it was

known the function is vulnerable to hash collisions where the attacker searches for a pre-image that hashes to the same product. If found, it can be exploited to impersonate legitimate users and invalidate the authentication procedure. Initially, it was shown a colliding hash can be found in 15 minutes on a supercomputer setup [11] which led to recommendations that MD5 be not used when generating digital certificates. In practice, adversary can parallelize the computations on consumer-grade hardware to gain performance comparable to low-tier supercomputer.

MD5 encryption round is schematically depicted in Fig. 2. Consisting of 64 iterations grouped by 16, M_i denotes 32b data block obtained by dividing the input message into 512b chunks, padding if necessary. K_i represents a constant added in each round, specified in the original standard [10]. $<<<_s$ denotes bitwise left shift for s positions, with s differing in each round, F a non-linear function, the primary source of complexity when reverse engineering the digest. The function is inputted to adder modulo 2^{32}. The process is repeated with different constant supplied in each round.

MD5 utilizes Merkle-Damgard construction [12] and [13] which postulates that if the compression function is collision resistant, the hash function utilizing it will be also collision resistant. Depicted in Fig. 3, the "... message m is divided into equal size message blocks $x_1 \,||\, ... \,||\, x_n$, the one-way compression function is denoted as H_k and x_0 denotes the initial value with the same size as message blocks $x_1 ... x_n$ (x_0 is implementation or algorithm specific and is represented by an initialization vector). The algorithm then starts by taking x_0 and x_1 as input to the compression function H_k and outputs an intermediate value of the same size of x_0 and x_1. Then for each message block xi, the compression function H_k takes the result so far, combines it with the message block, and produces an intermediate result. The last message block x_n contains bits representing the length of the entire message m, optionally padded to a fixed length output" [14].

In 2004, first practical attack on MD5, its predecessor MD4 as well as several other hash functions was successfully executed [15]. Further improvements were made based on these findings. In 2005, a pair of digital certificates compliant with the X.509 Public Key Infrastructure (PKI) standard was produced, proving the attack was feasible in real-world applications [16]. The collision mechanism is depicted in Fig. 4.

Fig 3. Overview of Merkle-Damgård construction [14]

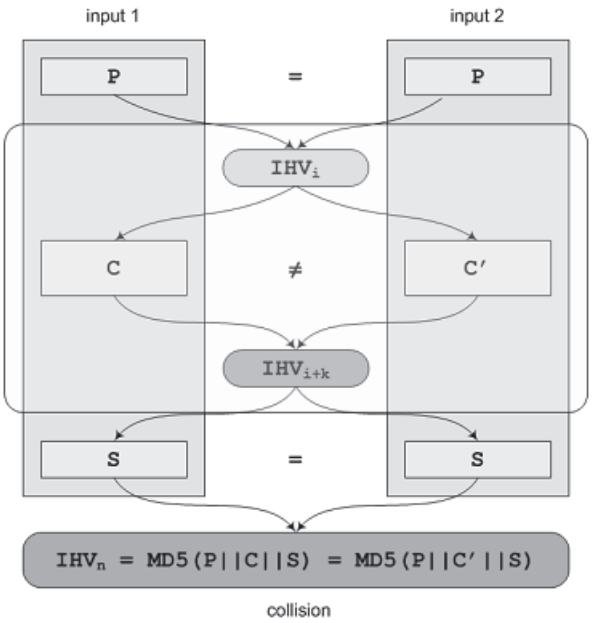


Fig. 4 MD5 collision demonstration [17]

Authors stated that "[d]ue to the iterative structure of MD5 and to the fact that IHV_0 [intermediate hash value] can have any 128 bit value, such collisions can be combined into larger inputs. Namely, for any given prefix P and any given suffix S a pair of "collision blocks" *[C,C']* can be computed such that *MD5(P||C||S) = MD5(P||C'||S).* We use the term 'collision block' for a specially crafted bit string that is inserted into another bit string to achieve a collision. One collision block may consist of several input blocks, even including partial input blocks" [17]. Therefore, for two non-equal inputs, a collision block can be calculated which when inserted into the hashing sequence, produce two identical outputs. The only prerequisite is for the intermediate hash value to be identical for both pairs. A chosen-prefix attack extends it to arbitrary IHVs.

Two modifications of the flaw were demonstrated, allowing identical signatures to be produced on a single machine with the former capable of performing the operation in several hours using consumer-grade notebook, the latter achieving the same goal within 60 seconds on the same hardware; it was stated that "[w]e did not use any supercomputer to find the collisions, just ordinary desktop computers. The author conducted his experiments on his notebook where he found tens of thousands of collisions for the first block and subsequently complete MD5 collisions for both original IV [initialization vector] and chosen IVs" [18]. This proved MD5 can be trivially reverse engineered, significantly reducing security and making it unsuitable for protecting sensitive data.

A research was also conducted which tested propensity to collision attacks in the PKI model. The resulting certificate corroborated that "[it] allows us to impersonate any website on

the Internet, including banking and e-commerce sites secured using the HTTPS [Hypertext Transfer Protocol Secure]" [17].

In 2008, the United States Computer Emergency Readiness Team (US-CERT) announced that "[s]oftware developers, Certification Authorities, website owners, and users should avoid using the MD5 algorithm in any capacity. As previous research has demonstrated, it should be considered cryptographically broken and unsuitable for further use" [19]. In 2012, a new attack purportedly demonstrated MD5's susceptibility to single-block collisions, enabling the attacker to forge 64-byte messages with arbitrary hash value, was announced [20]. Cryptographic community recommended migration to SHA-1.

B. SHA-1

The Secure Hash Algorithm 1 was designed by the United States National Security Agency (NSA) in 1995 as a successor to the 1993's SHA-0. With a 160-bit digest iterated for 80 rounds, it was used for protecting sensitive unclassified information as well as in Internet protocols such as Secure Sockets Layer (SSL) and Secure Shell (SSH) [21]. SHA-1 is represented as a 40-character sequence.

SHA-1 encryption round is depicted in Fig. 5. *A-E* are 32b words identical to MD5, *F* a non-linear function, <<< bitwise shift for arbitrary number of positions, K_t a round constant, and W_t an input data block. The output of *F* enters an adder modulo 2^{32}. The function is based on Merkle–Damgard construction.

Touted an MD5's replacement, SHA-1 saw enormous rise in applications which led to its thorough examination by the cryptographic community. Previously, research focused on its predecessor, SHA-0 for which a collision was found using disturbance vectors with "complexity [of] 2^{39} hash operations. Compared with existing attacks on SHA-0, our method is much more efficient and real collisions can be found quickly on a typical PC. The techniques... are also applicable to SHA-1. As SHA-0 may be viewed as a simple variant of SHA-1, the analysis... serves to verify effectiveness of these new techniques for other SHA variants" [22].

The result showed it is possible to find a collision in SHA-1 while requiring fewer computations than it would take to brute-force the hash, the most time- and resource-intensive cryptanalytic process.

Further attempts were made to reduce the number of operations after which the collision is found. A significant breakthrough was made in 2006 when "...for the first time an actual collision for 64-step SHA-1 is produced, with an expected work factor of 2^{35} compression function computations" [24]. Since then, several attempts have been made to extend the attack on full SHA-1 with mixed results. The latest discovery is dated to 2013 when a researcher estimated theoretical number of computations for full SHA-1 to 2^{61} operations [25].

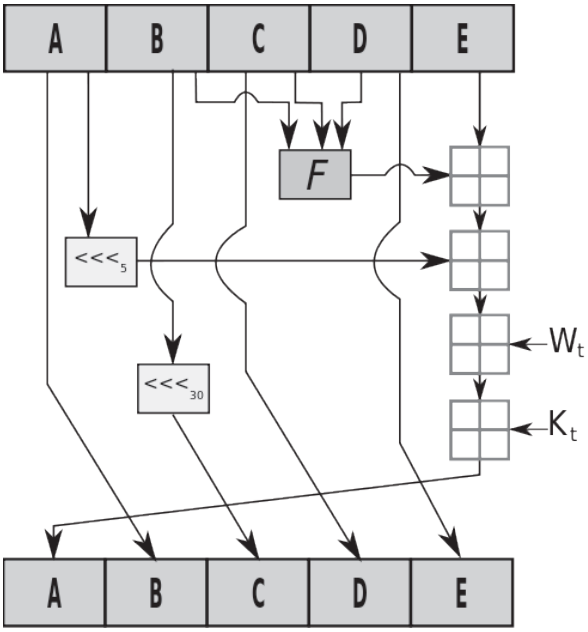


Fig. 5 An SHA-1 encryption round [23]

Because computational complexity of attacks on SHA-1 has been steadily decreasing, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) class was devised as a direct successor. However, both systems are based on identical algorithmic operations and it is expected optimized SHA-1 attacks will be applicable to SHA-2, as well.

In 2012, a successor to SHA-1 and SHA-2 was selected by the NIST (National Institute of Standards and Technology) after an open competition, aiming to choose a function dissimilar to its predecessors. Currently published reverse engineering attempts break 46 out of 64 rounds for SHA-256 [26] and equivalent amount of rounds for the 80-round SHA-512, it is expected the full system will be targeted eventually despite it being computationally infeasible at present time. SHA-3 utilizes functions with sponge construction [27], making harder for the attacker to differentiate it from a random oracle, a theoretical scenario in which any input is encrypted randomly in a black-box setting. Any outside agent cannot discern whether the output was produced based on a random function or a genuine encryption algorithm if no other information (timing measurements, heat emissions, cycle counts) is known. Independent on SHA-2, known attack vectors are not applicable to SHA-3.

Two theoretical vectors against SHA-3 were proposed: a zero-sum attack applicable to the 9-round reduced version with no effect on its security [28]; and an improved zero-sum distinguisher which applies to all 24 rounds and lowers the number of operations from 2^{1579} to 2^{1570} [29]. Both were published before the final version of SHA-3 was selected; no practical cryptanalytic breakthroughs on the final implementation has been published as of yet.

In 2011, National Institute of Standards and Technology asserted that "...the known research results indicate that SHA-1 is not as collision resistant as expected. The collision security strength is significantly less than an ideal has function (i.e., [2^{69}] compared to [2^{80}])... [C]ollision resistance has been shown to affect some (but not all) applications that use digital signatures" [30].

3. Best practices

Regardless of the hash function, the security best practice for storing sensitive data such as user credentials (logins, passwords) is to utilize randomized hashing. As the hash itself is deterministic (two identical strings produce identical outputs), additional probabilistically-generated data need to be supplanted and processed along with the input data stream. Titled cryptographic salt, its purpose is to increase time factor involved when adversary employs rainbow tables, a list of pre-computed values which speeds the process of iterating through the whole search space. Adding salt is depicted in Fig. 6.

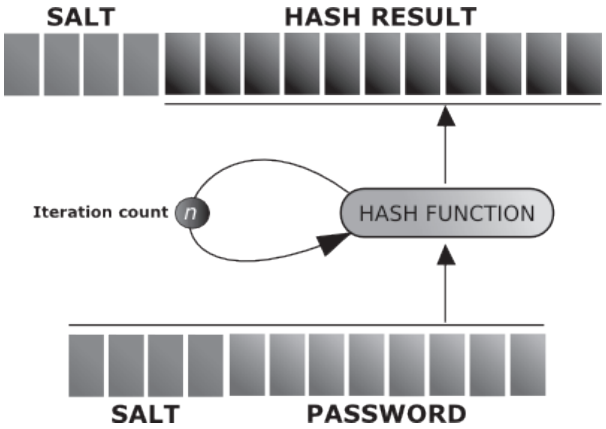


Fig. 6 Adding cryptographic salt to a password before hashing as well as concatenating another salt with the message digest [31]

NIST recommends "[t]he random value... [to] be a message-independent bit string of at least 80 bits, but no more than 1024 bits... [which] shall have sufficient randomness to meet the desired security strength..." [32]. Cryptographic salt should, therefore, be generated using a random number generator whose output meets randomness criteria, e.g., Linear Complexity, Approximate Entropy, Binary Matrix Rank, and Serial Tests [33]. A single value should not be used globally, instead a per-user or per-application salt stored in a database separate from the hashes is recommended. It is introduced to force threat agent to generate large sets of candidate hashes for to the string being reverse engineered. "[T]he number of possible resulting [hashes] is approximately 2^{sLen} where *sLen* is the length of the salt in bits. Therefore, using a salt makes it difficult for the attacker to generate a table of resulting [hashes] for even a small subset of the most-likely passwords" [34].

Even when generating (pseudo)random salts, they may be rendered ineffective if the attacker can exploit vulnerabilities in the way they are concatenated and added to the strings. Two frequent omissions are salt reuse and short salts. The former is "ineffective because if two users have the same password, they'll still have the same hash. An attacker can still use a reverse lookup table attack to run a dictionary attack on every hash at the same time. They just have to apply the salt to each password guess before they hash it," the latter does not prevent the attacker to "build a lookup table for every possible salt.... To make it impossible for an attacker to create a lookup table for every possible salt, the salt must be long. A good rule of thumb is to use a salt that is the same size as the output of the hash function" [35]. A one-time (pseudo) random data string is titled nonce; encryption schemes have been proposed which makes it impossible to decrypt (reverse engineer) the product without the nonce [36].

A break-through occurs when an attack vector enabling pre-image extraction after lower number of operations (and thus time factor involved) is discovered than during exhaustive search. It is defined as "[a]n attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list" [37].

Cryptographic salts also make time-memory tradeoff difficult to implement. First described in 1980 [38], the technique trades time dedicated to calculating candidate solutions for a pre-computed lookup data array where a simple search algorithm can be applied to find the correct value. A threshold exists, though, above which table lookups become costly and ineffective. After several improvements, a new version was introduced in 2003 making use of non-merging rainbow chains, addressing the issue in the original proposal [39]. The technique achieved 99.9% success rate when reverse engineering Microsoft Windows LM hashes with a lookup table the size of 1.4GB. As the prices of storage media decreases per Moore's law, rainbow tables in tens of terabytes will proliferate which utilize high-speed storage media such as SSD (Solid-State Drive).

If the input to the hash function concatenated with a salt prior to being reduced to a fixed-size output, the attacker is forced to pre-compute the lookup array for every possible salt value. Therefore, security depends on uniqueness and length of the random value being appended or prepended to the (presumably) non-random input string. Salts, key strengthening and key stretching make time-memory tradeoff difficult to balance compared to a brute-force attack. Key stretching is discussed in Section 4. Key strengthening was devised in 1994 and splits the salt in two parts: public and secret [40]. While the public part is stored, the secret is securely deleted after first use and becomes unknown. When the user enters a password, the server must perform a brute-force attack using the public part of the

salt to determine the secret portion, increasing both per-user computational requirements and security. The attacker, though, must exhaustively search the whole hash space, i.e., both parts of the salt. The salt or its part and the algorithm used to generate the output must be known server-side to allow comparison of the data to the stored value. No plaintext-formatted data should be stored at any point, only the fingerprints.

Compared to alternatives discussed below, implementing cryptographic hashes does not guarantee the adversary will not be able to extract the pre-image. Should system administrators be forced to select one of the countermeasures, i.e., transitioning to a new cryptographic hash function or adding salt to the existing infrastructure, the former should be strongly preferred as it results in significantly higher computational demands during reverse engineering. Moore's law dictates effectiveness of salting will decrease as hardware performance increase. By deploying strong cryptographic hash function, the work factor can be easily tweaked by means of parameters used during hashing, e.g., iteration count and parallelizability.

4. Alternatives and Discussion

In the paper, a security overview of SHA-1 and MD5 systems was presented. While MD5 phase out has been somewhat slow, by the time the shift to SHA-1 is completed, it may be necessary to discard the system in favor of a more secure one.

To ensure long-term resilience of the stored hashes to offline brute-force attacks, security community also recommends computationally-intensive hashing algorithms such as SHA-512 which generate more secure outputs; processing overhead is, however, increased. Every entity dealing with sensitive data must decide whether this benefit outweighs the disadvantage of higher computational demands, usually abundant in pervasive cloud infrastructure on a pay-per-use basis.

An alternative proposed in 1996 is titled Hash-based Message Authentication Code (HMAC). It guarantees increased security for MAC by combining hashing scheme with a cryptographic key [41]. Output strength is dependent on the hash function (SHA-1, MD5) and its bit size along with parameters of the key. Theoretical attacks exist which don't, however, in any way subvert HMAC security. Ways have been devised on how to compute HMAC efficiently in hardware to ensure minimum latency [42].

Several functions have been released which aim to make cryptographic hashing resource-demanding by introducing arbitrary computational overhead respected during reverse engineering. Implementation libraries utilizing key stretching are freely available: bcrypt, scrypt, PBKDF2, etc. Key stretching purposefully slows the process as much as possible by using longer salts, higher number of iterations (each round is repeated an arbitrary number of *times*), and limiting parallelizability through data arrays stored in memory. As demonstrated in Fig. 7, PBKDF2 utilizes HMAC.

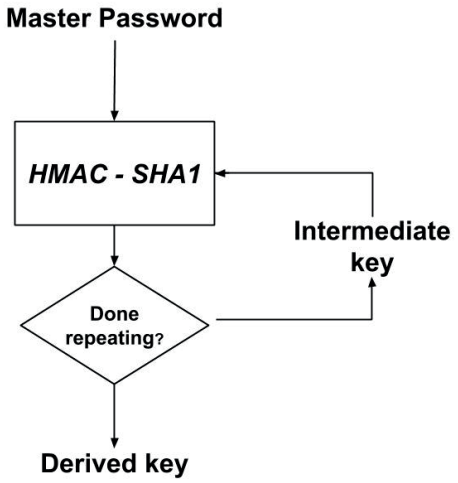


Fig. 7 Password-Based Key Derivation Function 2 [43]

Scrypt in particular hinders reverse engineering with rainbow tables as well as ASIC (Application-Specific Integrated Circuit), FPGA (Field-Programmable Gate Array) and GPU (Graphics Processing Unit), all dedicated hardware modules exhibiting high computational throughput for repetitive mathematical operations. Generating a large vector of pseudorandom bit strings in memory, it accesses the structure in a pseudorandom fashion [44]. Each element in the vector is resource-intensive to generate and can be accessed on many occasions during the algorithm's run, precluding workload distribution to a cluster of nodes. It is a memory-hard algorithm which "...asymptotically uses almost as many memory locations as it uses operations... [I]t can be also thought of as an algorithm which comes close to using the most memory possible for a given number of operations, since by treating memory addresses as keys to a hash table it is trivial to limit a Random Access Machine to an address space proportional to its running time" [44]. By tweaking three parameters, CPU/memory cost, parallelization, and block size, computational demands imposed on computing the hash can be increased arbitrarily.

Website administrators should be informed about advances in hash function cryptanalysis to ensure timely transitions to a well-developed and proven scheme with adequate security for data-storing infrastructures. Increasing the time factor involved via per-user salt, high iteration counts, and thorough testing should be considered priorities.

MD5 has been proven insecure against several attacks under realistic assumptions and its use is discouraged in favor of more resilient, key-stretching iterative hashing algorithms. Despite no full SHA-1 hash collisions have been produced so far, advances as

per Moore's law and future proofing should be taken into account when selecting suitable cryptographic hash function to deploy.

Hash functions have seen increased use in areas such as concurrent algorithm design [45] and continue to be active research field.

Acknowledgement

The work was performed with financial support of research project NPU I No. MSMT-7778/2014 by the Ministry of Education of the Czech Republic and also by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

References

[1] PCI Security Standards Council. *Payment Card Industry Data Security Standard 2.0* [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php, 2010.

[2] EU: *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data* [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri= CELEX:31995L0046:en:HTML, 1995.

[3] MOORE, G. E.: Cramming More Components onto Integrated Circuits, *Electronics*, vol. 38, No. 8, pp. 4-8, April 1965.

[4] LEE, T.-Y., LEE, H.-M.: Encryption and Decryption Algorithm of Data Transmission in Network Security, *WSEAS Trans. Inf. Sc. Appl.*, vol. 3, No. 12, pp. 2557-2562, 2006.

[5] QAWASMEH, E., MASADEH, E.: Developing and Investigation of a New Technique Combining Message Authentication and Encryption, *WSEAS Trans. Inf. Sc. Appl.*, vol. 3, no. 7, pp. 1417-1422, 2006.

[6] SCHNEIER, B.: *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. New Jersey : Wiley, 1996.

[7] FEISTEL, H.: Cryptography and Computer Privacy, *Sci. Am.*, vol. 228, no. 5, pp. 15-23, May 1973.

[8] GOTHBERG, D.: *Avalanche effect.svg*, 2006 [Online]. Available: https://commons.wikimedia.org/ wiki/File:Avalanche_effect.svg

[9] SUNACHIT: *MD5.svg*, 2005 [Online] Available: https://commons.wikimedia.org/wiki/File: MD5.svg

[10] RIVEST, R.: *The MD5 Message Digest Algorithm*, 1992 [Online]. Available: http://tools.ietf.org/ html/rfc1321

[11] WANG, X., YU, H.: How to Break MD5 and Other Hash Functions, *Lect. Notes Comput. Sc.*, No. 3494, pp. 561-577, 2005.

[12] DAMGARD, I. B.: A Design Principle for Hash Functions, *Lect. Notes Comput. Sc.*, No. 435, pp. 416-427, 1990, doi: 10.1007/0-387-34805-0_39

[13] MERKLE, R. C.: A Certified Digital Signature, *Lect. Notes Comput. Sc.*, No. 435, pp. 218-238, 1990, doi: 10.1007/0-387-34805-0_21

[14] SPRENGERS, M.: *GPU-based Password Cracking: On the Security of Password Hacking Schemes regarding Advances in Graphics Processing Units*, M. S. thesis [Online]. Fac. Sc., Radboud Univ. Nijmegen, Nijmegen, The Netherlands, 2012. Available: http://enricopagliarini. com/wp-content/uploads/2012/02/thesis.pdf

[15] WANG, X., FENG, D., LAI, X, YU, H.: *Collision for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, 2004 [Online]. Available: http://eprint.iacr.org/2004/199

[16] LENSTRA, A., WANG, X., De WEGER, B.: *Colliding X.509 Certificates,* 2005 [Online]. Available: http://eprint.iacr.org/2005/067

[17] SOTIROV, A., STEVENS, M., APPELBAUM, J., LENSTRA, A. et al.: *MD5 Considered Harmful Today*, 2008 [Online]. Available: http://www.win.tue.nl/hashclash/rogue-ca/

[18] KLIMA, V.: *Finding MD5 Collisions - a Toy for a Notebook*, 2006 [Online]. Available: http://eprint.iacr.org/2005/075

[19] US-CERT: *MD5 Vulnerable to Collision Attacks*, 2008 [Online]. Available: http://www.kb.cert.org/vuls/id/836068

[20] STEVENS, M.: *Single-block Collision for MD5*, 2012 [Online]. Available: http://marc-stevens.nl/research/md5-1block-collision/

[21] EATLAKE, D. 3rd, JONES, P.: *US Secure Hash Algorithm 1 (SHA1)*, 2001 [Online]. Available: tools.ietf.org/html/rfc3174

[22] WANG, X., YU. H. IN, Y. L.: Efficient Collision Search Attacks on SHA-0, *Lect. Notes Comput. Sc.*, vol. 3621, pp. 1-16, 2005, doi: 10.1007/11535218_1

[23] PIETRYGA: *SHA-1.svg*, 2007 [Online]. Available: https://commons.wikimedia.org/wiki/File:SHA-1.svg

[24] CANNIERE, C. RECHBERGER, C.: Finding SHA-1 Characteristics: General Results and Applications, *Lect. Notes Comput. Sc.*, No. 4284, pp. 1-20, 2006.

