BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Machinability analysis of carbon fibre-reinforced plastics (CFRP) using compression tools

Balázs SOMOSKŐI, Norbert GEIER
Budapest University of Technology and Economics, Department of Manufacturing Science and Engineering
Műegyetem rkp. 3., 1111 Budapest, Hungary
somibali@gmail.com, geier@manuf.bme.hu

***Abstract* — The widely spread use of polymer composites and their difficult machining behaviour have directly led to the appearance of tools with unique geometry, specialised for carbon fibre-reinforced plastics (CFRP). These so called compression tools are crafted in a way to reduce delamination, which is a common machining caused material defect. The present study focuses on the effect of technological factors on various optimization parameters in cases compression tools were used. Cutting width and feed rate have been chosen as factors. The factor levels have been determined beforehand, using central composite inscribed (CCI) design. The machining experiments were carried out on a Kondia B640 milling machine centre. A KISTLER 9257BA load cell was used for the measurement of the cutting force, likewise a Mahr Federal Pocket Surf IV instrument for surface roughness. Collected data were processed using analysis of variance (ANOVA) and response surface methodology (RSM) via Minitab 17. As a result of this research the change of tool-geometry and process parameters of CFRP machining were determined, induced by technological parameters, on two various compression tools. It was found that the feed rate has the most significant effect on the cutting force and surface roughness, followed by the cutting width.**

***Keywords* —** CFRP; milling; compression tool; multitooth tool; cutting force; surface roughness

1 INTRODUCTION

Lately widespread of carbon fibre-reinforced plastics (CFRP) was caused by it's outstandingly high specific strength and specific modulus [1], [2]. Nowadays, composites are widely used in military-, automotive- and aviationindustry. Aircraft constructions such as a Boeing 787 consist composites up to 50% by weight and 70% by volume [3]. Manufacturers aim to mold CFRP parts, to match their final size and shape. Moreover they use force bounded and glued joinings [4], [5]. However machining of these components is inevitable to meet required tolerances, and in some cases the final desired shape [6]. There have been preliminary studies on the milling of CFRP in order to optimize milling parameters. Geier et al. [7] have determined that the feed rate is the most significant parameter when it comes to cutting force. They also stated that the increase of feed rate results int the growth of cutting force. Wang et al. [8] have also verified this statement, and also concluded, that the next most determinative factor during face milling is the cutting width. In their paper they stated that parameter's raise also causes the increase of cutting force. One of the most systematic studies on surface roughness optimalization was conducted by Khairusshima et al. [9]. In their analysis they found that the most important factor in this aspect of research is the feed rate. Furthermore, at a constant feed rate surface roughness is the lowest, when the lowest cutting width is applied. Although all these previous studies, CFRP specific tools have been rarely reseached.

1.1 Compression tools

Compression tools (in some papers also called multitooth tools) are crafted specifically for the milling of CFRP. These tools are fabricated with a geometry, which directs passiv force components towards the center of the layers, thus pressing them together. This mechanism is favorable to avoid delamination (separation of layers in the composite material). Tool manufacturers reach this effect for instance with the formation of a double opposed helix along the tool's cyclinder surface, represented on Fig. 1.

Fig. 1 a.) Fraisa 20340.450 and b.) Fraisa 20360.450 compression end mills

In a previous study Lacalle et al. [10] researched these tool's wear, and wear dependent efficiency. Despite this interest, the investigation of optimized machining parameters for these special tools is still neglected.

The main objective of the present study was to reach a deeper understanding on how basic machining factors (tool and cutting width) influence the optimization parameters (cutting force and surface roughness), in cases where compression end mills were applied.

2 EXPERIMENTAL SETUP AND CUTTING CONDITIONS

2.1 Environment

The machining experiments were carried out on a Kondia B640 milling machine centre. A KISTLER 9257BA type load cell was used for the measurement of the cutting force, likewise a Mahr Federal Pocket Surf IV instrument for surface roughness. A Fraisa 20340.450 (referred as coarse tool) and a Fraisa 20360.450 (referred az medium tool) compression end mills (Fig. 3) were used with climb milling technology.

The examined UD-CFRP block was fixed with two clamps as can be seen in Fig. 2. Two microscopes were placed in the workspace for the detection of tool wear.

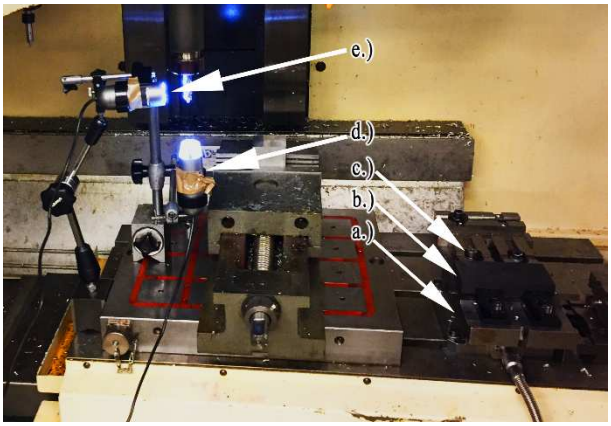


Fig. 2 Experimental setup. a) UD-CFRP specimen; b) fixture c) KISTLER load cell d.), e.) digital microscopes

Milling experiments were designed using central composite inscribed (CCI) design. Cutting with and feed rate were chosen as factors in order to analyse their influence on the optimisation parameters: cutting force and surface roughness. Other process parameters, such as revolutions per minute (n= 3185 1/min), milling style (down milling) and depth of cut (a_p=18 mm), as well as extreme values for the CCI design were fixed based on previous works [11], [12] and suggestions of tool manufacturers.

During the experiments, workpiece was face milled The edges of the cutting tool are captured in original state, to be used later as a control picture. The three dimensionas cutting force data were collected at 8000 Hz frequency. During the machining the abrasive chips were vacuumed. After the machining, images of the machined surface were taken by a Dino-lite AD7013MZT digital microscope. Thereafter the surface roughness was measured perpendicularly to the toolpath five times along the cut. In the meantime photos of the tool were taken for subsequent comparison.

3 Results and Discussion

Thirteen experiments were carried out for each tool. The randomised experiment design tables were calculated with MiniTab 17. The results for each experiment are shown in Table 1 and Table 2

Using response surface methodology (RSM), a quadratic polinomial model on data was developed. The second-degree formula was used in this study is expressed by Eq.(1).

$$y = b_0 + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{n} b_{ii} x_{ii}^2 + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} b_{ij} x_i x_j + \delta \quad (1)$$

,where y is the optimisation parameter, b marks constant multipliers, x marks the factors, and n is the number of factors, while δ is the error-factor.

3.1 Cutting force

The cutting force data were interfered with distortion such as machine noise from the milling centre. The data has been low-pass filetered with discrete Fourier transfomation (DFT). The signals which belong to higher frequency domains has been removed. The results shown in Table 1 and Table 2 are the maximum force values given by the filtered data set. The resultant maximum force is calculeted as expressed by Eq.(2).

$$F_{momentary} = \max