[25] STEVENS, M.: New Collision Attacks on SHA-1 Based on Optimal Joint Local-collision Analysis, *Lect. Notes Comput. Sc.*, No. 7881, pp. 245-261, 2013, doi: 10.1007/978-3-642-38348-9_15

[26] LAMBERGER, M, MENDEL, F.: *Higher-Order Differential Attack on Reduced SHA-256*, 2011 [Online]. Available: http://eprint.iacr.org/2011/037
[27] BERTONI, G., DAEMEN, J., PEETERS, M. ASSCHE, G.: *Sponge Functions,* Proc. ECRYPT Hash Workshop 2007, Barcelona, 1997.
[28] AUMASSON, J. P., MEIER, W.: *Zero-sum Distinguishers for Reduced Keccak-f and for the Core Functions of Luffa and Hamsi*, 2009 [Online]. Available: https://131002.net/data/papers/AM09.pdf
[29] MING, D. XUAJIA, L.: *Improved Zero-sum Distinguisher for Full Round Keccak-f Permutation,* 2011 [Online]. Available: http://eprint.iacr.org/2011/023
[30] POLK, T., CHEN, L., TURNR, S., HOFFMAN, P.: *Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms*, 2011 [Online]. Available: http://tools.ietf.org/html/rfc6194
[31] FERNANDEZ, D.: *How to Encrypt User Passwords,* 2013 [Online]. Available: http://www.jasypt.org/howtoencryptuserpasswords.html
[32] DANG, O.: *NIST Special Publication 800-106: Randomized Hashing for Digital Signatures,* 2009 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-106/NIST-SP-800-106.pdf
[33] RUKHIN, A., SOTO, J., NECHVATAL, J., SMID, M.: *NIST Special Publication 800-22, Revision 1a: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,* 2010 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/ 800-22-rev1a/SP800-22rev1a.pdf
[34] TURAN, M. S., BARKER, E., BURR, CHEN, L.: *NIST Special Publication 800-132: Recommendation for Password-Based Key Derivation, Part 1: Storage Applications,* 2010 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
[35] HORNBY, T.: *Salted Password Hashing - Doing it Right*, 2013 [Online]. Available: https://crackstation.net/hashing-security.htm
[36] WU, M.-L.: Nonce-aware Encryption Scheme, *WSEAS Trans. Inf. Sc. Appl.*, vol. 6, No. 9, pp. 1513-1522, 2009.
[37] SHIREY, R.: *Internet Security Glossary, Version 2*, 2007 [Online]. Available: https://tools.ietf. org/html/rfc4949
[38] HELLMAN, M.: A Cryptanalytic Time-Memory Trade-Off, *IEEE Trans. Inf. Th.*, vol. 26, No. 4, pp. 401-406, 1980.
[39] OECHSLIN, P.: *Making a Faster Time-Memory Trade-Off,* Proc. of 23rd Annu. Int. Cryptology Conf. (CRYPTO 2003), Santa Barbara, pp. 617-630, 2003.
[40] MANBER, U.: *A Simple Scheme to Make Passwords Based on One-Way Functions Much Harder to Crack,* 1994 [Online]. Available: http://webglimpse.net/pubs/TR94-34.pdf
[41] BELLARE, M., CANETTI, R., KRAWCZYK, H.: *Keying Hash Functions for Message Authentication,* 1996 [Online]. Available: http://cseweb.ucsd.edu/~mihir/papers/kmd5.pdf
[42] MICHAILH, E., KAKAROUNTAS, A.P., E. FOTOPOULOU, E., GOUTIS, C. E.: Novel Hardware Implementation for Generating Message Authentication Codes, *WSEAS Trans. Commun.*, vol. 4, No. 11, pp. 1276-1283, 2005.
[43] SHINER, J.: *Defending Against Crackers: Peanut Butter Keeps Dogs Friendly, Too,* 2011 [Online]. Available: http://blog.agilebits.com/2011/05/05/defending-against-crackers-peanut-butter-keeps-dogs-friendly-too/
[44] PERCIVAL: *Stronger Key Derivation via Sequential Memory-Hard Functions,* 2009 [Online]. *Proc. BSDCan'09*, Ottawa, 2009. Available: http://www.bsdcan.org/2009/schedule/attachments/ 87_scrypt.pdf
[45] DUDAS, A., JUHASZ, S.: Blocking and Non-blocking Concurrent Hash Tables in Multi-core Systems, *WSEAS Trans. Comput.*, vol. 12, No. 2, pp. 74-84, 2013.

Zdenek Hon - Pavel Smrcka - Karel Hana - Jan Kaspar - Jan Muzik - Radek Fiala - Martin Viteznik - Tomas Vesely
Lukas Kucera - Tomas Kuttler - Radim Kliment - Vaclav Navratil *

A SURVEILLANCE SYSTEM FOR ENHANCING THE SAFETY OF RESCUE TEAMS

The article summarizes preliminary results of the research and development of a system focused on enhancing the safety of teams participating in the integrated rescue system managing extraordinary events or crisis situations (fire, mass disaster, release of harmful industrial substances), and on the support in the course of training. Individual partial technical solutions are mentioned, which should lead to providing automatized telemetric monitoring equipment in a more resistant form making it possible to recognize the nature and intensity of the motion, including the determination of the topical and total energy outputs, monitoring of environmental parameters (temperature, smoke, etc.) and back analysis of the intervention course or training in real time, and the monitoring of health-physiological parameters and signalling risk conditions (physical exhaustion, stress, overheating, etc.) under extreme measures.

Keywords: *Integrated rescue system, monitoring, surveillance system, safety.*

1. Introduction

The contemporary world faces new challenges associated with the development of society, particularly the permanent and sustainable development, protection of the health and life of the population and environmental protection . The essential viewpoint includes the permanent flow of important data, their evaluation and final determination of appropriate decisions [1]. This doubtlessly also holds in the field of telemetry which includes a set of technologies and methods facilitating remote measurements of physical quantities including the transfer of the data measured. Bio-telemetric systems are also of importance from the operation stand point being based on the principles of monitoring the individual's psychophysiological condition applied to military disciplines and to monitoring workers in further heavy-duty professions, such as operators of complex technical facilities (as, for example, nuclear power plants), professional chauffeurs of motor vehicles in long-distance transport and, last but not least, members of rescue teams [2 and 3].

During interventions by and training of rescue teams, the members are able to take advantage of wearable automatized monitoring equipment which could also be able to provide combined relevant data about the position, personal health-physiological condition and environmental parameters in the surroundings of the monitored member of the rescue team even under extreme circumstances. These are very important parameters directly affecting the efficacy/quality of the intervention and safety of particular members of the team participating in the intervention.

The article dealing with the condition of the project studied within the framework of the safety research, with the aim to develop a functional sample of this bio-telemetric surveillance equipment for selected teams of the integrated rescue system, includes a brief outline of existing concepts of supporting systems for members of rescue teams throughout the world: those examples of systems were selected which exert their obvious application potential and thus, they are not a matter of academic projects only. The basic principal function of the surveillance equipment developed including partial results of the project is mentioned further.

2. Surveillance supporting systems developed for rescue services

LifeNet is a system aimed at the location of firefighters operating inside of complex buildings. It is based on a principle similar to that where the firefighters draw a guiding rope which, for example, serves to aid the rapid navigation through smoky environments where visual orientation is impossible, or can

* [1]Zdenek Hon, [2]Pavel Smrcka, [2]Karel Hana, [2]Jan Kaspar, [2]Jan Muzik, [2]Radek Fiala, [2]Martin Viteznik, [2]Tomas Vesely, [2]Lukas Kucera, [2]Tomas Kuttler, [2]Radim Kliment, [1]Vaclav Navratil
[1]Department of Health Care Disciplines and Population Protection, Faculty of Biomedical Engineering, Czech Technical University in Prague, Czech Republic
[2]Joint Department of Biomedical Engineering Czech Technical University and Charles University in Prague, Faculty of Biomedical Engineering, Czech Technical University in Prague, Czech Republic
E-mail: zdenek.hon@fbmi.cvut.cz

also help find a member of the team attached to the second end of the same rope. The LifeNet system attempts to implement this concept under conditions using modern technologies. The firefighter wears equipment making it possible to hand throw, or automatized throwing, away of a few beacons (buoys) which subsequently serve as admission points. These beacons are able to detect particular members of the team in their vicinity with the use of an ultrasonic transmitter including their distance and position with respect to the beacon. Thanks to this the firemen can be located inside of extensive complexes. Miniaturized monitors can be connected to the equipment which are situated in the respirator of the firefighter and thanks to them, the firefighter performing the direct intervention can observe his position and the position of other members with respect to particular beacons. The firefighter location with the help of particular beacons is provided in cooperation with equipment attached to the firefighter's footwear. This equipment also includes a temperature sensor with a possibility of connecting to further sensors, as, e.g., an accelerometer, with the help of the I2C interface. Currently, this system is in the developmental prototype stage [4 and 5].

The *MiTag* (Medical information Tag) system is designed for acquiring data from a number of persons involved. However, its concept is related to the surveillance system for intervening teams. The system is based on the MiTag platform which comprises two wireless interfaces. The interface providing the communication with sensors forms the Body Area Network (BAN). The communication with the display is provided by a MESH type long-range network. The system also includes repeaters which can be thrown away along the path between the display unit and patient in the cases where direct attainability of the signal from the platform on the patient to the display is impossible. The protocol of the MESH network then redirects the flow of data through these repeaters, thus providing a theoretically unlimited distance, along which the data can be transferred. Many different sensors can be connected to the platform (GPS, pulsed oximetry, blood pressure or temperature sensors, ECG, etc.) [6].

The *FireNet* presents an architecture of a wireless network directly designed for needs of transferring data taken by sensors in the case of firefighting emergency operations. The Ad-Hoc type network is capable of its own reconfiguration as required of transferring data to the site established. Different types of sensors are connected to the network, situated on firefighters themselves or on some parts of their equipment, as for example, on vehicles. On vehicles there is also a GPS receiver which can be used for the location of firefighters, and with the help of the network itself, it is then possible to partially locate relative positions of particular points. Data acquired is transferred to the display equipment at the commander of the intervention on the one hand, and with the help of internet, to the firefighting central command on the other. Thereafter, both groups have admission to online data acquired from the site of the intervention [7].

The *FIRE* (Fire Information and Rescue Equipment) system takes advantage of using the SmokeNet sensor network. These are sensors provided in the building within the framework of anti-fire prevention. The sensors must be installed in every room and separated one from another by about 10 m. The FIRE system is able to use the network of these sensors for the locating of the firefighters in the building. The system is simultaneously able to acquire further data from the Smoke Network as, e.g., information of what rooms have been hit by the fire. The system also includes a miniature display FireEye which the firefighter is equipped with and thus, is able to clearly monitor important data. The system is currently under development and testing [8].

ProeTex is a project which is implemented under the support of the 6th framework programme of the EU. The project is primarily focused on the development of "smart textiles" which could be employed in the future for the production of protective clothes and auxiliaries for firefighting teams. Textile sensors developed within the framework of this project are particularly aimed at scanning basic life functions, physiological parameters and potential activity of chemical hazards (toxic substances, etc.) along with problems of power supply units for their equipment [9]. In accordance with information available, some the textile sensors are interconnected in a classical way through cables, which facilitates the design and implementation of the system to a certain extent (the complicated stage of designing and testing the radiofrequency interface is eliminated; this solution has further positive effects on the electric power consumption, since compared to the wireless transfer, its energy efficacy is principally higher). However, a disadvantage of this solution is a certain restriction to the user and significant increase in effects on his comfort. Cables serving the interconnection of particular points are relatively susceptible to the damage (for example, material damage due to fatigue of the conductors themselves by mechanical stress in the same parts of clothing).

3. Surveillance system for supporting intervention by and training of Integrated Rescue System - FlexiGuard

FlexiGuard is an abbreviated name of the project which is currently being designed by a team of investigators at the Faculty of Biomedical Engineering, Czech Technical University in Prague. The target of the project is the development of a telemetric monitoring system in a more resistant form, allowing for the locating of particular members of the rescue team, monitoring of their health-physiological parameters (pulse, pressure, skin resistance - sweating, temperature), automatic detection and signalling of hazard conditions, such as physical exhaustion, excess stress, overheating, etc., in real time and under extreme circumstances. Further, it will make the differentiation of the nature and intensity of their motion (lying, standing, running,

crawling, etc.) possible, including the identification of topical and total energy output, monitoring of environmental parameters (temperature, smoke, etc.) and further conditions depending on actual requirements of selected teams of the Integrated Rescue System.

Expected users of the resulting project were defined in the course of the project preparation. The possibilities of its use were particularly based on the needs of training particular types of users and methods developed for use in possible extraordinary events and crisis situations both common and uncommon. The expected users of the project results with specifying the framework of the use are outlined below.

- Health rescue service – training, interventions of members of the health rescue service and monitoring of people injured in mass accidents, etc.
- Firefighting emergency teams – training, protection in all the types of interventions, particularly interventions with the use of respirators, physically tedious interventions, extensive fires, floods, mass accidents.
- Mountain rescue service – training, navigation and location, prevention of collapse and physical exhaustion under conditions of high altitudes above the sea level.
- Police corps – training, intervention of special teams, large-extent interventions.
- Mining rescue service – training, interventions under the ground, possibilities of location in smoky environment.
- Water rescue service – training, work under the water surface.
- Army – training and special interventions.

Principles of the function and continuous results of the FlexiGuard surveillance system

The surveillance system is focused on establishing a sensor network allowing for the wireless transfer of physiological and environmental quantities from the user body or from a close vicinity (for example, from clothes). The wireless solution was chosen with respect to the possibility of system integration into equipment and resistance to the mechanical damage.

Particular quantities, i.e., technical, physiological, environmental, etc., are scanned with the help of a network of sensors and data from sensors measured in this way and are digitalized and transferred wirelessly by a modular scanning unit: for details see Fig. 1.

The topology of the system testing sample is based on the BAN (Body Area Network) and the data is thus scanned from probands with the help of a network of sensors (in the future incorporated for example in the gear of the Integrated Rescue System member), and signals from the sensors can be digitalized and transferred within the framework of the BAN network node to the modular scanning unit wirelessly, by a short-range communication interface.

Every member of the team has his own modular scanning unit to which data from appropriate autonomous sensors are transferred. The data is transferred from the modular scanning unit to the local visualizing unit and processed by the software to simple output data, useful, for example, for the intervention commander. A possibility of the transfer to a distanced visualizing unit is also expected, for example, to the controlling position, if possible.

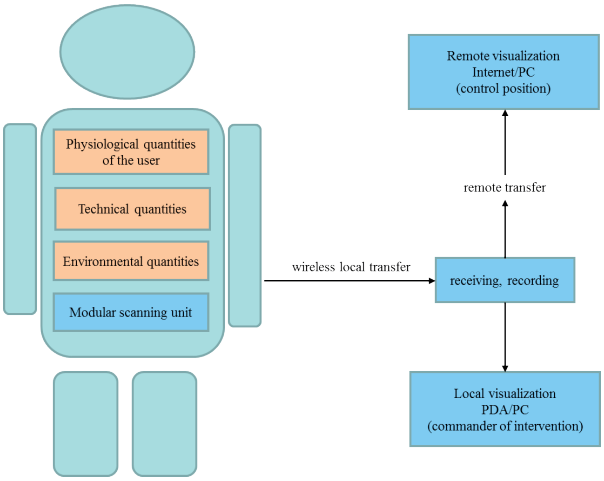


Fig. 1 Principles of the FlexiGuard surveillance system function

The data can be distributed in two independent manners. The first one dispatches in real time to the visualizing unit with the help of a long-range wireless network (on-line regimen). There is also a possibility to store the data on a recording medium (microSD) which is a part of the modular scanning unit and to read them later with the help of the USB connection to the PC (off-line regimen).

Within the framework of the project, several variants of visualization (analysing) units were prepared and verified in the form of a PC, more resisting notebook and PDA which were equipped with a specially designed and debugged application software. For purposes of testing the basic modular scanning unit, at the present stage of the project, the notebook with enhanced resistance was most successful as the visualization unit. The visualization unit in its basic variant is able to receive, display and file data from connected modular scanning units in real time.

The visualizing unit software itself is arranged as a component system and makes possible the subsequent extension by advanced reconstructing and visualizing algorithms which are able to display data received in real time, to file them on a memory medium and to evaluate them in real time in accordance with the requirements of future application variants of the system. The software for the visualizing unit is also ready to work with a remote data base (administration of personal safety profiles of users and data). In the basic variant of the supporting software visualizing unit, at this stage of the project solution, processing and analysis of the following quantities were implemented:

- topical load – calculation based on the Astrand-Ryhming chart; input parameters such as the mass, height, age, sex, maximum pulse frequency, maximum oxygen consumption (VO2max), energy equivalent for oxygen and topical pulse frequency,
- integral load – aggregation of the topical load in defined sliding time window,
- body position – differentiation between several positions (lying, standing, etc.),
- load – as calculated from accelerometers data,
- actual condition of the battery and estimate of its endurance,
- body temperature – measured by a thermistor in the zone of the thorax,
- external temperature (temperature of the environment),
- adaptive processing of the pulse frequency, elimination of artefacts.

The principle of the interconnection of modular scanning units with the visualizing unit is shown in Fig. 2. The modular scanning unit is equipped with several interfaces (wireless BAN network, A/D converters) for connecting various sensor types. Any sensor equipped with an appropriate interface can be theoretically connected. Every member of the team has his own modular scanning unit to which data is sent from relevant nodes of the BAN network, i.e., autonomous sensors. There is also a possibility of directly connecting the analogue sensors without using a further node of the BAN network. The modular scanning unit is also equipped with a wireless communication interface for the communication with the visualizing unit.

The connection of sensors (BAN nodes) to the modular scanning unit is completely automatized. After switching on the sensor and situation within the wireless range of the unit, the sensors are automatically connected to the unit. In the course of the measurement, particular sensors (BAN nodes) can be arbitrarily connected or disconnected. The disconnection of sensors is performed only by their deactivation or removal beyond the range of the radio communication. The re-connection is carried out by switching on or returning into the range of the modular scanning unit without necessary re-starting or affecting already connected sensors.

Within the framework of the project, the basic hardware platform was provided for the research and development of particular required measurements and communication modules with detection algorithms of subsequent debugging application variants. The testing sample arranged, already in the basic variant, makes it possible for the on-line monitoring of basic physiological and environmental parameters:

- ECG and pulse frequency derived from it – a source signal for monitoring the adaptability of the Integrated Rescue System members to load and stress situation and for automatized estimate of the energy output,

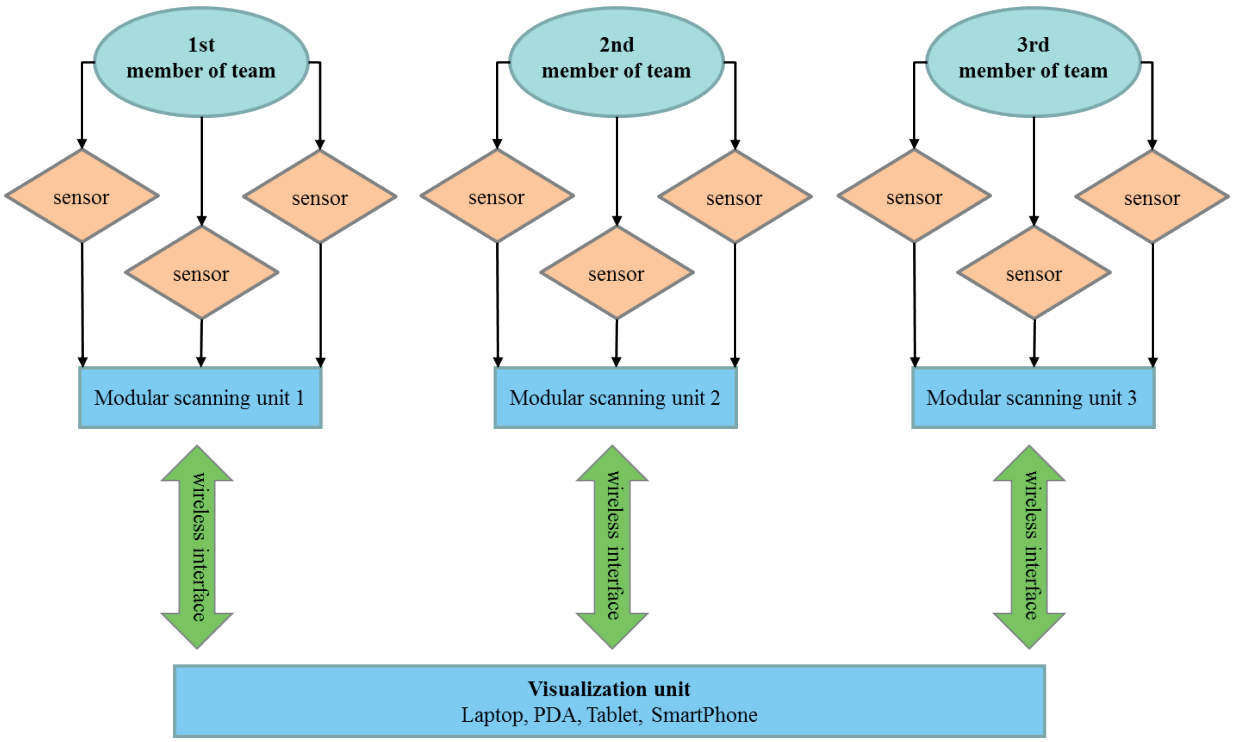


Fig. 2 Modular concept of the FlexiGuard surveillance system

- actigram measured by a tri-axial accelerometer, serving as a source signal for subsequent derivation of information about the nature and intensity of the physical activity (rest, walking, running, crawling), about the body position (lying, standing) and about the physical load intensity,
- body temperature, temperature of the environment and air humidity (can be measured at several points - a source signal for the assessment of the thermal comfort or of overheating selected parts, for example, the gear, etc.).

Modules have also been prepared for the measurement of the blood saturation with oxygen, surface scanning of the myogram, blood pressure, breathing frequency, skin resistance, etc. The set of these basic parameters is quite open, and based on continuously providing feedback in debugging of the system with members of the Integrated Rescue System, the set of source signals can be supplemented and refined on demand. For example, from the present analysis of the needs of the Fire Rescue Service of the Czech Republic it follows that for the application variant, the training monitor can be suitably supplemented, for example, by scanning the position of the proband (firefighter) or detecting selected gases. There is an important possibility to use the system for monitoring exposure to carbon monoxide through the course of the intervention without using an autonomous breathing apparatus. In accordance with the literature, there is a risk that particularly in long-term and repeated exposures, its effects are frequently underestimated due to its physicochemical characteristics (carbon-monoxide is odourless, colourless and non-irritating).

Technical verification of the FlexiGuard surveillance system function

Within the scope of the project, in addition to the proposal of the implementation of outputs from the visualizing unit, the function of the modular scanning unit was technically verified, which serves for scanning data from individual sensors and for their transfer just into the visualization unit. The technical verification of the function was provided with the help of laboratory and semi-field experiments. The team of investigators performed a number of controlled technical experiments simulating different loading situations in the laboratory (rest condition, running, knee bends, crawling, etc.). Data from these experiments will further serve in checking the algorithms of processing and also in the consideration of the use of the quantity monitored by measurements in practice.

Within the framework of the first field experiments, technical parameters of the basic scanning unit including the capacity of the communication channel were verified in the pilot plant environment. Information was acquired concerning the suitable situation of sensors, the physical arrangement and ergonomic requirements for the measuring equipment. The algorithm for the estimation of the load or energy output was also tested. The results and experience acquired will be immediately employed at the next stages of the project solution, on the one hand for the optimization of the testing sample, and also in the development of end application variants of the system (training and intervention monitor).

4. Conclusion

The surveillance system developed is designed in a modular form with the possibility of easy extension by further application hardware and software modules based on the requirements of particular end users. It is thus possible to add, for example, a sensor for the detection of selected groups of dangerous substances, or to arrange the software for outputs from data measured and thus to establish a system “tailored to” a particular user.

In cooperation with selected components of the Integrated Rescue System, application requirements will be further developed for the training or intervention module in order that the resulting application variants of the system might be used in practice while enhancing the safety of the intervening members of the Integrated Rescue System teams.

The resulting training module will be applicable to individual monitoring and quantification of the course of training particular members of the team in real time, to determining the immediate reaction to different situations (stress, load), to recording the course of the training and subsequent long-term monitoring of the course of particular parameters during the training process - determination of the progress of particular members in the course of training, evaluation of the training efficacy, and the determination of individual limit parameters of particular team members at a certain stage of the training.

The resulting intervention module will be applicable as a supporting, protecting and surveillance tool for members of selected teams of the Integrated Rescue System through the course of the intervention. The system operation will be based on the principle of monitoring physiological parameters in individual intervening persons and supplementary information on the surrounding environment. It will also be able to provide automatized detection of critical conditions (overheating, physical exhaustion, extreme stress) their automatic signalization and location of particular members of the team.

The whole surveillance system is designed on the one hand for supporting the decision process of the commander of the Integrated Rescue System intervention in real time and also for back evaluation of the course of the intervention and for acquiring and visualizing summarized and individual data on the behaviour of members of the team in managing different situations through the course of the intervention and in training.

Acknowledgements

This work was supported by Project No. VG20102015002, Ministry of the Interior of the Czech Republic.

References

[1] RISTVEJ, J., ZAGORECKI, A.: Information Systems for Crisis Management - Current Applications and Future Directions. *Communications - Scientific Letters of the University of Zilina*, vol. 13, No. 2, pp. 59-63, 2011, ISSN 1335-4205.

[2] HON, Z. et al.: Biotelemetry and its Use for Rescue Teams. *Urgent Medicine,* vol. 16, No 1, 2013, pp. 29-32, ISSN 1212-1924.

[3] REHAK, D., DUDACEK, A., POLEDNAK, P.: A Multipurpose Robotic Vehicle for the Rescue of Persons and Interventions in Emergency Situations. *Communications - Scientific Letters of the University of Zilina*, vol. 15, No. 1, pp. 103-109, 2013, ISSN 1335-4205.

[4] KLANN, M. et al.: *LifeNet: An Ad-hoc Sensor Network and Wearable System to Provide Firefighters with Navigation Support*. Adjunct Proc. Ubicomp Innsbruck, Austria. 2007. pp. 124-127. Available at: http://eprints.lancs.ac.uk/13037/2/2007-LifeNet.pdf.

[5] KLANN, M.: *Tactical Navigation Support for Firefighters: The LifeNet Ad-Hoc Sensor-Network and Wearable System*. J. Loffler and M. Klann. Mobile Response. Berlin: Springer, 2009. pp. 41-56, ISBN 978-3-642-00439-1.

[6] TIA, G. et al.: *Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results*. Proc. 2008 IEEE Intern. Conference on Technologies for Homeland Security. May 2008, pp. 187-192. Available at: http://www.cs.jhu.edu/~ljh/ paper/ieeehst2008.pdf.

[7] KEWEI, S., WEISONG, S., WATKINS. O.: *Using Wireless Sensor Networks for Fire Rescue Applications: Requirements and Challenges*. Electro/information Technology, 2006 IEEE Intern. Conference, May 2006, pp. 239-244. Available at: http://ocu-stars.okcu.edu/ksha/sha06-firenet.pdf.

[8] WILSON, J., et al.: *A Wireless Sensor Network and Incident Command Interface for Urban Firefighting*. 2007 Fourth Annual Intern. Conference on mobile And Ubiquitous Systems: Networking & Services, 2007, pp. 19-25. ISBN 978-1-4244-1024-8. Available at: http://fire.me.berkeley.edu/Misc/Mobiquitous2007-JWilson.pdf.

[9] Advanced e-Textiles for Firefighters and Civilian Victims [online], [vid. 09. 09. 2014]. Available at: http://proetex.org.

Anton Osvald - Maria Luskova - Markku Parviainen - Mika Rasanen - Jozef Svetlik -Jaroslav Flachbart
Miroslava Vandlickova - Vladimir Mozer *

FIRST RESPONDERS FIELD TRIALS OF SALIANT TECHNOLOGY

SALIANT - Selective Antibodies Limited Immuno Assay Novel Technology is the title of the research project developed and realised by a European consortium of biotechnology companies, universities and government forensic laboratories within the Seventh Framework Programme (FP7), Security Theme. The aim of this project was to develop a hand-held device for real-time analysis of trace levels of explosives, chemicals and drugs. The key innovation was a positive detection lateral-flow test for small molecules that is rapid, highly sensitive and simple to use making it ideally suited to deployment by First Responders and Forensic Service Providers at crime scenes and terrorist incidents. The Faculty of Special Engineering of the University of Zilina (FSE) as a project team member, was responsible for the task of evaluating the efficacy and sensitivity of the SALIANT technology for explosives detection for emergency responders' use. This paper provides the results and details about conducted experiments for the TNT explosive which were carried out in real-world conditions. The trials were specifically oriented on verification of the explosion products coverage and possibilities of their measuring by the SALIANT system.

Keywords: *Security, explosive, first responder, field trials, SALIANT.*

1. Introduction

Preservation and development of values of justice, freedom, and security is one the European Union main objectives. Although the European countries live in relative security, in their daily life they face many complex security threats and challenges. The fight against terrorism and organised crime, the protection of the external European borders and civil crisis management has gained the main importance. Four of five Europeans want more actions at EU level against organised crime and terrorism [1 and 2]. But no single Member state is able to respond to these threats on its own.

In February 2004, the European Commission launched a "Preparatory Action in the field of Security Research" (PASR) endowed with an estimated budget of 65 M€ for the period 2004-2006.. It was an important first step in addressing the need for Community action and aimed at establishing a fully-fledged Programme for Security Research in Europe from 2007. The Preparatory Action prepared the groundwork for a successful Security Research Programme [3 and 4].

The PASR was complemented by a number of projects funded under the 6th Framework Programme (FP6). In September 2004, the European Commission proposed the establishment of a "European Security Research Programme" (ESRP), to be funded over the period 2007-2013 under the 7th Framework Programme (FP7), endowed with an envisaged budget of 1.4 Bn€ [5].

Within the FP7, priority Security, the Faculty of Special Engineering of the University of Zilina (FSE) participated in the research project Selective Antibodies Limited Immuno Assay Novel Technology - SALIANT (2010-2013).

The SALIANT project was developed by a European consortium of biotechnology companies, universities and government forensic laboratories.

SALIANT aimed to develop a hand-held device for real-time analysis of trace levels of explosives, chemicals and drugs. The key innovation was a positive detection lateral-flow test for small molecules that is rapid, highly sensitive and simple to use making it ideally suited to deployment by First Responders and Forensic Service Providers at crime scenes and terrorist incidents.

Lateral flow immunodiagnostics has long offered the promise of fast, high quality testing for substances of low molecular weight such as explosives. There have, however, been very real challenges to bringing the full power of such technology to bear in this area. The problem is simply size. Large analytes can support the simultaneous binding of both capture and detector antibodies, allowing typical excess-reagent sandwich immunoassays to be formatted in which increasing analyte concentration provides an increase of observable signal over a very low zero background. Small molecules are simply not large enough to support such

* [1]Anton Osvald, [1]Maria Luskova, [2]Markku Parviainen, [2]Mika Rasanen, [1]Jozef Svetlik, [1]Jaroslav Flachbart, [1]Miroslava Vandlickova, [1]Vladimir Mozer
[1]Department of Fire Engineering, Faculty of Security Engineering, University of Zilina, Slovakia
[2]Reagena Oy Ltd, Toivala,, Finland
E-mail: anton.osvald@fbi.uniza.sk

simultaneous binding. Alternative systems in effect measure how much analyte is not present. This brings major problems in terms of precision, sensitivity and read-out where, classically, increasing concentration of analyte reduces the signal produced, making point-of-need devices often difficult to read. What is required is a robust system in which there is no observable signal in the absence of analyte, and even low level samples give an obvious observable signal over this zero background.

SALIANT offers a system based on a small bindable molety that is first conjugated close to the binding site of a primary antibody against the analyte such that when analyte binds the antibody, the molety can still be bound by a labelled secondary antibody. A large reagent-analogue of the analyte is also introduced, binding analyte – unbound primary antibody, and thereby blocking binding of the secondary antibody to the molety. Thus the more analyte that is present the more binding of secondary antibody occurs and the more signal is produced [6]._

2. Scope, objectives and the method of work

At present, taking and analysis of post-blast samples is carried out using standard methods. These methods use physical and chemical properties of the substances used in the manufacture of explosives. Sampling and subsequent analysis is carried out by laboratory methods IMS and LC MS that provide relevant results but they are demanding regarding to instrumentation and time. Method SALIANT focuses on sampling and detection of explosives based on the principle of immune assay.

The aim of the field trials was to verify the efficacy of the immunological method SALIANT for measuring explosion products.

2.1 TNT - 2, 4, 6 - trinitrotoluene

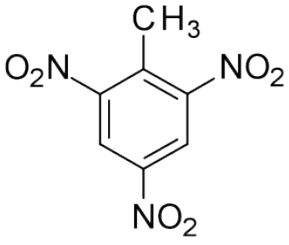


Fig. 1 Chemical formula for TNT

It is yellow-coloured solid best known as a useful *explosive material* with convenient handling properties. The explosive property of TNT is considered to be the *standard gauge of strength* of other *explosives*. By *detonation*, TNT decomposes in these ways:

$2\ C_7H_5N_3O_6 \rightarrow 3\ N_2 + 5\ H_2O + 7\ CO + 7\ C$

$2\ C_7H_5N_3O_6 \rightarrow 3\ N_2 + 5\ H_2 + 12\ CO + 2\ C$

Because TNT has an excess of carbon, explosive mixtures with oxygen-rich compounds can yield more energy per kilogram than TNT alone [7].

TNT is reported to contain 2.8 mega joules per kilogram explosive energy. The actual heat of combustion is 14.5 *megajoules* per kilogram, which requires that some of the carbon in TNT react with atmospheric oxygen, which does not occur in the initial event [8].

Quantitative methods used untill now are time consuming to evaluate what makes the investigation work more difficult. On the contrary, applied qualitative methods can quickly identify the various typical components of explosives but on the other hand the investigator can hardly map the whole area of events according to them.

Unlike the used methods, the system can also quantify the amount (concentration) in taken sample and thus to contribute to better and rapid mapping of the area of events after the explosion whereby the whole process of collection and analysis does not take more than 5 minutes.

2.2 Field tests – experiment SALIANT

2.2.1 Conditions and course of the SALIANT experiment

Based on the results of the zero experiment, the scheme of the sampling points for the experiment was adjusted (see Fig. 2). This experiment was carried out on April 9, 2013 in Kamenna Poruba - Zilina in the same area. Distances of sampling points from the explosion epicentre were shortened.

To capture detonation particles ceramic tiles, placed on the ground, were used. The samples were taken in direction of the axes 1, 2 and 3 in sequence from the explosion epicentre to the edge of the monitored area.

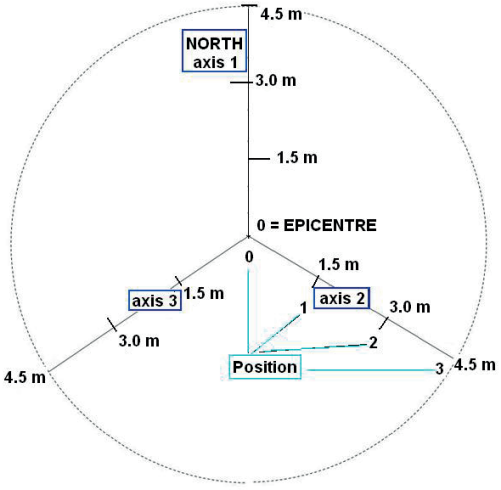


Fig. 2 Sampling points layout for the 1st SALIANT experiment

For explosions we used: 4 x 75 g of explosive (TNT - technical quality, volume of TNT min. 85%), (T).

2.2.2 Course of the first experiment

Figure 3 shows the experiment conditions. There was snow (several cm). Meteorological situation in the time of explosions is given in Table 1. Figure 4 shows collection of explosion products by SALIANT method.

Meteorological situation during explosions – first experiment Table 1

Date	Time of explosion	Wind course	Wind speed (m/s)	Pressure (hPa)	Humidity (%)	Temperature (°C)	Explotion
9. 4. 2013	8:45	NE	0.7	980	68	1.7	TNT 1
9. 4. 2014	9:53	ES	0.4	976	75	2.6	TNT 2

Fig. 3 Position of explosive charge and meteorological situation before explosion

Fig. 4 SALIANT wet wipe

2.2.3 Collection and evaluation of post blast products by SALIANT method

SALIANT method requires special tools to collect explosion products (see Fig. 5) as well as special process for chemical analytical evaluation of the sample (see Fig. 6).

Materials

- MilliQ water,
- Methanol,
- Glass tube 130 x 16 mm,
- Polyester TX715 swab (Basan),
- Paper mould for a square 10 x 10 cm.

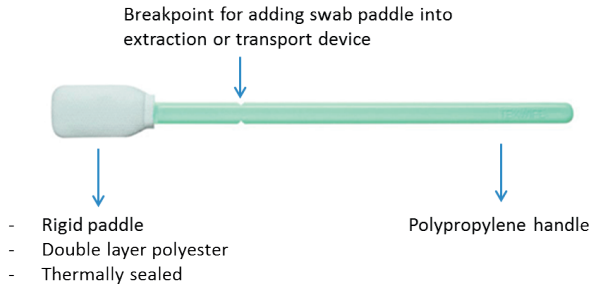


Fig. 5 Polyester TX715 swab

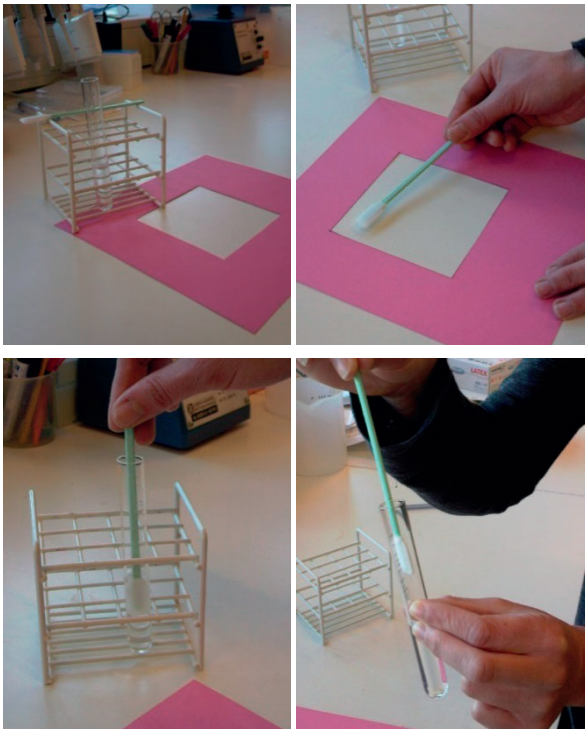


Fig. 6 Sampling of surfaces. Materials needed for wipe surface sampling (a), wiping a designated area with a swab (b), adding the swab to a tube with 5 ml methanol (c) and removal of swab from extract after incubation (d).

Sampling Method

1. Pre-wet swab with MilliQ water. Approximately 500 µl/swab, no dripping of liquid from swab.
2. Wipe area of 10 x 10 cm, use the paper pattern for the correct area - see Fig. 2.

Extraction with methanol:

- Add 5 ml of methanol to a clean glass tube.
- Place the swab in the tube.
- Shake and let it stand for 15 minutes at room temperature.
- Remove swab from tube.
- Homogenise the extract and use part of the extract for immunoassay.
- Store extract at 4 °C for conformation with LC/MS.

Dilute extract with LFIA assay buffer:

Dilute the sample 1/10 in LFD running buffer (100mM PBS with 0.25% BSA, 0.1% Triton X 100) NB final loading of Methanol should not exceed 10%.

Proceed with protocol immunoassay SALIANT

Add 80 ml of the extracted sample dropwise into the small aperture of the LFD cassette. A clear band of gold should been seen at the bottom of the window shortly after this. If no clear band is seen LFD may not be running correctly and repetition will be necessary.

Fig. 7 SALIANT wet wipe of the TNT explosive

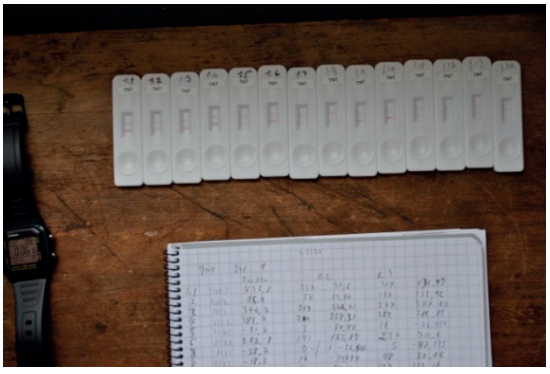


Fig. 8 Results

The wipes were evaluated by the reader (see Fig. 7). Figure 7 shows the reader with inserted wet strip and connected with computer. Figure 8 shows the results of experiment of April 9, 2013.

3. Results

The results of two explosions of each explosive are given in Tables 2 and 3. The first column indicates the No. of the sample with type of explosive (TNT - (T)). The second column indicates position at the explosion axis (A1, A2, A3) and distance from epicentre (1.5; 3.0; 4.5m) (see Fig. 1), the third and fourth columns indicate measurements, results of the reader, the third column - data after 2nd minute, the fourth column - data after 3rd minute. Symbol BG indicates the background (purity before explosion), epicentre is the place vertically below charge. **The values in the second and third minutes are different. Regarding the needs to develop high-speed detection system, it is assumed to make the methodology for measuring the second minute more accurate. For comparison the results, taken samples were analyzed also by current method IMS (Ionscan 4000) which did not indicate presence of the explosives in any of the samples.**

The results of measurements by SALIANT for the first TNT explosion Table 2

Code	Position	After 2nd min [ppb]	After 3rd min [ppb]
T1.0	BG		
T1.1	epicentre	234	314
T1.2	A1 / 1.5	54	120
T1.3	A1 / 3.0	209	274
T1.4	A1 / 4.5	200	282
T1.5	A2 / 1.5	3	18
T1.6	A2 / 3.0	141	234
T1.7	A2 / 4.5	1	5
T1.8	A3 / 1.5	16	48
T1.9	A3 / 3.0	62	124
T1.10	A3 / 4.5	171	271

The experiment confirmed the quality and sensitivity of the explosion products measurements. The BG (background) values were null. Because this area is usually used for making various indicated experiments it was needed to carry out check measurements. The area was free of explosion traces left from previous explosions. It is reasonable that wind affects direction and quantity of explosion products. This fact was confirmed by our experiments that indicated sensitivity of measurement by SALIANT. It is documented also by the graphs (Figs. 9 and 10).

The results of measurements by SALIANT for the second TNT explosion Table 3

Code	Position	After 2nd min	After 3rd min
		[ppb]	[ppb]
T2.0	BG		
T2.1	epicentre	11	43
T2.2	A1 / 1.5	32	69
T2.3	A1 / 3.0	5	53
T2.4	A1 / 4.5	1	19
T2.5	A2 / 1.5	31	92
T2.6	A2 / 3.0	84	142
T2.7	A2 / 4.5	77	137
T2.8	A3 / 1.5	17	64
T2.9	A3 / 3.0	31	81
T2.10	A3 / 4.5	189	240

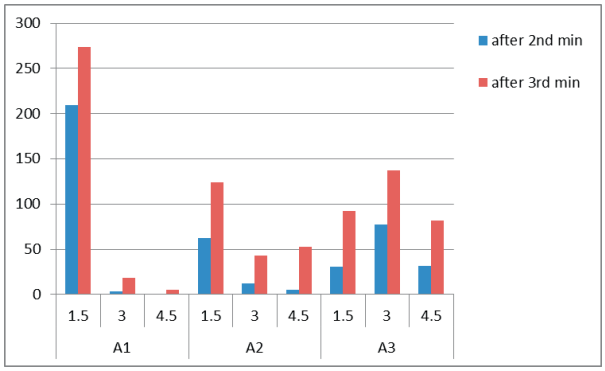


Fig. 9 First TNT explosion – results of measured values by SALIANT method

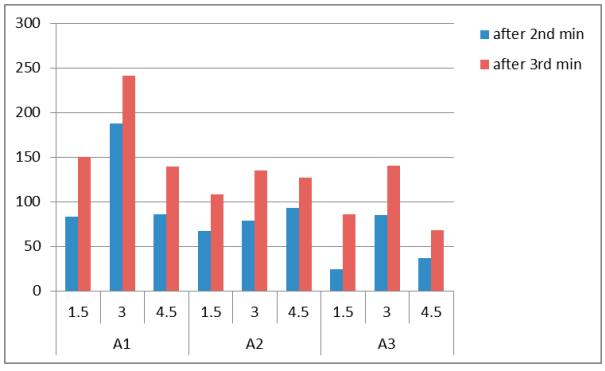


Fig. 10 Second TNT explosion – results of measured values by SALIANT method

The first experiment (Fig. 9) was performed under conditions of slow dead wind from the north side that blew away more explosion products within distance 1.5 m in axis A1. Minimum quantity fell in a distance of 4.5 and 3.0 m. . On other axes (A2 and A3) the explosion products were distributed proportionally.

The second experiment (Fig. 10) was performed under conditions of slow wind of south direction, which resulted in higher concentration of explosion products on axis A1, especially in position 2 (three meters). Other positions had proportional arrangement of explosion products with regard to collection place and atmospheric conditions.

The SALIANT system allows detection of other groups of explosives (RDX , HMX) in addition to TNT detection.

4. Conclusion

The SALIANT project yielded many positive experiences and benefits for the University of Zilina team. The first major benefit was the work experience in an international team of experts. The task our team was responsible for also brought its own challenges. The goal was aimed at the identification of dangerous substances, explosives and drugs. The area of explosives, which became the major objective of the project, was a new experience for us and required significant amount of learning and research into the topic for the UNIZA project team. With the assistance of the partner organisations we were successfully able to devise the methodology for the field tests. This was also positively appraised at the project workshop that was held at the University of Zilina at which the field tests and their outcomes were presented.

The results of the field trials confirmed two basic hypotheses. Firstly, the dimensional parameters of field trials were validated for low amounts of explosives together with the ways of residual sample collection for forensic purposes. Secondly, the SALIANT methodology, based on the immunological identification of explosives residue, was validated, as well as its qualitative and quantitative sensitivity [9].

The experimental work was quite difficult. The field trials were carried out in an open terrain affected by adverse weather conditions. Heavy machinery was required to manipulate and place the test vehicles in the right location on site. This had to be combined with high laboratory precision and sensitive electronic analysis. Is should be noted that not only Stage 6 – Field trials, but the entire SALIANT project required dedicated and focused work from all involved teams.

Acknowledgments

The paper presents the results of the research, namely the field tests carried out in the project SALIANT.

References

[1] Directorate - General for Internal Policies: *Citizens Rights and Constitutional Affairs.* Edition 5/2011[online]. [cited 1March 2012]. Available at: http://www.statewatch. org/news/2010/nov/ep-review-security-research-programme.pdf

[2] Research for a Secure Europe - *Report of the Group of Personalities in the field of Security Research,* Luxembourg : Office for Official Publications of the European Communities, 2004, ISBN 92-894-6611-1

[3] *Selective Antibodies*. 2013. Home. [online]. [cited 14 October 2013]. Available at: http://www.selectiveantibodies.com/

[4] BABRAUSKAS, VYTENIS: *Ignition Handbook*. Issaquah: WA: Fire Science Publishers/Society of Fire Protection Engineers, 2003, p. 453, ISBN 0-9728111-3-3.

[5] KLOUDA, K., KUBATOVA, H., ZEMANOVA, E.: Nanomaterials: Pros and Cons. *Communications - Scientific Letters of the University of Zilina*, 2011, vol. 13, pp. 6-12, ISSN 1335-4205

[6] JEANDESBOZ, J., RAGAZZI, F.: *Review of Security Measures in the Research Framework Programme.* European Parliament: Brussels, 2010 [online]. [cited 28 February 2012]. Available at: http://www. europarl.europa.eu/studie

[7] http://mysite.du.edu/~jcalvert/phys/bang.htm 08.12.2013

[8] TNS Opinion & Social: Special Eurobarometer 371 *Internal Security,* Fieldwork: June 2011, Publication: November 2011. [online]. [cited 1March 2012]. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf .

[9] OSVALD, A. et. al.: *SALIANT - Selective Antibodies Limited Immuno Assay Novel Technology*. Zilina : EDIS University of Zilina, p. 121, ISBN 978-80-554-0838-5.

Zoran Cekerevac - Zdenek Dvorak - Ludmila Prigoda - Petar Cekerevac *

RISKS OF BITCOIN VIRTUAL CURRENCY

Bitcoin, digital money got into focus after the Mt Gox crash. It uses P2P interaction where an owner transfers the electronic coin to the next owner signing and adding a hash of the previous transaction and the public key of the next owner. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double-spending and generation of non-existent money. Among the users, there is uncertainty about the safety on the theft and fraud. Among the authorities, there are dilemmas about present and future risks related to the Bitcoin implementation. The article deals with the benefits and risks of Bitcoin use.

Keywords: *Bitcoin, e-business, eWallet, fiat money, hash, P2P.*

1. Introduction

In history there were different means of payment. The U.S. dollar was the most frequently used means of paying almost fifty years after the World War II, but thanks to many problematic moves of the Federal Reserve reputation of dollar declined significantly and many began to seek alternatives [1]. To be a suitable means of payment, an asset must have some important features, such as: to remain valuable for a long time, to be in limited supply, to be easily divisible into parts, to be portable ... If these characteristics are compared to the dollar, gold (silver) and bitcoin, one can get the results shown in Table 1.

Payments through financial institutions are associated with numerous limitations and include relatively high costs whose amount is measured in percentage. Thus, for example, when money changes hands, significant amount remains in the banks. Because of that, and many other reasons, bitcoin[1], digital money, was created and launched in the year 2009. For Bitcoin creation Satoshi Nakamoto[2] is credited. He published the principles of its creation in the article Bitcoin: A Peer-to-Peer Electronic Cash System [2]. Bitcoin concept implies P2P interaction, and electronic coin is defined as a chain of digital signatures. Each owner transfers the coin to the next owner by signing a hash[3] of the previous transaction and the public key of the next owner, and adding it all to the end of the coin. The recipient can verify the signatures to verify the chain of ownership. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double payment and avoids the generation of non-existent money. Checking may take a few minutes. Average time of transaction

Comparison of characteristics of dollars, gold (silver) and BitcoinTable 1

Characteristic			
Stays Valuable	×	✓	✓
Limited Supply	×	✓	✓
Divisible	✓	✓	✓
Portable	✓	✓	✓✓

Source: Authors modelled on FEE [1]

[1]bitcoin – written in small letter b is considered as a currency; Bitcoin – with upper case letter B capital implies Bitcoin as a concept [29].

[2]It is not yet known whether „Satoshi Nakamoto" is real name or a pseudonym [31].

[3]More information about hash can be found in [28 and 30].

* **[1]Zoran Cekerevac, [2]Zdenek Dvorak, [3]Ludmila Prigoda, [4]Petar Cekerevac**
[1]Faculty of Business & Industrial Management UNION" University in Belgrade, Serbia
[2]Research Department of Crisis Management, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Maykop State Technological University, Maykop, Russia
[4]Faculty of Political Science, University of Belgrade, Serbia
E-mail: zoran@cekerevac.eu

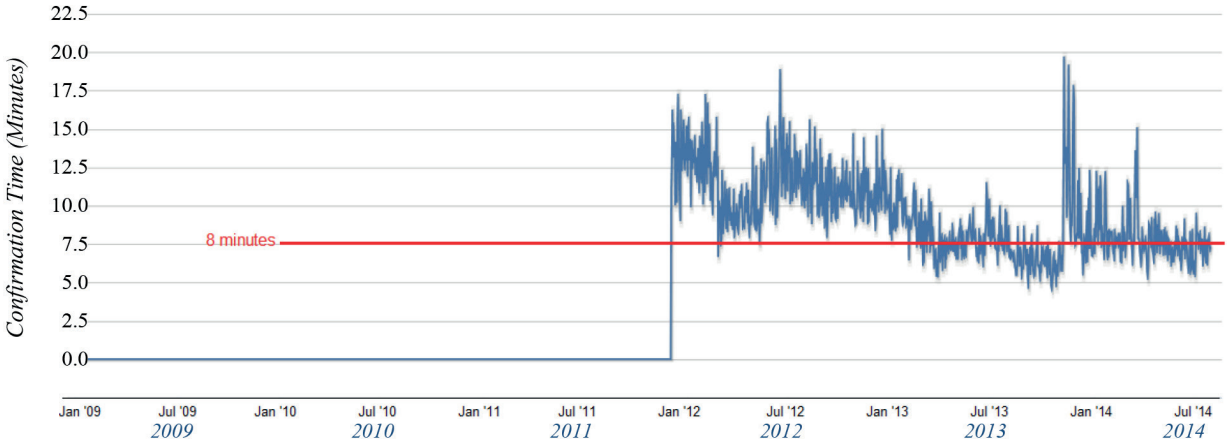


Fig. 1 Average transaction confirmation time in minutes. (Source: blockchain.info [3])

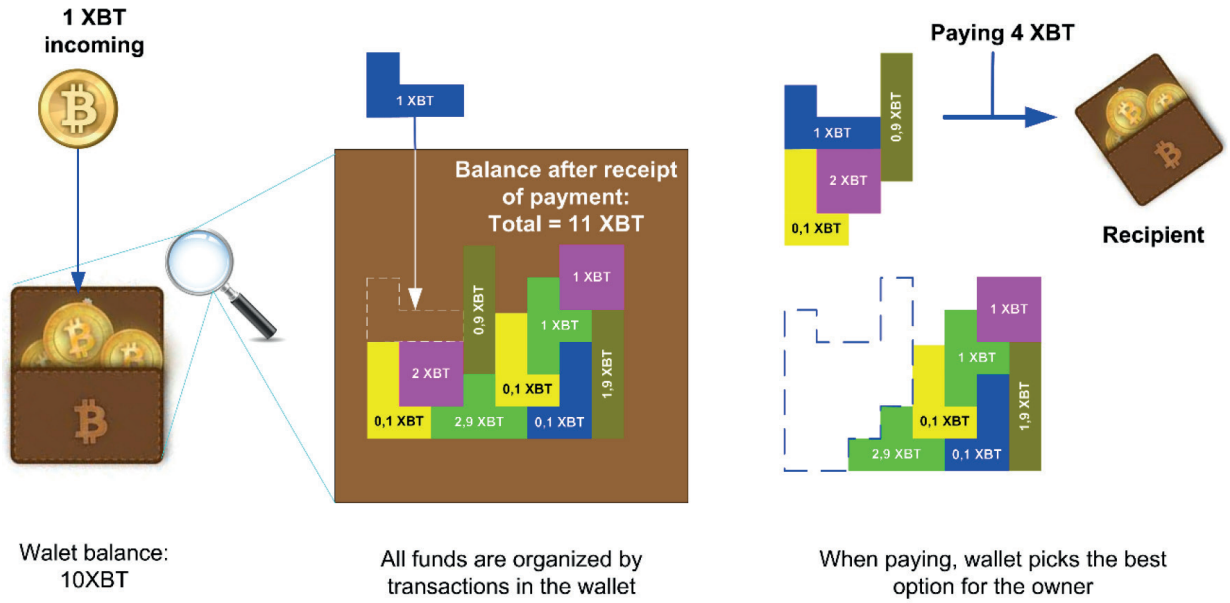


Fig. 2 Bitcoin payment technology (Source: Authors modelled on [4])

checking in 2014 was around 8 minutes. The transaction confirmation time in previous years is shown in Fig. 1.

These transactions do not transfer personal information between parties in the transaction. Unlike completely anonymous transactions, Bitcoin payment record of the transaction remains recorded and available to public. The participants in the transaction do not have to operate under their own names, but they can log in through aliases.

Bitcoin mining and payment details are discussed in [5, 6, and 7]. Figure 2 shows an example of Bitcoin payment. Some other examples of payments and the fees determining are presented in the Bitcoin Transaction Fees Explained [4]. Details on the application of Bitcoin technology are explained in R. Skudnov´s thesis: Bitcoin Clients [8].

2. Benefits and risks of using Bitcoin

2.1 Economic aspects of Bitcoin

Bitcoin offers lower transaction costs to users, increased privacy and protection of the purchasing power from inflation in the long run. However, Bitcoin still doesn't have enough participants and a financial base to ensure stability and bitcoin value considerably oscillates, as it is shown in Fig. 3 [9].

Still among the users there is uncertainty about the safety on the theft and fraud. Among the relevant state authorities, there are also numerous dilemmas and analyses of existing and future risks related to the implementation of Bitcoin. Despite all the dilemmas, many see the Bitcoin as an excellent means of payment that allows [10]:

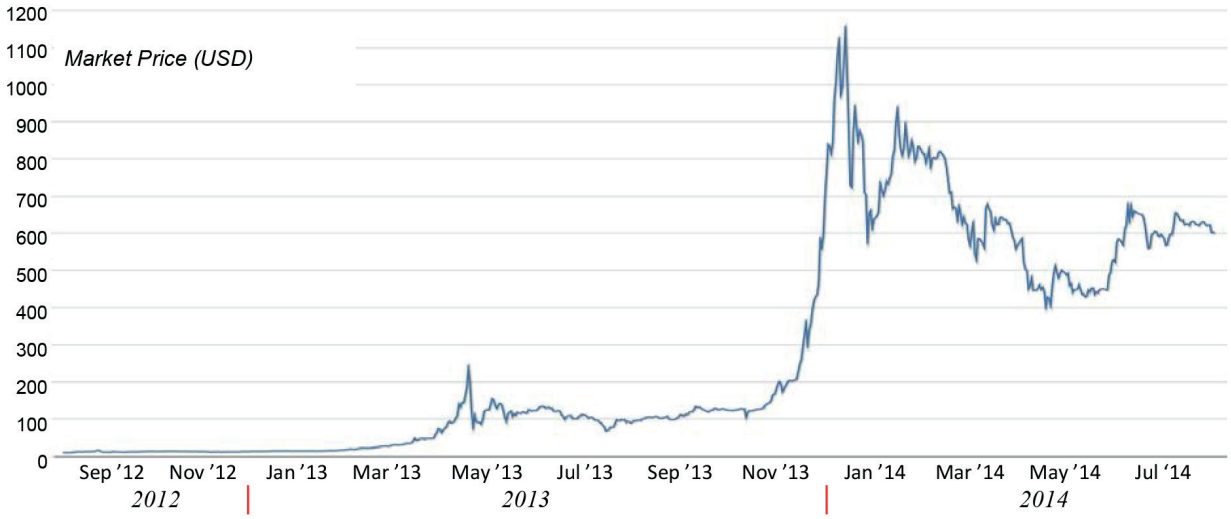


Fig. 3 XBT market price in USD Source: blockchain.info [9]

- buying anything in secret,
- absence of banks in the chain of payments,
- paying without commission,
- no worries that inflation will devalue the money in the future.

For the latter, as an example can serve the analysis of changes in the value of USD during the time. For example, if someone had 100 USD in his wallet in 1953, due to inflation, using the Consumer Price Index, today he could count with $11.48. The situation is even worse if calculation is made according to other criteria. Table 2 shows the equivalents of 100USD in comparison with 1913 and 1963.

Equivalent value of 100 USD from 1913 and 1963 in 2013 Table 2

	$100 from the year:	1913	1963
Equivalent in 2013	Using Consumer Price Index	$2,430	$761
	Using GDP deflator	$1,750	$588
	Using unskilled wage	$9,960	$817
	Using Production Worker Compensation	$14,200	$987
	Using nominal GDP per capita	$13,100	$1,570
	Using relative share of GDP	$42,500	$2,630

Source: Authors' compilation of data from MeasuringWorth.com [11]

How did it come to such a decline in the USD value? Simply! By printing money without backing. Bitcoin lets users know exactly how many bitcoins and when will be on market. Due to the applied algorithm it is known that the number of Bitcoin will asymptotically approach the figure of 21 million. From the first bitcoin launched in 2009, their number grew to 13 million in mid-July 2014 [12], and there will be 18 million (in 2024), and 21 million in 2140. After that, the number of issued bitcoin practically will not change. In this manner the second essential criterion from Table 1 is provided.

USD, silver, and gold are difficult to forge. Since the Bitcoin is based on the open source software it may seem that it is easier to falsify. However, Bitcoin is based on cryptography and it is practically impossible (or rather, unprofitable) to forge bitcoin. In addition, each transaction requires confirmation of other participants in the system, which prevents any wrongdoing of double payment.

In addition to the aforementioned benefits, there are also other benefits Bitcoin offers:

- Bitcoin can be very easily transferred from and to any point on Earth regardless of the quantity and geographic location if there is an Internet connection;
- accepting of Bitcoins is free;
- no chargeback;
- Bitcoin can be exchanged for any currency.

As a result of these advantages a favourable gradient increase in the daily number of transactions is recorded. From about 550 in January 2012, it rose to about 80,000 in January of 2014. After Mt Gox bankruptcy and disorder that was created, the number of transactions fell to about 55,000 in January 2014, but then suddenly increased to 70,000 in April, and then with oscillations fell to 60,000 in July of 2014 [13]. It can be said that it is very likely that Bitcoin will overcome the crisis caused by Mt Gox bankruptcy.

It's hard to declare some of the payment methods as the best, especially because the conditions are constantly changing, but it is likely that the Bitcoin, thanks to all its advantages will be able to take a very high position. Also, it is likely that the current dollar payment method can (will) be pushed toward the (much) lower positions [1].

2.2 Legal aspects of the risk of the use of Bitcoin

Bitcoin, due to the relative anonymity of its users, allows individuals to generate, transmit, launder and/or steal funds. Its application brings to investigators similar challenges as other virtual money, for example WebMoney, but also additional difficulties because of its decentralized nature. According to FBI estimates, with medium confidence, in the near future "cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies such as WebMoney, which they have little reason to abandon" [14]. This conclusion is based on the large bitcoin fluctuations in 2011. With the same confidence FBI believes that the Bitcoin will be used for money laundering. These assumptions are difficult to prove because there are too few reports on Bitcoin. Due to its decentralization, attacks to Bitcoin system will likely prove to have little success. Criminals will focus their attacks on private Bitcoin wallets and the third-party services.

Bitcoin transactions are public, but the only information that identifies Bitcoin user is pseudo random generated Bitcoin address that makes the transaction fairly anonymous. The transaction is not completely anonymous. Although the Bitcoin is highly decentralized, there is a place that can provide information about the participant in the payment. This is where the bitcoin is converted to fiat currency[4]. To increase the anonymity of transaction, users can [15, 16, 17, and 18]:

- create and use a new Bitcoin address for each incoming payment;
- route the entire traffic across the Bitcoin anonymisers;
- combine old Bitcoin addresses into a new address to deliver a new payment;
- use specialized services for money laundering;
- use eWallet services of third parties to consolidate their addresses. Today, there are third-party services that offer the option of creating eWallet which allows users to consolidate many Bitcoin addresses and to access simply to their bitcoins from any device;
- create Bitcoin clients and to increase anonymity easily, and to have a choice of Bitcoin addresses from which they wish to make the payment. In doing so users do not have to be particularly technically educated to make anonymous transactions.

Specifics of Bitcoin today represent a special challenge to detection and stopping of illegal activities. As a decentralized system, Bitcoin does not have a central institution and is not able to control and to report suspicious activities in accordance with the program of prevention of money laundering or to accept and enforce legal requirements, e.g. subpoenas. According to the FBI [14] the main vulnerabilities of decentralized payment systems are:

- lack of software or the ability to monitor and identify suspicious monetary pattern occurring in money laundering;
- lack of identification of the actual account holders as well as their physical location;
- absence of the history of transactions associated with the actual participants in the transaction;
- much more difficult identification of sources of funds compared to other types of online money;
- law enforcement cannot target one central location or company in investigations, or turn the system off.

As mentioned above, Bitcoin, like most virtual money, requires the user to use the services of a third party when converting Bitcoin in fiat money. Buying, selling, or bitcoin conversion to other types of money are done outside of P2P system. Due to the number and diversity of third-parties there is a real possibility of money laundering [19, 20, and 21]. Users who do not wish to use the services of third parties are given the opportunity to put their "buy" or "sell" the request on the freenode IRC (Internet relay chat) [5].

In July 2011, FinCEN[6] revised the definition of "money transmission services" which now means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." It is likely that the business model of many third-party Bitcoin services qualifies third party as money transmitter, and therefore, the money transfer services subsumes under 31 CFR Part 1010.100(ff) [22]. Third parties, Bitcoin service providers qualified as transmitters of money when want to work legitimately are required to register with FinCEN, and to implement programs to combat money laundering, to keep certain records, and to report suspicious activity and Foreign currency transactions. In some states Bitcoin third party service providers are required to obtain an official state license [23]. Therefore, under the pressure of legal norms, some of the service providers of Bitcoin set as a condition to the members to agree to provide provider "with current, accurate, and complete information about yourself as prompted by the registration process, and to keep such information updated" [25].

2.3 Aspect of system users

The risk of using Bitcoin exists and can also be analysed from system users' aspect. As mentioned, criminals cannot attack a central server, but can attack individual wallets and a third party - Bitcoin service providers. The first malware designed to

[5]fiat money: money (as paper currency) not convertible into coin or specie of equivalent value [24]
[6]http://webchat.freenode.net/
[7]Financial Crimes Enforcement Network – US Department of the Treasury

steal bitcoins from compromised Bitcoin wallet, "Infostealer. Coinbit" was discovered in mid-June 2011. The program was able to infect user's computer and to transfer digital Bitcoin wallet to the server in Poland [26]. Particularly at risk are users who do not use encryption in their Bitcoin wallets. About 25,000 Bitcoin theft cases, an attempt of fraudulent sale of Bitcoin worth 7 million USD, and stealing Bitcoin with online gaming sites in 2011, as well as theft of computer resources for bitcoin mining are discussed in the FBI report [14].

It is easy to conclude that banks will not look with favour to the development of competition and it wouldn't be odd if they tried to disrupt Bitcoin business.

A particular problem for many Bitcoin system users appeared when Mt Gox went down. It occurred from December 2013 until the final downfall of February 2014 when a message appeared on the website: "In light of recent news reports and the potential repercussions on Mt Gox's operations and the market, a decision was taken to close all transactions for the time being in order to protect the site and our users. We will be closely monitoring the situation and will react accordingly" [24]. Details about the Mt Gox fall were published in [27, 28, 29 and 30], and other sources. The other major providers of Bitcoin to fiat money exchange services distanced themselves from the Mt Gox act, and announced that they continue to operate normally.

Mark Karpeles, a former director of the service Mt Gox, spoke on the uncertainty of investing in Bitcoin. In his presentation, he explained that investing in Bitcoin is risky and that the high value of the Bitcoin is based on high demand, but there is no guarantee that tomorrow it will not be reduced to a value of 0. In the statement he said that it is not expected, but that it is possible [31]. Users have to decide whether they will continue to do business with bitcoins.

3. Conclusions

Number of users of Bitcoin system is growing, but it is still small compared to the number of credit card or fiat money users. Bitcoin system is great conceptual and technical achievement that can be used by existing financial institutions, and even governments.

Application of the Bitcoin system brings a number of benefits to users. It enables them to transact in a reasonably short time, for free or a minimal fee. In addition, this system allows them freedom and independence of financial institutions. With the growing number of participants the Bitcoin system should become more stable, and the value of bitcoin should less oscillate allowing to owners security in terms of the value of their money, bitcoin.

On the other hand, when the bitcoin stabilizes itself, and when the number of users becomes big enough, according to the FBI, and many others, Bitcoin will become a very useful tool for a variety of fraud and criminal activity. However, it is the same with any other money, including gold. Neither gold, nor paper money keep any record of previous money owners.

A slowdown in growth of number of Bitcoin system customers can be caused by unpleasant events, such as it was the case of the Mt Gox, as such as some reported cases of Bitcoin theft, or the legal prohibition on Bitcoin trade (China and India), but when the situation stabilizes and a legal framework is established, climate can change in a positive direction for Bitcoin.

Based on the above it can be trusted that Bitcoin will not be only a temporary phenomenon and that it will take its place on the Internet as a regular means of payment.

References

[1] FEE:. *The Truth about Bitcoin and Alternative Currencies*. YouTube. [Online] 12 11, 2013. [Cited: 07 26, 2014.] www.youtube.com/watch?v=AVdKgQ0jmH8.

[2] NAKAMOTO, S.: Bitcoin: *A Peer-to-Peer Electronic Cash System. bitcoin*. [Online] 2008. https://bitcoin.org/bitcoin.pdf.

[3] BLOCKCHAIM.INFO: *Average Transaction Confirmation Time*. BlockChain. [Online] 02 19, 2014. https://blockchain.info/charts/avg-confirmation-time?timespan= all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

[4] ANON: *Bitcoin Transaction Fees Explained. Bitcoin Fees*. [Online] 02 05, 2014. http://bitcoinfees.com/.

[5] VELDE, F. R: Bitcoin: *A Primer*. Chicago Fed Letter. [Online] 12 2013. http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

[6] CEKEREVAC, Z., CEKEREVAC, P.: *Bitcoin - Benefits and Risks*. Belgrade : Faculty of Business and industrial Management, 2014. Intern. scientific conference Management 2014, 978-86-6375-012-8.

[7] CEKEREVAC, P., CEKEREVAC, Z.: *Bitcoin - Benefits and Risks*. FBIM Transaction. [Online] 03 11, 2014. [Cited: 07 25, 2014.] http://www.meste.org/fbim/fbim_srpski/ FBIM_najava/V_Cekerevac.pdf. 2334-704X.

[8] SKUDNOV, R.: *Bitcoin Clients*. Turku : University of Applied Sciences, 2012.

[9] BLOCKCHAIN: *Market Price (USD).* Blockchain. [Online] Blockchain, 07 26, 2014. [Cited: 07 26, 2014.] https://blockchain.info/charts/market-price?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

[10] LUKIC, M.: *Electronic Currency Bitcoin Could Destroy the Dollar (in Serbian)*. Biznis & Finansije. [Online] 12 07, 2013. http://bif.rs/2013/12/elektronska-valuta-bitkoin-bi-mogla-unistiti-dolar/.
[11] WILLIAMSON, SAMUEL H: *Seven Ways to Compute the Relative Value of a U.S. Dollar Amount - 1774 to Present.* MeasuringWorth.com. [Online] 2014, http://www. measuringworth.com/uscompare/result.php?year_source=1913&amount=100&year_result=2013.
[12] BLOCKCHAIN.INFO. *Total Bitcoins in Circulation*. BlockChain. [Online] 02 19, 2014. https://blockchain.info/charts/total-bitcoins.
[13] BLOCKCHAIN. *Number of Transactions Per Day*. Blockchain. [Online] 07 26, 2014. [Cited: 07 26, 2014.] https://blockchain.info/charts/n-transactions?timespan=all&show DataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.
[14] FBI: *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Directorate of Intelligence, Washington : Federal Bureau of Investigation, 2012.
[15] WIKI: Anonymity. *Bitcoin wiki*. [Online] 05 30, 2013, https://en.bitcoin.it/wiki/ Anonymity.
[16] CODERRR. *Patching the Bitcoin Client to Make it More Anonymous*. Bitcointalk Forum. [Online] 06 30, 2011, https://bitcointalk.org/index.php?topic=24784.msg 307661#msg307661.
[17] LEE, T. B: *How Private Are Bitcoin Transactions*? Forbes. [Online] 07 14, 2011. http://www.forbes.com/sites/timothylee/2011/07/14/how-private-are-bitcoin-transactions/.
[18] LOWENTHAL, T.: *Bitcoin: More Covert than it Looks*. *Active Rhetoric.* [Online] 07 14, 2011. http://activerhetoric.wordpress.com/2011/07/14/bitcoin-more-covert-than-it-looks/.
[19] BITCOIN.IT. *Selling Bitcoins. Bitcoin wiki*. [Online] 01 20, 2014. https://en.bitcoin.it/wiki/Selling_bitcoins.
[20] *Buying Bitcoins.* Bitcoin wiki. [Online] 02 19, 2014. https://en.bitcoin.it/wiki/Buying_bitcoins.
[21] *Secure Trading.* Bitcoin wiki. [Online] 10 24, 2012. https://en.bitcoin.it/wiki/Secure_Trading.
[22] FDIC: *FDIC* Law, *Regulations,* Related Acts. FDIC Federal Deposit Insurance Corporation. [Online] 09 16, 2013. [Cited: 07 28, 2014.], http://www.fdic.gov/ regulations/laws/rules/8000-1400.html#fdic8000fra1010.100.
[23] FEDERAL REGISTER: *Bank Secrecy Act Regulations: Definitions and Other Regulations Relating to Money Services. Rules and regulations.* [Online] 07 21, 2011. http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.
[24] MT.GOX TEAM: *Mt.Gox.* [Online] 02 25, 2014. https://www.mtgox.com/.
[25] MT.GOX: *Acceptance of Terms of Use.* BITSTAMP. [Online] BitStamp. [Cited: 07 28, 2014.] https://fi.bitstamp.net/terms-of-use/.
[26] POULSEN, K.: *New Malware Steals Your Bitcoin*. Wired. [Online] 06 16, 2011. http://www.wired.com/threatlevel/2011/06/bitcoin-malware/.
[27] A.N.R: *Platform for Bitcoin Trade Mt.Gox Stopped Working (in Serbian).* Pobjeda. [Online] 02 25, 2014. http://www.pobjeda.me/2014/02/25/platforma-za-trgovinu-bitcoin-valutom-mt-gox-prestala-sa-radom/#.Uw0nS_ldWYw.
[28] TAKEMOTO, Y., KNIGHT, S.: *Mt. Gox Files for Bankruptcy, hit with Lawsuit.* Reuters. [Online] Reuters, 02 28, 2014. [Cited: 07 26, 2014.], http://www.reuters.com/ article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.
[29] MTGOX: *Announcement of Commencement of Bankruptcy Proceedings. MtGox.* [Online] MtGox, 04 24, 2014. [Cited: 07 26, 2014.], https://www.mtgox.com/img/ pdf/20140424_announce_qa_en.pdf.
[30] PICK, L.: *U.S. MtGox Bankruptcy Filing Approved to Clear Way for Japan Proceedings.* Digital Currency Magnates. [Online] Digital Currency Magnates, 06 18, 2014. [Cited: 07 26, 2014.] http://dcmagnates.com/u-s-mtgox-bankruptcy-filing-approved-to-clear-way-for-japan-proceedings/.
[31] KARPELES, M.: *The Greatest Service to Exchange Bitcoin Shuts Down (in Serbian).* [interv.] Lejla Madlic : Aljazeera. 02 25, 2014.

Ladislav Hofreiter - Ladislav Maris - Ludek Lukac - Lukasz Kister - Zbigniew Grzywna *

NEW APPROACHES TO THE ANALYSIS OF THE SECURITY ENVIRONMENT AND THEIR IMPORTANCE FOR SECURITY MANAGEMENT

Examination of security environment in many security papers and studies is focused primarily on analysis of external security environment of different countries. Analyzing the current security problems led us to the realization that the security environment is characterized by a systemic arrangement in which there are systems of lower and higher order. We want to demonstrate that to ensure safety of the reference object at a lower level (e.g., small social groups, individuals) it is important to evaluate the security environment of the lower order (i.e., at sub-regional, local and sub-local level). Defining and analyzing security environment at lower levels is a prerequisite for creating effective situational prevention strategies and for improving personal safety of citizens and their property.

Keywords: *Security environment, security situation, security management.*

1. Introduction

Whole range of factors affects safety of reference objects. These factors result from the characteristics and properties of the object of protection, but also from the environment in which the object exists.

The environment is generally characterized as a set of all conditions and influences in which the reference object is located and which are able to affect or alter the terms of existence of the object. This term is also referred to nearby or distant environment that directly or indirectly affect the reference object. The environment in which there are conditions for the existence and development of reference objects, their activities, relationships and interests determined primarily by safety, we have named **security environment** [1].

Analysis and evaluation of the factors of the security environment is the starting point for assessing safety of the reference object. The aim of the assessment of the security environment is to identify those factors that have the potential to change the security situation and the conditions of existence of the reference object. The scope of the analysis of the security environment depends on the size and nature of the reference object. Different scope of the analysis is required for studying security environment of a state, a different one for studying a small business object.

In this article we want to point out to the approaches of assessment of the security environment according to the concepts of security.

2. The security environment in the concept of Security Studies

Security Studies are defined as one of the branches of the subject of international relations; in the initial period of the existence of these studies their subject was a state and ensuring the safety of the state in an international environment. The reference object is the state, security means protecting the state from external threats, and the citizens of the country are safe as much as the state itself is safe. State centrism was evident for such interpretation of Security Studies and their priority was military security.

Disappearance of bipolarity has changed the nature of the factors that directly affect safety. Instead, the risk of conflict between the superpowers or independent states aroused a new threat to the safety of conflicts originating within the state itself. Security began to be associated with economic, environmental and information factors. Priority was given to the problems of group identities and the fragmentation of the international system, religious and ethnic conflicts; international organized crime and terrorism started to emerge significantly.

* [1]Ladislav Hofreiter, [1]Ladislav Maris, [2]Ludek Lukac, [3]Lukasz Kister, [4]Zbigniew Grzywna
[1]Depatment of Security Management, University of Zilina, Slovakia
[2]Department of Security Engineering, Tomas Bata University in Zlin, Czech Republic
[3]Collegium Civitas, Warszawa, Poland
[4]Higher School of Economics and Languages, Katowice, Poland
E-mail: Ladislav.Hofreiter@fbi.uniza.sk

The contents of Security Studies, which are based on a new understanding of security according to the representatives of so called "Copenhagen School" - B. Buzan, O. Waere and J.de Wilde, [2] is not just the military dimension of security; but these studies are focused also on non-military aspects of security. They study not just wars and their state actors, but research also non-state actors and non-military sources of danger, especially such resources which cannot clearly be identified. Nevertheless, the state remains the dominant reference object. In their views the *security environment is of subjective character and is being created by the actors* [2].

Analysis of the approach of the majority of Slovak security community [e.g. 3, 4 and 5] to defining the security environment shows the following:

- Security environment is perceived mainly as an external area of state (or a coalition of countries), defined by the need and possibility of implementing its interests.
- Security environment is identified only with the area of activity of state or non-state actors in international relations.
- Focus on external security environment does not allow identifying sources of potential threats in the internal environment of the state.
- Assessment of the security environment does not reflect the full spectrum of analytical planes and security sectors.

3. The security environment in the field of protection of persons and property

Discipline of protection of persons and property began to develop in 2001 at the Faculty of Special Engineering (since 1.9.2014 Faculty of Security Engineering). The object of the study was to ensure the safety of reference objects of different nature. The paradigm used for assessing the security environment within the concept of Security Studies did not suit. In the first theoretical studies, the security environment was related to subjects of protection which were production and non-production buildings, office buildings and private buildings (houses, flats, etc.). We characterized the security environment by allocating a certain space, relatively compact, size of which was given by spatial characteristics of the reference object. Depending on the needs of the security analysis, we expanded the spectrum of factors of the security environment.

In the first definitions we mainly emphasized the social factor of the security environment, then, we expanded the spectrum of natural and technogenous factors, as the reference object is always located in an environment that has its natural, social and technogenous component which affects its safety [6]. We also accepted the influence of mutual interactions of the factors of the environment [7]. The development of views on the structure and content of the security environment from the point view of safety management was completed by adopting a definition, stating that *security environment is a part of social, natural and technogenic environment, in which at a given time and space, arises an adequate security situation due to interactions of actors of the environment and environmental factors* [8].

4. Systematic approach to security environment

Security environment of the reference object is a complicated, complex system which consists of subsystems of social, natural and technical (technological) nature and their interactions. The complexity of the security environment as a system cannot be understood only in a relation to the number of subsystems and actors, but also in the context of variety, diversity, intensity and quality of interactions between the elements and factors.

Most complex subsystem in the security environment is social, societal, and human subsystem which represents human society. Human society itself is a system consisting of several societies that may be, or actually are, racially, culturally, religiously distinct [9]. In addition, each of these companies, representing a social space, there may exist social, political, economic or occupational stratification of its members [10]. Subsystem of natural origin, also called physical environment, has developed in a process of natural evolution of the world and without influence of human interventions. This environment is characterized in particular by geographical and geomorphologic arrangement, created by nature. It also includes human-altered, transformed environment, the part of the natural environment transformed by man according to his needs to ensure conditions of his life.

Subsystem of technogenic character is formed by a set of technical and technological production systems, operations, production and non-production infrastructure, transport infrastructure system of pipelines (oil, gas, water) and so on.

Security environment of the modern world is not an environment that could be defined as a *Newtonian, deterministic* system governed by deterministic laws which have a linear character of the processes leading to equilibrium. In Newtonian, deterministic system applies that after the occurrence of the phenomenon, event or process always follows its respective predictable results. Such a system operates under rules that are known or detectable. According to these rules, it is possible to identify the condition of the system in a chronological order. Based on this approach it would be sufficient to know the initial conditions so that we can predict the status of the situation in the security environment at any time in the future [11].

Processes in the real world and its security environment do not run according to deterministic models. It does not apply what existed in the past exists in the present and this will logically continue well into the future. Not always has one and the same phenomenon or event the same result. We cannot predict a future state only as a result of some sort of agreement, rules of action, as a result of processing the current conditions and values.

Real security environment exists in space and time, has its own internal dynamics and structure of actors, agents, their conditions and their interrelations. At each point of the trajectory of its development there may occur unexpected, dramatic phenomena which may cause deviations from the expected condition or trend of development. It's because the real security environment is characterized by instability which is due to the inability to control and manage all the processes that take place in it. Also, we cannot control and manage all the factors that these processes give rise to the security environment. Although we can fairly accurately describe the initial, starting conditions in the security environment, at any time of its development there may occur unpredictable, unexpected phenomena and processes (also called strategic shocks), unintended consequences of human action or element of coincidence, which will be a source of new quality condition security environment. As an example, we can see the impact of natural disasters with great destructive effect, the effects of large epidemics on human security and entire nations. In a social setting it could be poverty, social exclusion, which provokes violent conflicts, often with destructive effects on the natural environment and technogenous subsystems.

Real security environment exists in space and time, has its own internal dynamics structure of actors, agents, their conditions and their interrelations. Respecting the systemic arrangement of the security environment we come to the conclusion that there are real links between subsystems and actors in the security environment. Through these links there is transfer (diffusion) of influences and events from one subsystem to another, the mutual influence of conditions of the subsystems thus to influence of the security situation in the security environment of the reference object.

5. New classification of the security environment

The process of analysis of the security environment is systematic, purposeful, cyclic and continuous process of acquisition, collection and processing of information on the characteristics of the environment which can be a source of security risks and threats in relation to the protected object [11, 12 and 13]. This process is linked to objective and critical analysis of the structure of the security environment, factors of the security situation and the dynamics of its development.

5.1 Structure of security environment

The structure of the security environment will always be dependent on the nature and structure of the reference object. The more complex the size and structure of the reference object, the more extensive the geographical boundaries and structure of the environment will be. For each of the reference objects, we can identify and analyze **internal** and **external** security environment.

External security environment can be considered as the *space located outside the boundaries of objects of reference in which the factors occur, the processes are taking place, which have a decisive impact on the level of safety of particular reference object* [13]. The external security environment reference objects consist of a summary of **determinants and other factors** that may affect the existence and performance of the functions of the reference objects. External security environment can also be identified as:

- **closer** in which there is an imminent interaction between the reference object and the surroundings, i.e. that they interact or may interact,
- **remote** which consists of unbounded area in which exist, or there may occur factors with a significant impact on the performance of the functions and the existence of a reference object.

Internal security environment can be considered *a space located inside the boundaries of objects of the reference objects, in which there are factors, and ongoing processes that have or may have a decisive impact on the safety of particular reference object* [14]. We will identify and evaluate internal security environment when it is required by the character of the reference object – it means in the case of wider reference objects which themselves represent a more complex structure. Internal security environment may consist of:

- a set of individual objects / elements within the boundaries of the reference object,
- a summary of internal *social, natural and technogenic factors* that may affect the elements of an object in a given area and the reference object as a whole.

In terms of study of the security management it is growing importance of *local security environment* in urban areas.

Local security environment consists of a set of physical, economic, social, political and spiritual factors that affect the existence of the conditions of existence, creating and functioning of a reference object, it means individuals and social groups in a relatively small geographic area.

Nowadays towns and villages no longer constitute the basic unit for defining the local security environment. Streets, neighborhoods, or even city quarters can represent a local security environment. It is an environment in which the greater part of the interactions of the actors (reference objects) who live in it, or carry out their activities, is taking place. In this local environment can further differentiate the locations according to form of use of the site, according to historical or architectural characteristics or by socio-economic factors.

In each of these environments we can identify [15]:

- *Crime Generators* – is a place (space, object) which produces the criminal activity in a particular area, and, possibly, is a source of criminality for the area nearby. This is the place where the criminals meet, where they can find casinos, bars,

discotheques, places with widespread prostitution, etc. In such places, the conditions exist for general criminality, criminality connected with property, drugs or violence, or from these the criminals usually come from.

- *Crime Attractor* is a locality which attracts the offenders of criminal acts. Among these places or parts of the town are the ones like a department store, railway station, bus station, wealthy town districts, or distant places with a low density of population.
- *Crime Detractor* is a locality which distracts the offenders and prevents the criminal activity. These are the parts of the places where a sufficient control of all spaces has been secured, e.g., by the use of CCTV systems, by the presence of the police patrols, of security staff or sufficient lighting of those locations.

5.2 Factors of security situation

In relationship with providing security to critical infrastructure, Šimák has created a definition stating that *„the security environment is a variable complex of external and internal conditions, factors, relationships and activities which are determined by changes in state of security and their perception, cognition and survival is expressed in the conduct of social subjects „* [16].

When designing complex and systemic characteristics of the security environment for the need safety management we based the characteristics on the definition which states that the **security environment** is a comprehensive and concentrated expression of the **security situation** in a particular space at a particular time [17].

Security situation as a quantifier of quality of security environment is in the broadest sense the result of:

- interactions of relevant social security actors (individuals, social groups, safety authorities, institutions, etc.) among themselves,
- the impact of factors of the security environment on social actors in the security environment,
- operation of the security environment factors among themselves.

We distinguish two basic **types of factors** in the security environment, capable of producing an adequate security situation:

1. **Determining, conditioning factors** that fundamentally and in a long-term condition the state and development of security of reference objects. They are relatively stable, with a little change in their dynamics. Their impact and interaction is generally predictable, their evolution can be predicted with a certain credibility. They are mainly socio-political, legal, natural, climatic and urban factors.
2. **Dynamising factors** are the driving forces that have the potential to cause significant qualitative changes in the security of objects of critical infrastructure. The incidence and impact of these factors is less predictable, they might display and act with little warning time, unexpectedly and surprisingly. Due to the nature of their substance, we can identify the factors of:

- *social nature*, such as ethnic minority, religious, ethnical or political conflicts, terrorist attacks, crime, riots and other public disorder,
- *natural origin*, particularly earthquakes, volcanic eruptions, floods, landslides, avalanches, storms, whirlwinds etc.,
- *economic nature*, such as crisis, the sudden restriction of supply of raw materials and energy carriers, etc.,
- *technogenic nature*, manifesting as accidents, explosions, fires, technical equipment, spills of dangerous substances, etc.,
- *medical nature*, for example, endemics, epidemics (explosive or contact ones), or pandemics.

The result of the action of these factors can be accelerative if they have a positive impact on the existence and functioning of the object in the environment, or retarding, if they can cause a threat to the existence of the object carrying out its functions, or even cause its destruction.

It is clear that there is a causal relationship between determining and conditioning factors. Manifestations of some of dynamising factors may be caused directly by the nature of the underlying factors; on the other hand, manifestations of dynamising factors may induce changes in the character of their underlying factors. Thus, for example, cultural and historical factors may cause certain types of social conflicts, solution of these conflicts can be reflected in changes in political and legal factors.

Legal anomie can create conditions for certain types of crime and the need to address this problem can, in turn, cause changes in the legal system to ensure protection of the interests of citizens and society.

6. Conclusions

The role of security management is to minimize, or eliminate the risks associated with citizens‘ safety and protection of their health, lives and property. Due to a security entity, which is usually a physical or legal person, there is also relevant a spatial dimension of the security environment. It is mostly sectional, local security environment. Due to its structure and structure of its factors, the security environment is variable, uncertain, complex and ambiguous, and, therefore, will always be, to a greater or lesser extent, in a state of dynamic instability.

Security environment and especially the security situation are dynamic factors. Their changes are either predictable or unpredictable. Future conditions of security environment and situations within are not clear, hard-determined, or predestined.

Future states of the system can be considered vague, and of polyvariant nature.

The practice of safety management is affected by existing *conditioning factors*. When analyzing the security environment, we accept those limits resulting from these factors. If any of the above mentioned factors can act as a factor encouraging crime, it can be eliminated by implementation of social preventive strategy or other preventive measures (e. g. political, legal, organizational etc.).

From the point of view of safety management it is more difficult to eliminate the *effect of dynamising factors* that may act suddenly, unexpectedly, spontaneously. In such cases, the effectiveness is reached via a thorough and comprehensive analysis of the security environment, the identification of all relevant dynamising factors, characteristics of their potential impacts to forecast the development of the security situation. Variant-based study and processing of possible security situation allows then to design the structure of the system of physical protection (physical protection system) and build such a system of preventive measures which allow flexible adaption to the situation. This is true not only for symptoms of negative factors of a social nature, but also for factors of natural or technogenic nature.

The goal is to reach the ability to anticipate:

- *what may happen*, what security situation may arise,
- *why this may happen*, what or who may be causing changes in the security situation,
- *what needs to be done in order to prevent it from happening*, to prevent negative developments in the security situation,
- *what to do if this has already happened*, how to react to a dangerous situation.

Finding answers to these questions is the main contents of safety management activities, fulfilling its preventive function with respect to a particular security environment, interests and needs of the subject of security.

Acknowledgement

This work has been supported by the Scientific Grant Agency of the Ministry of Education of the Slovak Republic (Projects *VEGA 1/0175/14, VEGA 1/0787/14*).

References

[1] HOFREITER, L.: *Security Management (in Slovak)*, EDIS : University of Zilina, 2002, ISBN 80-7100-953-9.

[2] BUZAN, B., WAER, O., WILD, J.: *A New Framework for Analysis (in Czech),* Brno : Centrum strategickych studii, 2005. ISBN 80-903333-6-2.

[3] DOLINEC, V.: *Factors which Influence Perception of the State Security Environment,* Bezpecnostne forum ´09, Banska Bystrica, FPVMV UMB, 2009, ISBN 978-80-8083-790-7.

[4] LASICOVA, J.: *Security. Contemporary Security Agenda (in Slovak)*, Banska Bystrica, 2006, ISBN 80-8083-352-4.

[5] LASICOVA, J., USIAK, J.: *Security as a Category (in Slovak).* Bratislava, Veda, 2012. ISBN 978-80-224-1284-1.

[6] MIKOLAJ, J.: Crisis Management in Security Environment, *Communications - Scientific Letters of the University of Zilina,* vol. 7 No. 3, pp. 49-52, 2011, ISSN 1335-4205.

[7] KORZENIOWSKI, L. F.: Securitology - the Concept of Safety, *Communications - Scientific Letters of the University of Zilina,* vol. 7, No. 3, pp. 20-23. 2025 ISSN 1335-4205.

[8] HOFREITER, L., MATIS, J.: *Key Determinants and Drivers of Current and Future Security Environment (in Slovak),* Zlin, 2009. ISBN 978-80-7318-864-1.

[9] HIRNER, A.: *Methodological Notes on the Study of Social Life (in Slovak*), Martin : Matica Slovenska, 1945.

[10] SOROKIN, P.: *Social Mobility (in Polish).* Warszawa-PAN, 2009. ISBN 978-83-7683-002-5.

[11] HOFREITER, L.: *System Approach for Examination of the Security Environment (in Slovak),* Bezpecnostne forum 2014, Belianum : Banska Bystrica, pp. 199-200, 2014. ISBN 978-80-557-0677-1.

[12] LOVECEK, T., REITSPIS, J.: *Designing and Evaluation of Systems of Protection of Objects (in Slovak)*. EDIS : University of Zilina, 2011. ISBN 978- 80-554-0457-8.

[13] HOFREITER, L. et al.: *Protection of Critical Transport Infrastructure Objects (in Slovak),* EDIS : University of Zilina, 2013. ISBN 978- 80-554-0803-3.

[14] HOFREITR, L.: Approaches to Assessing the Security Environment (in Slovak), *Crisis Management - Scientific-technical Magazine of Faculty of Special Engineering at University of Zilina,* vol. 5, No. 2, 2006, pp. 28-33. ISSN 1336-0019.

[15] FELSON, M., CLARKE, R. V.: *Opportunity Makes the Thief, Practical Theory for Crime Prevention*, London, 1998, ISBN 1-84082-159-0.

[16] SIMAK, L. et al.: *Protection of Critical Infrastructure in the Transport Sector (in Slovak),* EDIS : University of Zilina, 2012. ISBN 978-80554-0459-2.

[17] HOFREITER, L.: *Security Situation, its Components and Dynamics (Slovak),* Bezpecnostne forum : Banska Bystrica, 2011, pp. 23-29, ISBN 978-80-557-0136-3.

Stanislava Strelcova - David Rehak - David E. A. Johnson *

INFLUENCE OF CRITICAL INFRASTRUCTURE ON ENTERPRISE ECONOMIC SECURITY

This article deals with critical infrastructure and its influence on enterprise economic security. In the introduction, the sectors of critical infrastructure from the point of view of the European Union, Czech Republic and Slovak Republic are characterized. Attention is paid to individual links between the elements of critical infrastructure and the enterprise. Subsequently, enterprise economic security, fundamental factors participating in its creation, and threats disturbing it with emphasis on critical infrastructure failure are discussed. The final part of this article presents possible impacts of critical infrastructure failure on the enterprise economic security.

Keywords: *Critical infrastructure, enterprise, economic security, threats, failure.*

1. Introduction

The current society is more and more dependent on the system arrangement and services provided. One of the relevant factors of a prosperous society is also a functional infrastructure [1]. It is inevitable not only for the citizens to be satisfied but also for the activity of many enterprises. Its disruption would result in a whole range of negative impacts in all manufacturing and non-manufacturing lines of business. A certain part of this infrastructure is even of such importance that it is called critical infrastructure [2]. The impacts of its disruption or failure would be so extensive that even the existence of some companies could be threatened.

2. Critical infrastructure and its influence on enterprise activity

The critical infrastructure represents for each country a summary of strategically important elements and subjects whose disruption or destruction would have a serious impact on the interests protected by the state, i.e. security of the country, economy and basic needs of the inhabitants necessary for life [2]. While the state security and ensuring the life essentials are exclusively in the management of the state, the economic security is ensured by the state only partially. The state is responsible exclusively for the macroeconomic security while the microeconomic security is created, first of all, by the subjects themselves [3]. In the following text our attention will be aimed especially at the enterprises and their relation to the critical infrastructure.

The critical infrastructure of the EU is created by sectors which can be classified as European and national ones. The European sectors are unified for all member states and include energy (electricity, oil, gas) and transport (road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping and ports) [2]. Contrary to this, the national sectors were defined by each member state separately based on its need reflecting the current security environment (e.g. [4] and [5]). However, generally we can say that the structure of these sectors is very similar in all countries and includes especially the following sectors:

- communication and information systems (information system and networks),
- financial market (banking and insurance sector),
- emergency services (integrated emergency system, monitoring networks),
- water economy (water treatment and supplying with drinking water),
- industry (chemical, metallurgical, pharmaceutical),
- food industry (crop farming and livestock production),
- health care.

* [1]Stanislava Strelcova, [2]David Rehak, [3]David E. A. Johnson
[1]Faculty of Security Engineering, University of Zilina, Slovakia
[2]VSB - Technical University of Ostrava, Faculty of Safety Engineering, Czech Republic
[3]Missouri State University, Department of Political Science, USA
E-mail: Stanislava.Strelcova@fbi.uniza.sk

The relation of the critical infrastructure (CI) and the enterprise can be expressed through individual links which arise between them. The basic classification of these links results from their character and includes the unilateral links which represent the influence of the CI sector on the enterprise and the dependence of the enterprise on the CI sector and bilateral links consisting in the dependence of the CI sector and the enterprise.

Due to the extent of the area being solved we will concentrate on a medium-sized manufacturing industrial enterprise (e.g. a chemical factory). At the same time it is necessary to draw your attention to the fact that the enterprise can be also part of the critical infrastructure (e.g. a nuclear power plant), however, such a type of enterprise is not the subject of our article. The graphical depiction of this relation is obvious from Fig. 1.

The figure shows that some sectors of the critical infrastructure affect significantly the enterprise activities or the enterprise is dependent on them. This influence or dependence can be so fundamental in some sectors (e.g. energy, transport) that the impacts of their failure can disrupt the economic security of the enterprise.

3. Enterprise economic security

When we implement a modern approach to security, the economic aspect of maintaining the system (social, technical, environmental,...) comes to foreground in such a state where it enables fulfilling the stated functions as well as their development which results in developing a new security component – the economic security.

Zeman et al. [6] define the economic security as a state where the economy of the object whose security is to be ensured (enterprise, state, group of states, world, individual, family, etc.) is not endangered by threats which significantly reduce or could reduce its performance efficiency necessary for ensuring the defence as well as other security capacities, social reconciliation and competitiveness of the object and its individual components (especially individual companies) on the internal as well as external markets.

However, the economic security can be also viewed from another angle. Then, the economic security can be defined as security of economic subjects, processes and relations between them but, at the same time, it can be perceived as sustainability of the given processes and relations between the economic subjects

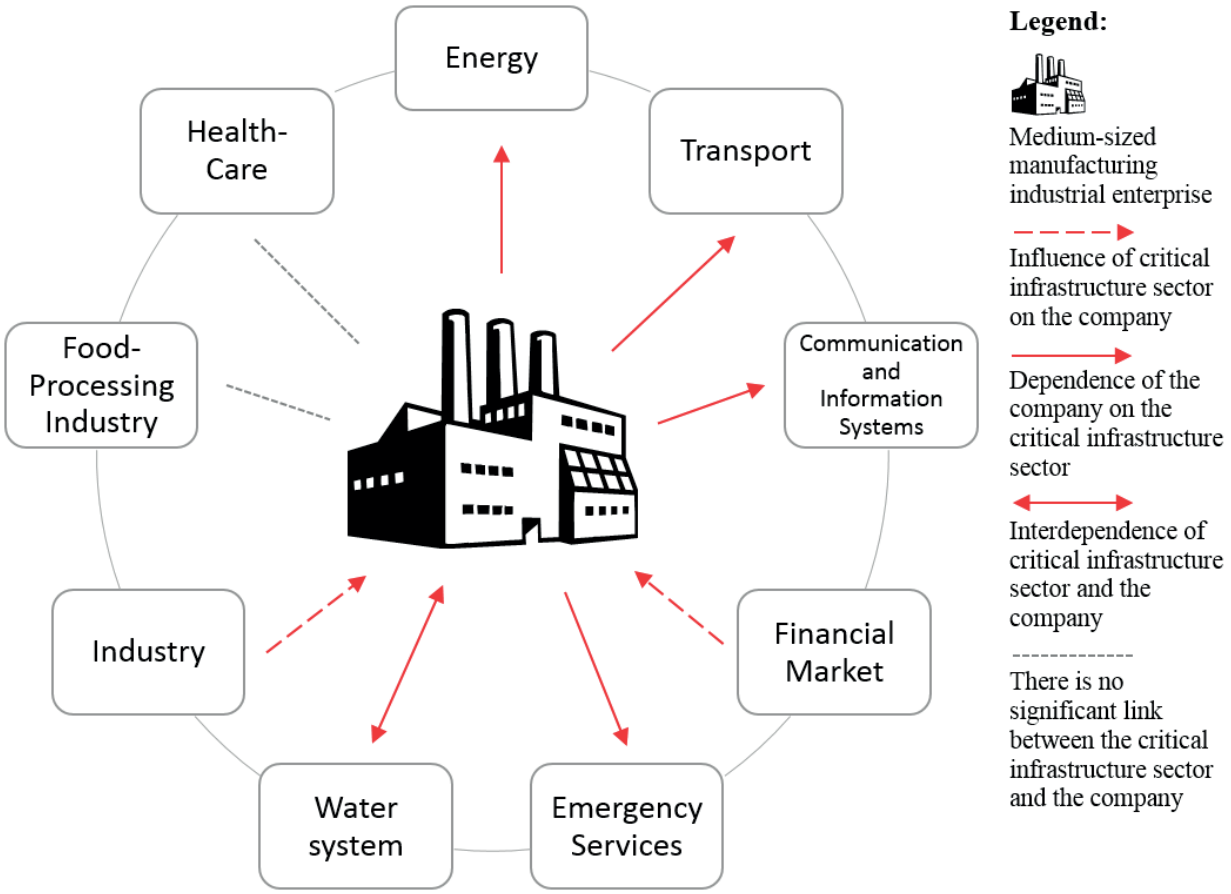


Fig. 1 Relation of the critical infrastructure sectors and the enterprise

in the sense of fulfilling the requirement of economy. However, it can be said the definitions of economic security (e.g. [7], [8] and [9] and [10]) are more oriented on protecting ourselves against effects of negative influences than detecting the economy of means which is expended.

The enterprise perceives economic security, on the one hand, from the point of view of ensuring sufficient resources for realising activities in routine as well as emergency conditions and, on the other hand, from the point of view of return of the means invested.

Not only money in cash or other financial assets are understood under the means for doing business but also other enterprise manufacturing factors (workforce, long-term tangible and intangible assets, short-term material assets) and links between them. We call them sources of economic security. They can be divided into two basic groups:

- material resources of enterprise economic security:
  - financial resources of the enterprise economic security (enterprise capital) which the enterprise gains from its own or outside financial resources and utilises it for its entrepreneurial activity [11] and [12],
  - natural resources of the enterprise economic security – buildings, manufacturing and other equipment, means of transport, estates, inventories and energy or material components of the long-term and short-term assets used in the entrepreneurial activity or ensure space for its realisation [13],
- intangible sources of the enterprise economic security – human abilities, information, technologies utilised, management system, patents, licenses, know-how but also the enterprise reputation [14].

The task of the enterprise management (in relation to maintaining the economic security) is to choose and make use of employees, manufacturing equipment, technologies and other sources in a way which will ensure the highest productivity of work [15]. At the same time it has to take into account the fact that excessive utilisation of these factors can result in failures and losses of the property, health and possibly also lives. Besides, it has to respect external conditions in which the enterprise realises its activities and take measures preventing any reduction of the enterprise performance efficiency.

4. Threats disrupting the enterprise economic security

The economic security of an enterprise is influenced by a complex of factors which affect the enterprise in the same time. These factors result in threats for the enterprise which can be classified as internal and external ones (see Fig. 2).

The internal threats result from the activity of the enterprise itself and consists of items such as an unsuitable structure of capital and assets, insolvency, inability to maintain the ownership structure, the character and development of the transformation process (production, warehousing, sale), intentional or unintentional errors caused by employees, process and management failures, shortages and errors in the area of concluding contracts, information explosion, etc. [16]. As the figure shows, these threats can be classified as process, personal and actual ones.

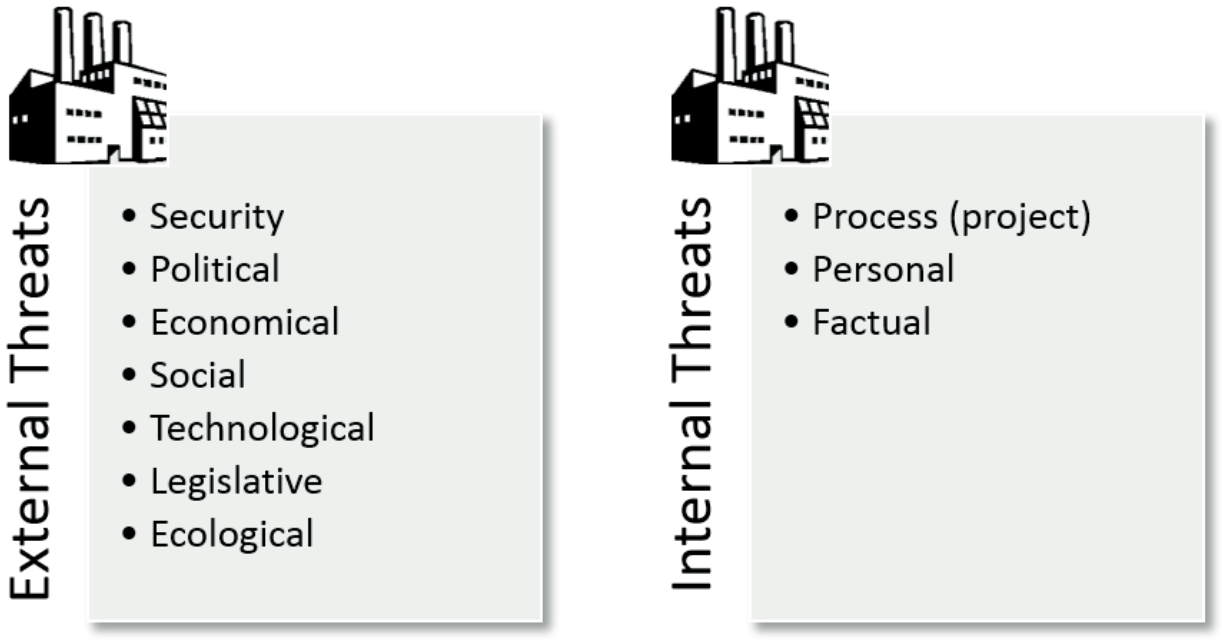


Fig. 2 Classification of threats disrupting the enterprise economic security

The external threats impact the enterprise from its surroundings. Here belong competition, disruption of confidentiality, accessibility and integrity of information, corruption, situation on the financial market, exchange rate risk, act of sabotage, espionage [17], demographic and educational structure, industrial accidents, geophysical and climatological phenomena, etc. A lot of these threats endanger the economic security of other market subjects or affect other components of the complex security model.

The failure of some critical infrastructure elements (e.g. failure of financial market, supplies of energy or communication and information systems) which can cause direct or indirect disruptions of supplying resources to the enterprise represents a significant external threat for the enterprise economic security.

5. Impacts of critical infrastructure failure on enterprise economic security

Disturbances and subsequent failures of the critical infrastructure can be connected with physical and chemical processes (corrosion, wear) but also with inappropriate management and projects [18]. Even if the disturbances are natural, more modern technologies are developed and they are more complicated and are typical in a network structure which increases the risk of a failure. Therefore, it is important for every country to possess an efficient system of effective assessment of the critical infrastructure element protection [19] and [20].

Three basic types of failures which have a negative impact on the enterprise economic security can develop in the framework of the critical infrastructure [21]. The first type is the cascade failure when a breakdown in one infrastructure is the cause of a failure of an element or subsystem in another infrastructure and this fact arouses non-functionality of such an infrastructure. E.g. Beccuti et al. [22] deals with the area of quantifying dependences between electrical and information infrastructures. The escalating failure is another type – a failure in one infrastructure deteriorates the failure parameters in another infrastructure. The last type is the join failure when two and more infrastructures have a breakdown at the same time and these failures have a similar cause (this type mostly evolves due to natural disasters).

Based on the aforementioned explanations, the impact of the critical infrastructure failures on the enterprise economic security can be classified according to their significance as follows:

- insignificant (they do not disrupt the enterprise economic security) – these impacts are early identified in the framework of the risk analysis and subsequently security measures to minimise them are taken,
- significant (they disrupt the enterprise economic security) – these impacts are also identified in the framework of the risk analysis, however, their minimisation is demanding from the point of view of time or costs,
- critical/fatal (they threaten the existence of the enterprise) – these impacts were either identified late or the enterprise has not enough means (financial, material, personnel) for their minimisation.

The nature of the critical infrastructure failure on enterprise economic security is a significant factor for determining the importance of the impacts. The nature of the impacts is characterised by four basic values which are closely connected to each other and create information about the extent of potential damages in the enterprise (see Fig. 3).

The first, and most significant, value is the area of the impact performance. The impacts affecting the sources of the economic security can negatively influence the financial resources (e.g. due to the failure of the financial market), the natural resources (e.g. due to the failure of the energy supply) or non-material resources (e.g. due to failure of the communication and information systems).

The second value characterising the nature of the impacts is the structure of their performance. From this point of view the impacts can be classified as direct, i.e. directly affecting the enterprise economic security (e.g. impacts caused by artificial devaluation of the national currency) or indirect, i.e. impacts affecting the enterprise economic security secondarily or tertiary (e.g. impacts due to power blackout).

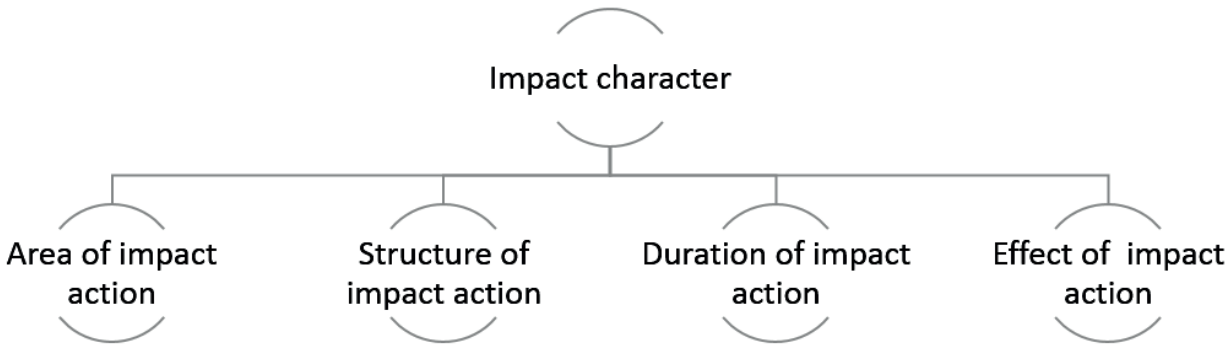


Fig. 3 Values characterising the nature of impacts of critical infrastructure failure on enterprise economic security

The third value which determines the nature of the impacts is duration. If it is only a short-term duration (e.g. power failure taking one hour) the enterprise suffers almost no losses. In the case of a medium-term duration of impact action (i.e. a few days) the losses are considerable; however, the enterprise is able to compensate them from the reserve resources. If the impacts are of a long-term character (i.e. months – the natural gas crisis in January 2009, when its impacts were visible especially in Slovakia and Bulgaria [23], can serve here as an example) the losses cumulate and even increase rapidly. In such a case the crisis scenarios are activated and the existence of the enterprise can be endangered.

The last value characterising the nature of the impacts is their effect. From this point of view the effect of the impacts can be defined as a single-way one, i.e. caused by failing one sector of the critical infrastructure or a multi-way one, i.e. caused by parallel or cascade failure of two or more sectors of the critical infrastructure (e.g. power failure, subsequently the communication and information systems fail and this results in limiting the accessibility of emergency services).

6. Conclusion

The economic security of the enterprise is permanently endangered by a whole range of external and internal threats. One of the significant external threats is represented by failing the critical infrastructure elements which can cause direct or indirect disruption of supplying the enterprise. If an extensive critical infrastructure failure develops, some companies could suffer such significant impacts that could influence their future existence. That is why it is necessary to carry out a thorough analysis of the external (but also internal) enterprise environment to ensure the enterprise economic security [24]. Subsequently, it is necessary to take a whole range of management measures using adequate methods [25] to minimise permanently the risks resulting not only from the potential failure of the critical infrastructure. Through implementing such an approach it will be possible to ensure the required level of the enterprise economic security.

Acknowledgements

This article was prepared with support of the grant project of the Slovak Research and Development Agency "Critical Infrastructure Protection in Sector Transportation" (APVV-0471-10) and grant project of the Ministry of the Interior of the Czech Republic "Security of Population – Crisis Management" (VF20112015018).

References

[1] DAIDO, K., TABATA, K.: Public Infrastructure, Production Organization, and Economic Development. *J. of Macroeconomics*, vol. 38, No. Part B, 2013, pp. 330-346, ISSN 0164-0704.

[2] Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infra-structures and the Assessment of the Need to Improve their Protection.

[3] KELISEK, A., KLUCKA, J., ONDRUSEK, M., STRELCOVA, S.: Economic Security: A Principal Component of Multilevel Security Concept in Global Economy. *Communications - Scientific Letters of the University of Zilina*, vol. 13, No. 2, 2011, pp. 44-48, ISSN 1335-4205.

[4] Act No. 45 from 8 February 2011 on Critical Infrastructure (in Slovak).

[5] Government Decree) No 432 from December 22 2010 on Criteria for Determination of the Critical Infrastructure Element (in Czech), 2010.

[6] ZEMAN, P. et al.: *Czech Safety and Security Terminology (in Czech),* 1st ed., Brno : Masaryk University, 2003, 186 p. ISBN 80-210-3037-2.

[7] BUSINESS DICTIONARY: *Economic Security* [online]. [cit. 2014-08-28] Available at: http://www.businessdictionary.com/definition/economic-security.html

[8] INTERNATIONAL COMMITTEE OF THE RED CROSS: *Ensuring Economic Security* [online]. [cit. 2014-08-28]. Available at: https://www.icrc.org/en/what-we-do/ensuring-economic-security

[9] INTERNATIONAL LABOUR ORGANIZATION: *What we Mean when we Say "Economic Security"* [online]. [cit. 2010-11-11]. Available at: http://www.ilo. org/public/english/protection/ses/download/docs/definition.pdf

[10] WELLER, C., LOGAN, A.: Measuring Middle Class Economic Security. *J. of Economic Issues*, vol. 43, No. 2, 2009, pp. 327-336, ISSN 0021-3624, DOI: 10.2753/JEI0021-3624430205

[11] VLACHYNSKY, K. et al.: *Corporate Finance (in Slovak),* Bratislava : Iura Edition, 2006, 482 p. ISBN 80-8078-029-3.

[12] IVANCHENKO, N. O.: Semantic Modelling of Technical-technological Functional Constituent of Enterprise Economic Security. *Actual Problems of Economics*, vol. 127, No. 1, 2012, pp. 276-282, ISSN 1993-6788.

[13] KUPKOVIC, M. et al.: *Business Economics (in Slovak),* Bratislava : Sprint vfra, 2003. 452 p., ISBN 80-88848-71-7.

[14] STRELCOVA, S.: *Economic Security of Enterprise (in Slovak)*, [online]. Security Revue: Inter. Magazine for Security Engineering, 2012. ISSN 1336-9717 [cit. 2014-08-28]. Available at: http://www.securityrevue.com/article/2012/10/ekonomicka-bezpecnost-podniku/.

[15] BERNANKE, B.S.: Skills, Ownership, and Economic Security. *Economists' Voice*, vol. 3, No. 2, 2006, pp. 1-6, ISSN 1553-3832.

[16] CHOD, J., ZHOU, J.: Resource Flexibility and Capital Structure. *Management Science*, vol. 60, No. 3, 2014, pp. 708-729, ISSN 0025-1909, DOI: 10.1287/mnsc.2013.1777

[17] SINHA, S.: Understanding Industrial Espionage for Greater Technological and Economic Security. *IEEE Potentials*, vol. 31, No. 3, 2012, Article No 6193307, pp. 37-41, ISSN 0278-6648, DOI: 10.1109/MPOT.2012.2187118

[18] SENOVSKY, M., SENOVSKY, P.: Critical Infrastructure Risks. *Communications - Scientific Letters of the University of Zilina*, vol. 10, No. 1, 2008, pp. 54-59, ISSN 1335-4205.

[19] HROMADA, M., LUKAS, L.: Multicriterial Evaluation of Critical Infrastructure Element Protection in Czech Republic. *Communications in Computer and Information Science*, vol. 340, No. CCIS, pp. 361-368, ISSN 1865-0929, ISBN 978-364235266-9. DOI: 10.1007/978-3-642-35267-6_48.

[20] LOVECEK, T., RISTVEJ, J., SIMAK, L.: Critical Infrastructure Protection Systems Effectiveness Evaluation. *J. of Homeland Security and Emergency Management*, 2010, Vol. 7, Iss. 1, Article 34, ISSN 1547-7355. DOI: 10.2202/1547-7355.1613 Available at: http://www.bepress.com/jhsem/vol7/iss1/34

[21] RINALDI, S. M., PEERENBOOM, J. P., KELLY, T. K.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 2001, 21(6):11-25.

[22] BECCUTI, M., CHIARADONNA, S., DI GIANDOMENICO, F., DONATELLI, S., DONDOSSOLA, G., FRANCESCHINIS, G.: Quantification of Dependencies between Electrical and Information Infrastructures. *Intern. J. of Critical Infrastructure Protection*, vol. 5, No. 1, 2012, pp. 14-27, ISSN 1874-5482, DOI: 10.1016/j.ijcip.2012.01.003

[23] Commission Staff Working Document, Accompanying Document to the Proposal for a Regulation of the European Parliament and of the Council Concerning Measures to Safeguard Security of Gas Supply and Repealing Directive 2004/67/EC, 'The January 2009 Gas Supply Disruption to the EU: An Assessment' COM(2009) 363, Brussels, SEC(2009) 977 final, 16 July 2009.

[24] REHAK, D., GRASSEOVA, M.: *The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis*, pp. 162-184, DOI: 10.4018/978-1-61350-311-9.ch007. In ALSHAWI, Mustafa, ARIF, Mohammed (eds.). Cases on E-Readiness and Information Systems Management in Organizations: Tools for Maximizing Strategic Alignment. 1st edition. Hershey, IGI Global, 2011, 318 p. ISBN 978-1-61350-311-9, DOI: 10.4018/978-1-61350-311-9

[25] GRASSEOVA, M., DUBEC, R., REHAK, D.: *Analysis of the Enterprise at the Hands of Managers: 33 Most Frequently Applied Methods of the Strategic Management (in Czech),* 1st ed., Brno : Computer Press, 2010, 325 p. ISBN 978-80-251-2621-9.

Adam Zagorecki - Jozef Ristvej - Krzysztof Klupa *

ANALYTICS FOR PROTECTING CRITICAL INFRASTRUCTURE

In this paper we review the key trends related to application of information technology and, in particular, automated data analysis to the problem of protecting critical infrastructure. We focus on technologies that use automated data collection and analyses that can be exploited for improving security provision for critical infrastructure in the future. Of our particular interest are technologies that are at relatively early stage of adaptation and in our judgement have potential to significantly affect how the security is provided in the future, the technologies that support physical aspect of security. Then we discuss analytics in context of cyber-security with applications.

Keywords: *Critical infrastructure, analytics, data mining, cyber-security.*

1. Introduction

The terrorist attacks in September 2001 have changed the perception of critical infrastructure security. These attacks were characterised not only by sophistication of planning and execution but as well the selection of targets – a diverse set of critical infrastructure buildings that included government, defence and commerce [1]. Those were followed shortly by London bombings and attack on trains in Spain, proving that complex attacks on critical infrastructure are becoming a new trend in terrorism [2].

In this paper we review the key trends related to application of information technology and, in particular, automated data analysis to the challenge of protecting critical infrastructure. We focus on technologies that use automated data collection and analyses that can be exploited for improving security provision for critical infrastructure in the future. Of our particular interest are technologies that are at relatively early stage of adaptation and in our judgement have potential to significantly change how the security is provided in the future. We mostly focus our discussion on technologies that support physical aspect of security: biometric technologies, video analytics, sensors and integration/data fusion. Then we briefly discuss the big data and analytics in the context of big data. Finally, we discuss analytics in context of cyber-security. We focus on the man-made threats to critical infrastructure. These are typically divided into two categories: physical threats and cyber threats. We want to emphasise that this division does not imply that these two categories are separate; in fact, one should expect that more sophisticated attacks in the future should combine the two domains.

2. Data for analytics and security

Data analytics [3] is the process of discovery and communication of meaningful patterns in data typically with use of data-mining techniques [4]. It has become a very prominent trend especially in business context (often referred to as business intelligence). The premise behind the analytics is that the use of (objective) data gathered on multiple aspects of the problem (data fusion) should improve understanding of the problem and provide new insights. In the context of providing security to critical infrastructure, one should be able to use data coming from various sensors, cameras and other data sources (for example: authorised users database) to improve provision of security by enhanced capability of identifying security breaches, reducing costs of providing security and supporting security personnel in their tasks [5]. Below we review key classes of technologies that, in our opinion, are becoming prominent for providing security and rely upon or explicitly use analytics.

2.1 Biometrics

The biometric technologies [6] are aimed at verifying personal identity – ensuring that only authorised personnel is able to access the area or perform tasks by measuring some physical aspect of a person. The most popular biometric techniques focus on the following aspects: finger prints, face recognition, and iris scans. All of them make use of sophisticated digital data analysis. Below we will briefly discuss all three types.

* [1]Adam Zagorecki, [2]Jozef Ristvej, [3]Krzysztof Klupa
[1]Cranfield University, Defence Academy of the United Kingdom, Senior Research Fellow, Shrivenham, United Kingdom
[2]Department of Crisis Management, University of Zilina, Slovakia,
[3]Department of Security Sciences, the General Tadeusz Kosciuszko Military Academy of Land Forces, Wroclaw, Poland
E-mail: a.zagorecki@cranfield.ac.uk

Finger prints were recognised as a useful tool of identification individuals as early as 19th century. It was recognised that this method of biometrics is relatively easy to bypass and susceptible to noise while reading, often requiring multiple scans. However, it is accepted that this technique can be successfully used as an additional security measure in order to increase security by diversifying methods.

Face recognition is considered as natural and least invasive method of biometric identification. Facial recognition systems range from software based solutions to complete close circuit TV systems. The technology relies on samples of images of an individual stored in the database against which the pictures taken by cameras are compared. In practice high-quality enrolment material is essential, with quality of the enrolment material determining the performance of the system. The face recognition systems have advantage for environments with a large number of people – public transportation to mass events. However, one should remember that this technology is relatively easy to be fooled and, therefore, not suitable for situations where high reliability is required from a biometric system.

Iris recognition is believed to be the most promising of the biometric methods. The iris patterns are believed to be unique to an individual, constant over time and not subject to changes caused by medical conditions. Scanning process is performed using a camera (visible or near-infrared light) and, therefore, is non-invasive (unlike retina scanning). In terms of accuracy it has low occurrence of false positives and extremely low of false negatives. The iris recognition systems have been fielded in some environments, however at the current stage they have not been widely accepted with some systems being withdrawn (e.g. UK Iris Recognition Immigration System). Particular challenges include requirement for good quality samples and relative ease to fool the system by presenting an image.

Fig. 1 Example of biometric technologies in practice [7]

In summary, the biometric technologies (Fig. 1 is illustrative) are considered to be immature and not sufficiently reliable to provide definitive ways of authentication in large scale and general setting. However, with time they may become more mature and they are likely to provide increased levels of authentication, especially when their accuracy and speed will be increased.

2.2 Video analytics

The sophistication and costs related to digital imagery have drastically dropped due to advancements in related technologies. In the result, modern digital imagery systems may not only record high quality images and videos, but as well allow for more and more sophisticated means of image analysis [8]. The types of image analyses vary in complexity which translates into ability of automated systems to address those problems (Fig. 2 is illustrative). We can identify four key types of analytics that relate to security-based tasks:

- Motion detection – a simple task of detection of changes in an otherwise static image. This task is extremely useful for identifying situation that may potentially require security officer's attention in order to analyse the scene.
- Object detection and classification – a task of automated interpretation of images in order to identify particular types of objects of an interest (e.g. a person or a van).
- Object recognition – for example, face recognition. A task of identifying a particular instance (e.g. person) of an object.
- Object tracking – a task of following an object on an image, or even following the object in a series of images (using views from different cameras).

Fig. 2 Illustration of video analytics [7]

Automated image analysis is a relatively new domain with first more sophisticated practical applications (such as face recognition) being fielded no more than 15 years ago. More sophisticated functionalities such as object tracking are still on relatively early stage of maturity. One of interesting problems with the image processing techniques are differences between reported performance of algorithms achieved in the laboratory setting and actual fielded applications. Similarly, it has been often reported that the performance claimed by suppliers is much higher to that achieved by fielded systems. These may be not necessarily

due to intentional actions, but due to the nature of phenomena related to algorithm evaluation and it emphasises the fact that a proper scientific approach to evaluation of such systems is necessary. From practical perspective, substantial research is needed till such systems achieve desirable performance. Another challenge with video analytics is that they require relatively large computational power due to sheer amount of data encoded in an image. Therefore, further computational performance improvements can make video analytics even more prominent for providing security in the future.

2.3 Sensing technologies

During the recent decade a revolution in development of sensing technologies has taken place. Examples of different sensors include:

- Accelerometers – which are so affordable that often they are installed 'just in case' in other electronic devices.
- Digital cameras – experiencing dramatic lowering of costs and improvements in terms of resolution.
- Transmitters/receivers - which allow for communication between sensors and the information infrastructure.
- Other sensors such as temperature, pressure, light, etc.

An example of a sensor platform is a smart phone – a typical smart phone includes all the above sensors – and typically it is not strictly required by the primary function of the device (making phone calls) but the sensors are included just because they are affordable and can provide value added to the user making the model more competitive on the market. Sensors are able to produce large volumes of data which can be used by data-mining algorithms to derive automatically new knowledge of the domain. However, a common misconception should be clarified here – the data produced by sensors do not imply the useful knowledge – this should be extracted from the data through the analytical processes that are not trivial. Therefore, the sensors should be considered as an enabling technology with analytics required for making efficient use of the data generated by sensors.

2.4 Integration

The key trend in security systems is integration [9] - security systems are becoming more integrated and it can be observed at several levels:

- Monitoring of several buildings or structures from the same location by exploiting remote sensing and telecommunication infrastructure that allows for transferring video streams. The primary benefit of such integration is lowering security costs by reducing number of personnel and facilities.
- Integration with other building systems (such as HVAC, electrical systems, etc.). The purpose of it is utilising common infrastructure and useful information about the state of the monitored infrastructure that can be used to inform security.
- Integration with business processes – for example, integration with organisational data warehouse to use up to date personnel data for the security purposes. The purpose of such integration is reduction of organisational costs and enhancing security by means of data fusion.

3. Big data

'Big data' is a term that describes a set of technologies that are related to collection, storage and analysis of large volumes of data. By its definition the big data technologies exceed capabilities of a single computer, especially in terms of storage. The key characteristics of the big data that differentiate it from traditional data warehouses that store large volumes of data are the 'four Vs':

- Volume – the quantity of data should greatly exceed storage capabilities of a single computer, which means that dedicated IT infrastructure should be in place.
- Variety – this is probably the most important criterion that distinguishes the big data from traditional data storage: the data must be multidimensional, which should guarantee that it captures complexities of the domain it relates to.
- Velocity – the data should be constantly generated and keep up with the changing environment.
- Variability – the data should reflect dynamics of the environment. This aspect is particularly important from the analytics perspective, as traditional data mining algorithms assume that the data relates to the system (or at least most aspects of it) that is constant over time.

The big data is more than just a scale-up version of traditional data warehouses. The big data carries a premise of using large volumes of multidimensional data to make predictions about the world that would not be possible otherwise. This premise is based on the fact that the sheer volume and complexity of data exceeds human abilities to analyse it, and, therefore, one should expect that the algorithms that are able to handle and exploit the big data, would be able to provide knowledge and insights that are beyond human capabilities. To validate if this premise is true requires some time and maturity of the big data solutions, however, current practical applications of the big data concept show that there is at least some merit in the big data.

The big data is becoming a trend both in commercial and government sectors. The commercial applications are mostly driven by solutions that allow customisation of provided service. Typical examples are recommender systems implemented for online shops, or more from security domain tools that allow personalised risk scoring: for example tools that use data fusion of different sources of data for credit scores.

There are challenges related to the big data – in particular the cost of implementation and the fact that there is no guarantee that

the investment in massive data infrastructure will be justified by benefits that cannot be guaranteed or even estimated at the time of investment. Currently, there is a lot of optimism and hopes related to the big data, but one will need to wait till those are verified by actual implementations.

4. Cyber-security

In the recent decades the rise of cyberspace and related threats associated with this domain has been observed and widely discussed in the literature [10]. In particular, it is the networked nature of the monitoring systems and their connectivity to the Internet that creates a bridge between providing physical security and the cyberspace. This is not intention to discuss cyber-security threats and application of analytics in this paper, however automated intrusion detection systems based on constant monitoring and automated interpretation of data are an active and very promising research field [11] (Fig. 3 is illustrative).

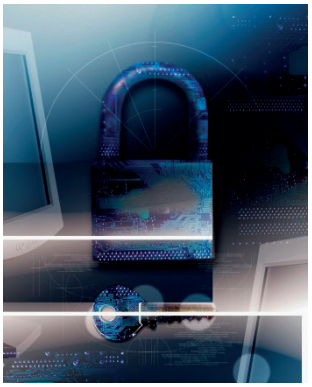


Fig. 3 Illustration of cyber-security [7]

The big data technologies are particularly relevant to cyber-security. It is because of the two aspects that characterise cyber-threats:

- The ease of collecting large volumes of data related to cyber-security – implementing data collection on IT infrastructure is relatively affordable and technically unchallenging. Large organisations are already aware of cyber-threats and a typical first response is implementation of the data collection infrastructure, often with false assumptions that the data itself will help improving security.
- The nature of cyber-threats – unlike civil unrests, bomb attacks or simple perimeter violations, cyber-threats are hidden from the eyes. The most dangerous cyber-threats may remain undetected for long periods of time and require specialised knowledge and tools to be detected. The cyber-threat detection is basically based on analyses of computer logs, process that can be naturally automated.

The most common approaches to analysis of cyber-security data can be summarised in two broad categories:

- Patterns or signature detection – this approach is based on identifying known patterns of attacks by using various kinds of pattern-matching methods. They rely on the experts identifying patterns of typical cyber-attacks and describing them in form of patterns that are later used by analytical software to match against suspected activities. The strength of this approach is simplicity and use of known facts about cyber-threats. An obvious disadvantage is their unsuitability for detecting new threats, and inability to learn.
- Anomaly detection – these methods are based on automated methods that detect unusual behaviours in the system, and flag them for interpretation by human analysts. These methods are more suitable for unknown threats, however, require input from humans.

It is likely that the development of analytical tools for cyber-security will be intensified in the future, as cyber-security is being put in the spot light by industry and governments.

5. Conclusions

In this paper we outlined the trends in analytics for the problem of providing protection for critical infrastructure, as it was highlighted in several paper before (such as: [12] and [13], [14] and [15]). The field of analytics is currently dynamically developing and in our opinion it is at a relatively immature not only for security applications but for a wide spectrum of applications in general. The trends from other domains (especially business) indicate that the data fusion and the concept of 'big data' carry a promise of revolutionary changes in analytics in general. If it is the case – it is yet to be seen. But certainly some more basic applications and concepts outlined here have a potential to substantially affect how the security for critical infrastructure will be implemented.

Cyber threats and cyber-security are emerging phenomena. Even though that the immense number of strategies, reports, white-papers and both professional and academic papers have been proposed and published, we are yet to see the development of these threats into a security daily reality.

Acknowledgements

This work was co-funded by the Slovak Research and Development Agency under the contract No. DO7RP-0025-12. And the project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No. 313308.

References

[1] EDWARDS, M.: *Critical Infrastructure Protection*, vol. 116 of NATO Science for Peace and Security Series - E: Human and Societal Dynamics, M. Edwards (ed.), IOS Press, 2014.

[2] LEWIS, T. G.: *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Wiley, May 2006, ISBN: 978-0-471-78628-3.

[3] KOHAVI, R., ROTHLEDER, N. J., SIMOUDIS, E.: Emerging Trends in Business Analytics. *Communications of the ACM*, 45 (8): 45–48, 2002.

[4] HAN, J., KAMBER, K., PEI, J.: Data Mining: *Concepts and Techniques*. Morgan Kaufmann, 2006.

[5] SHANKAR, M., RAO, N., BATSELL, S.: *Fusing Intrusion Data for Detection and Containment*, Proc. of the 2003 IEEE conference on Military communications (MILCOM'03), vol. II, 2003. IEEE Computer Society, Washington, DC, 741-746.

[6] JAIN, A. K., ROSS, A., PANKANTI, S.: *Biometrics: A Tool for Information Security.* IEEE Transactions on Information Forensics and Security, vol. 1, No. 2, June 2006, 125-143.

[7] Fotosearch, *Security Alert by Brand X Pictures*, 30.3.2008.

[8] KO, T.: *A Survey on behavior Analysis in Video Surveillance for Homeland Security Applications*, Applied Imagery Pattern Recognition Workshop, 2008. AIPR'08. 37th IEEE, pp. 1-8. IEEE, 2008.

[9] BASS, T.: Intrusion Detection Systems and Multi-sensor Data Fusion. *Communications ACM*, 43, 4, April 2000, 99-105.

[10] MILLER, R. A.: Cyber War Realities - What Lies Ahead, *Intern. J. of Critical Infrastructure Protection*, vol. 5, No. 2, July 2012, 84-85, ISSN 1874-5482.

[11] DI PIETRO, R., MANCINI, L. V.: *Intrusion Detection Systems*. Springer, 2008.

[12] HOLLA, K.: Dealing with Key Terms in Risk Analysis and Phenomenon of Uncertainty in this Process, *Communications - Scientific Letters of the University of Zilina*, vol. 9, No. 4, 2007, 59-61, ISSN 1335-4205.

[13] ZANICKA HOLLA, K., MORICOVA, V.: Human Factor Position in Rise and Demonstration of Accidents, *Communications - Scientific Letters of the University of Zilina*, vol. 13, No. 2, 49-52, 2011, ISSN 1335-4205.

[14] SIMAK, L.: Increasing the Security Level in the Slovak Republic, *Communications - Scientific Letters of the University of Zilina*, vol. 10, No. 2, 2008, 67-71.

[15] REHAK, D., SENOVSKY, P.: Preference Risk Assessment of Electric Power Critical Infrastructure, *Chemical Engineering Transactions*, vol. 36, 469-474, 2014, ISSN: 1974-9791.

Alexandria Martinelli Navratil Van Praag - Vaclav Navratil - Leos Navratil *

ISRAEL'S READINESS FOR HEALTH EMERGENCIES

Due to the geographic locations of Slovakia and the Czech Republic in Central Europe and the perceived threat of a mass terrorist act, along with the current economic climate, this article looks to determine the degree of readiness of both the Czech and Slovak Health Systems in addressing the impact of incidents in which there would be a large number of affected among population, particularly in cases where civilian contamination by any substance belonging to the group of CBRN (chemical, biological, radiological and nuclear agents) is minimal. Specifically, this article will inform readers about the readiness of State Health Services, in which the population is exposed to this risk for decades on end, and the number of victims of such attacks will be higher than ten thousand (10,000). As this model is one the State of Israel is accustomed to, all data from the Czech and Slovak Health Systems will be seen in reference to Israel's performance, and further recommendations will be made where the Czech and Slovak Health Systems are found to be lacking.

Keywords: *Emergency preparedness, crisis management, terrorism, health services, medical response, Israel.*

1. Introduction

The health sector in the Czech Republic, encounters few crisis situations [1] which involve a number of wounded or disabled individuals, therefore, leaving the majority of hospitals ill-equipped and at a disadvantage should such scenarios occur.

The major contributing factors for this are as follows:

- There is a minimal amount of theoretical training given to medical personnel, including physicians.
- The effectiveness of practical exercises carried out in health care facilities is grossly underestimated, and in some cases fully dismissed.
- A lack of material supplies, a common by-product of the current financial situation in the health sector, coupled with the State attempting to leave health facilities shouldering the costs alone, has had a crippling effect on running crisis prevention drills.
- A general malaise felt on the part of the populace when it comes to the gravity of a terrorist attack in Central Europe.
- The mainstream media contributes to the aforementioned malaise by downplaying the scope and reach of such terrorist groups like Daash (ISIS/ISIL), and Al-Shabaab, leading many to think of terrorism as an African problem, as opposed to a European or world issue.
- Czech Republic also lacks the specialized departments needed for dealing with heavy casualty scenarios.

Even in the Slovak Republic, in the health sector field of crisis management there are a number of shortcomings that may have a negative impact in the event of an actual threat to the population.

On the other side of this scale is Israel, a country whose citizens understand the threat of terrorism all too well, and whose health facilities handle mass casualties on a regular basis with maximum efficiency and professionalism.

2. Gertner Institute

Playing a vital role in this area, the Gertner Institute (Fig. 1), founded in 1991 by Professor Mordechai Shanim to promote extensive epidemiological research of key chronic diseases and to formulate a national policy for health services, has housed since 2001, the Israel National Center for Trauma & Emergency Medicine Research Center, directed by Prof. Dr. Kobi Peleg, M. D., Ph.D., MPH [2].

Serving as the official workplace of the World Health Organization from 2011, the research center is involved in many international projects aimed at the prevention of accidents, including those, of course, resulting from acts of terror.

While the main task of the organization is to lead the National Trauma Registry (a network of 17 hospitals and over 200,000 patients), the center itself has a multidisciplinary

* **Alexandria Martinelli Navratil Van Praag, Vaclav Navratil, Leos Navratil**
Department of Health Care Disciplines and Population Protection, Faculty of Biomedical Engineering, Czech Technical University (CTU) in Prague, Kladno, Czech Republic
E-mail: vaclav.navratil@fbmi.cvut.cz

Fig. 1 Gertner Institute

character working with experts from varying fields spanning from technicians, chemists, physicists, psychologists to medical response teams. All data is accessible and is regularly analyzed through the Barell Matrix to maintain high quotas of quality control where by key trends of high-risk groups can be identified allowing for the effective use of hospital equipment and procedures.

The main objectives of the center are as follows:

[a] Manage, maintain and update the National Register.
[b] Research, document and present fresh data.
[c] Use the data found in point b in order to improve the quality of health care, therapy and crisis prevention.
[d] Draw attention among the medical community and populace about the range of issues faced.

The center has an extensive network of cooperating organizations, both domestic and foreign. The activities of the Gertner Institute are significantly larger than similar facilities. It is the guarantor of the activities carried out by the Center for Disease Control and the Israel National Institute for Medical Research, Care, Policy and Services. It is responsible for monitoring any reforms or change management needed, an important aspect for the national economy and the related health of the population.

Besides the "Trauma" center there are other operators at work at the Institute including those focused on:

- The study of ionizing and non-ionizing radiation on an organism.
- Genetic and molecular epidemiology.
- Epidemiological studies of infectious diseases, focusing on the transmission of pathogens in the community and the interaction between the host and pathogen to prevent infectious diseases.
- Pharmacology.
- The epidemiology of malignant diseases.
- Epidemiology of atherosclerosis, including a healthy diet.
- Telerehabilitation or the complex methodologies used to monitor the rehabilitation of the patient through their home computer, therefore, not forcing them to leave home, providing consultations 24 hours a day, 7 days a week. Results are evaluated in real time using a computer system, which provides immediate feedback.

3. Sackler Faculty of Medicine, Tel Aviv University

The Sackler Faculty of Medicine, at Tel Aviv University is Israel's largest medical faculty. It currently has over 3,000 students involved in master studies and about 1,400 teachers and lecturers. The vast majority of teachers operate in one of the 17 teaching hospitals which provide health care for more than two million inhabitants.

The Sackler Faculty of Medicine devotes considerable attention to reforming and improving their teaching methods and the curriculum, their goal being to prepare future doctors in coping with the exponential growth of technical knowledge (one approximately doubling every 30 months). The Sackler Faculty of Medicine believes that students must acquire the habits of critical thinking based on evidence-based medicine. This modern approach in educating future physicians is interactive, based on an interdisciplinary study of individual systems to strengthen the contact between the doctor and patient known as the MPS program (Medicine - Patient - Aid Company) [3].

This faculty recently built a "Laboratory of clinical skills" which gives students the opportunity to learn clinical skills using computer simulations, sophisticated animated models and other advanced techniques.

The extensive medical research undertaken by the Faculty there is funded by a number of companies, including full cooperation with pharmaceutical companies in developing new medicines and medical technologies, thereby again allowing for many of the lessons learned in the field or due to data gathered to be quickly put into practice as shown by the 1,200 patents achieved.

4. Hospital Tel-Hashomer ha

Hospital Tel-Hashomer ha (or the Sheba Medical Center) lies on the southern outskirts of Tel Aviv and is the largest hospital in the Middle East. Founded in 1948 to serve as the first military hospital in Israel, there are several buildings still preserved from the original hospital layout (Fig. 2) which are currently used for long-term patients, lower staff accommodations and technical support.

Providing medical care for approximately 1.5 million patients, the hospital is located on 60 hectares of greenery, houses more than 1,990 beds (Fig. 3), and employs 7,500 people (1,400

doctors and 2,600 nurses), covering 25% of all examinations performed in Israel.

Fig. 2 Original hospital layout

Fig. 3 Hospital Tel-Hashomer ha

Sheba Medical Center's Department of Surgery is divided into 18 departments and has 362 beds, employing 280 doctors and 500 graduate nurses. In the Intensive Care Unit, each bed is equipped with monitoring devices, ventilators and other necessary equipment. Within the Department of Anesthesiology and the Intensive Care Unit there are two wards (15 and 16 beds) with similar instrumentation as the surgical clinic. All medical and nursing documentation is conducted strictly by computer, providing quick access to patient information.

In the event of an emergency the hospital initiates a program called extraordinary mode where normal shift operations are changed to meet a two-shift at twelve-hour schedule.

The hospital is ready at any given time to receive a considerable amount of affected causalities contaminated with toxic, biological, radiological and nuclear agents. The contamination line is located outside a large concrete area, along with cleansing showers set at different heights allowing for those standing or those that are transported via wheelchair or hospital bed to be quickly cared for (Fig. 4).

Fig. 4 Decontamination area

Those affected are brought directly to the decontamination area via ambulance or helicopter, and then are transferred to the entrance of a designated building equipped with an internal environment sealable door where a checklist is gone through as to ascertain further therapeutic procedures needed.

Additionally, the hospital is outfitted with a powerful source of backup electricity, domestic hot water tank, and tanks with potable water.

5. Rabin Hospital and Rabin Health Center

The hospital is located in the center of Petach Tikva which now fully merges into Tel-Aviv and consists of two historical institutes of health. One institute was originally named after the founder of the first Israeli blood bank, Dr. Moshe Beilinson (1889 – 1936), and the other is named after the former Israeli Prime Minister Yitzhak Rabin.

These institutes with 1,300 hospital beds, 4,500 employees, 1,000 physicians and 2,000 nurses, have housed numerous medical firsts for the Nation, including the first use of dialysis in 1968 and in 1995 the first heart transplant.

Rabin is part of the hospital department designated to receive the wounded during emergencies. The department's receiving center (Fig. 5) is equipped with a sufficient number of separate ambulances, allowing for a patient to receive varying types of care. The patient can be treated either on an outpatient basis, including infusion therapy, then transferred to home care or inpatient care in the appropriate department. As in other Israeli hospitals, extraordinary mode equates to twelve-hour shifts for the staff.

Fig. 5 Department's receiving center of Rabin Hospital

The hospital is also equipped with the latest medical technology, allowing for blood samples to be quickly sent for analysis through a special laboratory tube post.

6. Organization of Health Services

Four main health insurance companies operate in Israel, covering 29 large hospitals, 21 psychiatric hospitals and 242 after-care or geriatric hospitals (with about 18,200 beds).

The 29 large centralized hospitals (with about 14,000 beds) are used to ensure high levels of efficiency during emergency care in cases of mass disasters. In addition to large hospitals there are still a number of non-governmental health facilities owned by non-governmental organizations or endowments also accessible to the public.

The emergency services organization of Magen David Adom (MDA, literally translated to the *Red Shield of David*), was founded in 1930 and was originally run on a voluntary, non-governmental basis. The basic goal of the MDA is to provide first aid at the epicenter of a crisis, as to not to overload nearby hospitals, while also helping to identify terror victims.

There are 11 regional centers throughout the region, with more than 700 ambulances with basic amenities (Basic Life Support), indicated by blue stickers, and about 110 ambulances for full resuscitation and intensive care (Advanced Life Support) noted by red stickers. The MDA has an armored mobile intensive care unit, and their Air Rescue Service has 105 helicopters which cooperate with the Israeli Air Force when necessary [4].

All hospitals involved in crisis management decontaminate surfaces and equipment before entering patients into the interior and must be equipped with a hermetic closure with pressure system in the event of chemical and radiological emergencies. All of these medical devices must go to extraordinary mode in 15 minutes and be ready to receive the bulk of the affected from the disaster. Each hospital must have permanently available medical supplies to security emergencies and allow for a 20 percent hospital bed capacity. All hospitals, therefore, require a perfectly prepared and practiced emergency plan, with functions that shall be checked at least once a year.

The National Blood Transfusion Service also plays a vital role in Israel's emergency recovery responses, by having detailed information on each donor, and maintaining a surplus blood supply, 90 percent of which is collected by mobile units.

Finally the digital information systems used in Israeli hospitals are bidirectional and allow for information to be passed quickly from physicians to patients with ease [5].

7. Conclusion

The health system of the state of Israel is fully prepared, based on their years of experience with a high number of terrorist attacks. Their crisis management system is efficient, effective and economically sound. It has the support of both the government and the populace, and as of such, the adoption of the procedures used in Israel would surely benefit both the Czech and Slovak Republics [6] and [7].

It is therefore essential that the issue of crisis management in health care becomes a permanent part of the undergraduate and the postgraduate training for doctors, while adding in aspects of career long or lifelong learning. The situation is deemed to be much more favorable for paramedics.

The risks of emergency situations coupled with the various possibilities of prevention and protection must be repeatedly presented to the population through public media and other appropriate forms of education.

Protecting the population must become a priority of state and local governments. An apparent case of these measures being disregarded can be found when the Prime Minister of the Czech Republic, Mgr. Bohuslav Sobotka was forced to apologize for the extraordinary incompetence shown in the handing of the situation at the ammunition depot in Vrbětice, located in the Zlin region.

Acknowledgments

This work was funded by the ESF and the State budget of the Czech Republic (Project CZ.1.07/2.4.00/31.0224 "Protecting the population and the crisis solutions").

References

[1] *Protection of Population in case of Non-Military Emergency Situations and Incidents (in Czech)* - 2nd ed., editor Safr, G., Brno : Nakladatelství Tribun EU, 304 p., 2014, ISBN 978-80-263-0724-2
[2] PELEG, K: *Disaster and Emergency Medicine - A Conceptual Introduction.* Front Public Health 2013; 5(1): 44
[3] ADINI, B, PELEG, K: *On Constant Alert: Lessons to be Learned from Israel's Emergency Response to Mass-casualty Terrorism Incidents.* Health Aff (Millwood), 2013; 32(12): 2179-2185
[4] ELLIS, DY, SORENE, E: *Magen David Adom - the EMS in Israel.* Resuscitation, 2008; 76(1): 5-10
[5] DRESCHER, M. J., AHARONSON-DANIEL, L., SAVITSKY, B, LEIBMAN, J, PELEG, K.: A Study of the Workforce in Emergency Medicine in Israel: 2003. *J. Emerg. Med.*, 2007; 33(4):433-437
[6] *Protection of Population in case of Non-Military Emergency Situations and Incidents. (in Czech)*, 1st ed., editor Safr, G., Brno : Nakladatelství Tribun EU, 152 p., 2014, ISBN 978-80-263-0721-1
[7] *Concept of Protection of the Population in 2020, with Prospect to 2030* adopted by the Government of the Czech Republic on October 23rd, 2013.

Matus Pleva - Anton Cizmar *

CAR TRAJECTORY CORRECTION AND PRESENTATION USING GOOGLE MAPS

This paper describes a trajectory correction algorithm which calculates the kinetic parameters of the tracked object (car using GPS data from tracking device) and detects faulty GPS samples. Input parameters contain GPS geographical coordinates of the object and the timestamp code of capturing the position. Based on these data and physical object limits, which the operator could modify, the algorithm decides if the sample is precise or faulty. In the case of faulty sample the algorithm suggests the estimated location of the point using Kalman filter implementation and the results are presented on the map using online web interface. When the operator confirms a predicted sample, the previous predicted (not confirmed samples) are recomputed using a backward correction algorithm. The final corrected trajectory is presented using a developed specialized interactive web interface with embedded Google maps API.

Keywords: *Kalman filter, route correction, GPS, trajectory, Google maps API.*

1. Introduction

The security forces tasks involve tracking of escaping mobile objects (man, car, motorcycle, etc.) whose position is scanned from a hidden GPS device and transmitted using MANET or infrastructure wireless network [1]. The operator of the dispatching centre or the security officer with mobile terminal needs to track the position of the suspicious object on the map, using the most accurate and reliable trajectory of the tracked object. The tracking application should give him an opportunity to correct detected (by the system) defective samples (according to the mobile object parameters and the calculated actual parameters). Next improvement is that the tracking application could offer the most probable trajectory approximation according to the physical probabilities of the observed object (weight, maximal acceleration, speed, turning radius). This work was motivated by solving a task in the 7th Framework Programme project INDECT [2].

The problem of a simple route presentation on the map is that the GPS device inaccuracy is causing a wobble of the point on the screen [3]. The navigation devices are trying to put the point on the road (because they expect a decent vehicle), but the escaping car (followed by security forces) could use undocumented roads, or even sidewalks. Next approach is using so called "static GPS" which is presenting a new position only if the measured speed of the vehicle is larger than the defined limit (5 m/s), so the result is that the point on the map is "more static" [4] if it is not moving, but this is not this case. So we try to build a solution without relation to existing maps (road vector data were not used).

The application developed should be cross-platform and capable of using on wide range of mobile terminals so we decided to use web-application whose input samples are supplied from the GPS device of the tracked object with time stamp. The involved algorithms were first tested in the Matlab environment and then reprogrammed in PHP and JavaScript to be able to run independently from the operating system and without additional claims on operator's mobile terminal software [5].

This paper describes the final solution of interactive tracked object trajectory presentation. This solution gives the operator an opportunity to approve automatically corrected positions (automatically detected defective samples filtered using Kalman filters), define the parameters of the tracked object, everything in real-time using a web-service, GPS locator and online maps or from recorded position database.

The paper is organized as follows: firstly, the Kalman filter algorithm is presented, the detection of defective sample conditions are described and then, the principle of retroactive correction is explained. Next, the pilot trial GPS tracking data samples collection is presented, and finally the web-service

* **Matus Pleva, Anton Cizmar**
Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics,
Technical University of Kosice, Slovakia
E-mail: Matus.Pleva@tuke.sk

trajectory presentation Google maps API based solution is described.

2. Kalman filter and object trajectory correction

In 1960, R. E. Kalman presented the recursive algorithm for linear discrete data filtering [6]. Since then, the Kalman filter is the subject of extensive research and applications, particularly in the area of self or assisted navigation [7]. This publication and the main conclusions, which are presented, were used to develop algorithms to predict the location of the tracked object.

Equations of predictions (updates in time) for the discrete Kalman filter are as follows (*A* - state transition model, *B* - control-input model applied to the control vector *u, R-Q* noise):

$$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \tag{1}$$

$$P_k^- = AP_{k-1}A^T + Q \tag{2}$$

where P_k^- is *a priori* error covariance matrix, P_{k-1} *a posteriori* error covariance matrix from previous state.

And for the correction (updates from new measured samples from mobile object) the following equations are used:

$$K_k = P_k^- H^T \left(HP_k^- H^T + R\right)^{-1} \tag{3}$$

$$\hat{x}_k = \hat{x}_k^- + K\left(z_k - H\hat{x}_k^-\right) \tag{4}$$

$$P_k = \left(I - K_k H\right)P_k^- \tag{5}$$

which implies that Kalman gain K_k for the correction should be calculated first, then the *a posteriori* estimation $\hat{x}_k$ is computed. The final step is to obtain *a posteriori* covariance matrix P_k. Every time *a posteriori* correction is used as input from previous prediction for the current prediction of a new *a priori* prediction. The recursive principle is one of the main characteristics of the Kalman filter [8] and [9] and this algorithm is used for the trajectory correction described below.

3. Defective samples detection & backward correction

Detection of the defective sample is based on knowledge of the physical properties of the observed object which can be summarized as follows [10]:

a) *maximum speed* - current speed is calculated as the distance of the last measured points divided by time between samples (or the average speed is calculated from the last 5 samples taken at short intervals, thereby reducing inaccuracy),

b) *maximum acceleration* - change in velocity divided by time between samples for which the speed was calculated,

c) *maximum change in direction at a given speed* – here, it is important to note that for low speed the object is limited by its maneuverability, and from calculated marginal speed (depends on weight – momentum) the object is limited by centrifugal force.

An important feature of the system is the backward correction. In principle, the correction is made using newly adopted correct samples after the detection of defective input data described below.

In Figure 1 the empty circles are properly measured and algorithm assessed as realistic position of the object. In point 3 defective samples are detected and the inaccurate data are removed using the predictor (algorithm) which predicts values for samples 4, 5 on the basis of the last samples (3, 2, 1, further previous samples). This prediction is shown in the picture for the sake of the clarity of the image. After the algorithm gets the correct value of another point confirmed by operator (point 6), it makes backward correction for the points 4 and 5 as follows [5]:

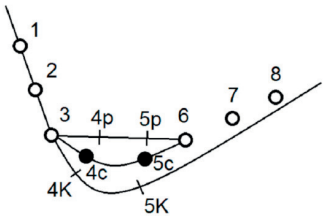


Fig. 1 Backward correction algorithm

1) Recent correct samples (sample 6 was confirmed by the operator as correct using web-application) - points 3 and 6 are connected using a straight line and plotted points on it have been predicted (in this case points 4p, 5p) the distance between points 3 - 4p - 5p - 6 are the same.
2) Next, using the Kalman filter, the coefficients of the filter in point 3 (which are characteristics of object movement in point 3) and using points 4p and 5p, the prediction is performed and subsequent correction of the points thus resulting in 4K and 5K. In this step it uses the object properties in point 3.
3) In the final step of the backward correction the algorithm connects the point 4K with the 4p and 5p with 5K using a straight line, and in the middle the points 4c and 5c are defined (presented on the web-application output - screen), as a result of backward correction (see Matlab simulation example in Fig. 2) [5].

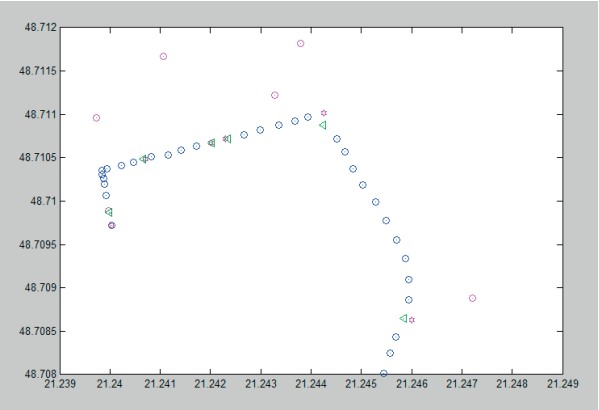


Fig. 2 Corrected (defective samples are magenta circles, magenta stars are Kalman predicted samples before backward correction) trajectory (blue and green) from Matlab

4. Trajectory measurements

Realistic trajectories were measured using a specialized GPS device GPSMAP 60CSx (Fig. 3) - navigation device that is equipped with a sensitive GPS module. Using this device a set of measure actions were taken saving a trajectory of the buses in public transport of city Kosice to the internal flash card and data was copied to the server for simulation purposes. There were 4 trajectory measurements done as you can see in the table depicted in Fig. 4.

In the final solution the system is able to replay the recorded trajectory, or tracking the observed object in the real time as the data will arrive using a wireless network communication infrastructure developed in another project [11].

The device allows recording the route travelled and storing it in GPX format (location and time stamp for each reading sample). This allows simulation of actual conditions when using the proposed system [12].

We choose a time interval 5s for recording the travelled tracks. This is the time interval that is also used to update the position on the web interface.

Fig. 3 GPSmap 60CSx device

5. Developed web interface for tracked object position presentation based on Google maps API

The web interface was developed respecting the multiplatform usage of the presentation module for mobile devices of the operators in the field. After Matlab simulations of all developed algorithms, the equations were rewritten to PHP scripts which could do the calculations on the server side, with minimal requirements on the mobile device hardware.

The design and deployment of the solution is using web application, calculations are done on the server side using PHP scripts and the interaction with the operator and GUI (Graphical User Interface) is performed using JavaScript language. The map resources were solved using evaluation license for Google maps [13] and their application programming (API) interface with registered API key [14].

In Fig. 4 you can see the web interface of the monitored objects location where the operator has a large number of options:

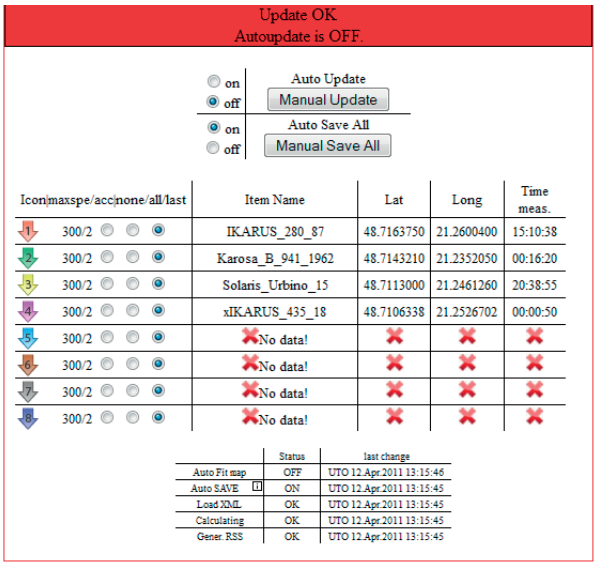


Fig. 4 Options of the web interface on the left side of the screen

1. Set how many points will be displayed on the map (“none/all/last 5” – choose a bullet).
2. Determine the maximum speed and acceleration of the object (“max spe” / “max acc”) or set it using JavaScript input field by clicking on the displayed numbers.
3. Can allow automatic updating of the map when a new sample arrived or slide display trajectory manually (“auto” / “manual update”).
4. Can save the corrected trajectory in a defined format (small icon in the upper right corner of “AutoSave” in the table in Fig. 4).
5. Replay the saved trajectory from external/internal XML file (not visible in Fig. 4).

6. Set auto zoom the map so that the entire visible trajectory of all objects displayed (depending on configuration in 1) should be visible.
7. Creating a RSS channel (link to it – "Link to RSS" in Fig. 5) with corrected samples (detected as defective and the operator confirmed the correction).

The operator can also see a description of the observed objects, their location on the map (using the proposed new icons – designed in our laboratory), the last time the samples were obtained when the last time the calculation of corrections using the Kalman filter was performed, etc.

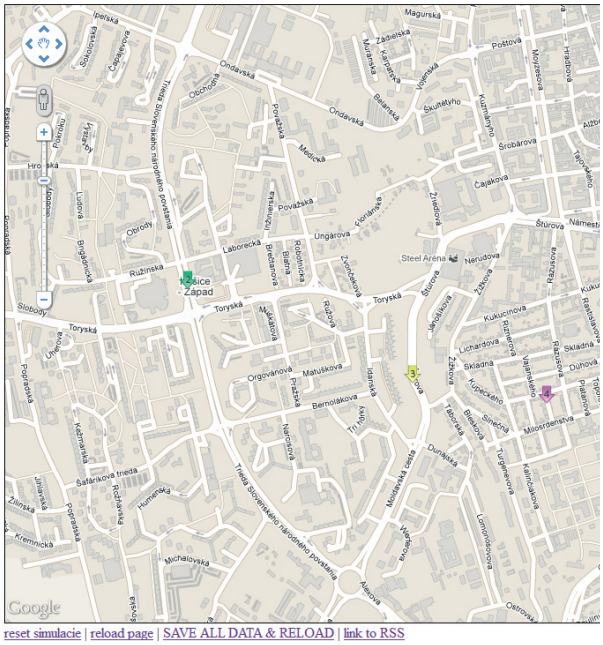


Fig. 5 The map of the web interface on the right side of the screen, please note the green/yellow/purple icons of the observed objects

The map in Fig. 5 is developed using official Google maps API for educational purposes [14]. Below the map also a possibility to restart the simulation from loaded XML file is depicted ("reset simulacie").

6. Conclusion

In our system the trajectory correction of mobile objects (GPS tracked and coordinates transferred to the server in real-time) and final trajectory presentation using Google maps API have been implemented. The system allows the deployment on the server that receives data from location sensors of monitored objects, provides a multi-user interface with easy object tracking (thanks to unified interface), detection of the faulty samples, proposal of a predicted sample, correction of the faulty sample confirmation by the operator and subsequent backward correction of the trajectory (of the detected faulty samples). The resulting trajectory can be archived and played back (from the XML file). This system represents an important contribution to the presentation of position in real applications and is suitable also for modern mobile devices (tablets, smartphones, etc.).

We plan to increase the security of the transferred data in WLAN [15] and mobile ad-hoc networks environment [16] using recently developed algorithms to ensure the privacy of the transferred data for security forces applications. Recently, also work on integration of the acoustic event detection module [17] for indicating gunshots or explosions on the map and a speech interface [18 and 19] has started.

Acknowledgement

The research presented in this paper was supported by Research & Development Operational Program funded by the ERDF (ITMS project code 26220220155) 80% and by 7th Framework Programme EU ICT project INDECT (FP7 - 218086) 20%.

References

[1] PAPAJ, J.: *Integration Process of Security as QoS Parameter via Security Service Vector in MANET,* Proc. of SCYR 2008, Kosice: FEI TU, pp. 108-111, 2008.
[2] http://www.indect-project.eu/ - INDECT 7th framework project website.
[3] ORELLANA, D., WACHOWICZ, M.: Exploring Patterns of Movement Suspension in Pedestrian Mobility*, Geographical Analysis,* vol. 43 (3), pp. 241-260, 2011.
[4] BERBER, M., USTUN, A., YETKIN, M.: Comparison of Accuracy of GPS Techniques, *Measurement: J. of the Intern. Measurement Confederation,* vol. 45 (7), pp. 1742-1746, 2012.
[5] MILCAK, K.: *Design and Implementation of the Location Presentation Module Based on GIS Data, and the Algorithms for Predicting the Position of Tracked Objects (in Slovak)*, Diploma Thesis, KEMT FEI : TU Kosice, p. 81, 2011.

[6] KALMAN, R. E.: A New Approach to Linear Filtering and Prediction Problems, Transaction of the ASME, *J. of Basic Engineering,* vol. 82 (Series D), pp. 35-45, 1960.

[7] WEISS, H., MOORE, J. B.: *Improved Extended Kalman Filter Design for Passive Tracking,* National Conference Publication - Institution of Engineers. Australia, vol. 79(4), pp. 54-58, 1979.

[8] WELCH, G., BISHOP, G.: *An Introduction to the Kalman Filter*, University of North Carolina at Chapel Hill, Department of Computer Science, Chapel Hill, NC, TR95-041, <http://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf>

[9] GADE, K.: *Introduction to Inertial Navigation and Kalman Filtering*, Proc. of High Precision Navigation and Positioning Conference. Norwegian Defence Research Establishment, June, 2008, <http://www.navlab.net/Publications/Introduction_to_Inertial_Navigation_and_Kalman_Filtering.pdf.>

[10] GECI, T.: *Design and Experimental Verification of Portable Measuring Instruments Software for In-site Conditions (in Slovak),* PhD Thesis, Slovak University of Agriculture: Nitra, 2009.

[11] CIPOV, V., DOBOS, L., PAPAJ, J.: Cooperative Trilateration-based Positioning Algorithm for WLAN Nodes Using Round Trip Time Estimation, *J. of Electrical and Electronics Engineering,* vol. 4, No. 1, ISSN: 1844-6035, pp. 29-34, 2011.

[12] DUHA, J., DADO, M., JARINA, R.: Communication Technologies and Services, *Communications - Scientific Letters of the University of Zilina,* vol. 5, No. 3, pp. 33-35, 2003.

[13] CHOW, T. E.: The Potential of Maps APIs for Internet GIS Applications, *Transactions in GIS,* vol. 12, No. 2, pp. 179-191, 2008.

[14] https://developers.google.com/maps/?csw=1 - Google Maps API website.

[15] KREKAN, J., PLEVA, M., DOBOS, L.: Security Audit of WLAN Networks Using Statistical Models of Specified Language Group*, J. of Electrical and Electronics Engineering*, vol. 6, No. 1, ISSN 1844-6035, pp. 47-50, 2013.

[16] PAPAJ, J.: *Modification of DSR to Implement SSV to the Mobile ad-hoc Network,* Proc. of SCYR 2009, Kosice : FEI TU, pp. 221-223, 2009.

[17] VOZARIKOVA, E. et al.: Surveillance System Based on the Acoustic Events Detection*, J. of Electrical and Electronics Engineering,* vol. 4, No. 1, ISSN 1844-6035, pp. 255-258, 2011.

[18] JUHAR, J., STAS, J., HLADEK, D.: *Recent Progress in Development of Language Model for Slovak Large Vocabulary Continuous Speech Recognition*. New Technologies-Trends, Innovations and Research, Rijeka: InTech, ISBN: 978-953-51-0480-3, pp. 261-276, 2012. http://www.intechopen.com/books/new-technologies-trends-innovations-and-research/recent-progress-in-development-of-language-model-for-slovak-lvcsr, Prof. Constantin Volosencu (Ed.), DOI: 10.5772/32623.

[19] VISZLAY, P., LOJKA, M., JUHAR, J.: *Class-Dependent Two-Dimensional Linear Discriminant Analysis Using Two-Pass Recognition Strategy.* Proc. of EUSIPCO 2014, Lisbon, IEEE, p. 4, 2014.

COMMUNICATIONS – Scientific Letters of the University of Zilina
Writer's Guidelines

1. Submitted papers must be unpublished and must not be currently under review for any other publication.
2. Submitted manuscripts should not exceed 8 pages including figures and graphs (in Microsoft WORD – format A4, Times Roman size 12, page margins 2.5 cm).
3. Manuscripts written in good English must include abstract and keywords also written in English. The abstract should not exceed 10 lines.
4. Submission should be sent: By e-mail – as an attachment – to one of the following addresses: komunikacie@uniza.sk or holesa@uniza.sk (or on CD to the following address: Zilinska univerzita, OVaV – Komunikacie, Univerzitna 1, SK-10 26 Zilina, Slovakia).
5. Uncommon abbreviations must be defined the first time they are used in the text.
6. Figures, graphs and diagrams, if not processed in Microsoft WORD, must be sent in electronic form (as JPG, GIF, TIF, TTF or BMP files) or drawn in high contrast on white paper. Photographs for publication must be either contrastive or on a slide.
7. The numbered reference citation within text should be enclosed in square brackets. The reference list should appear at the end of the article (in compliance with ISO 690).
8. The numbered references (in square brackets), figures, tables and graphs must be also included in text – in numerical order.
9. The author's exact mailing address, full names, E-mail address, telephone or fax number, the name and address of the organization and workplace (also written in English) must be enclosed.
10. The editorial board will assess the submitted paper in its following session. If the manuscript is accepted for publication, it will be sent to peer review and language correction. After reviewing and incorporating the editor's comments, the final draft (before printing) will be sent to authors for final review and minor adjustments
11. Submission deadlines are: September 30, December 31, March 31 and June 30.

COMMUNICATIONS

SCIENTIFIC LETTERS OF THE UNIVERSITY OF ZILINA
VOLUME 17

Address of the editorial office:
Zilinská univerzita
Office for Science and Research
(OVaV)
Univerzitna 1
SK 010 26 Zilina
Slovakia

E-mail: komunikacie@uniza.sk

Each paper was reviewed by two reviewers.

Journal is excerpted in Compendex and Scopus.

It is published by the University of Zilina in
EDIS – Publishing Institution of Zilina University
Registered No: EV 3672/09
ISSN 1335-4205

Published quarterly

Single issues of the journal can be found on:
http://www.uniza.sk/komunikacie

ICO 00397 563
February 2015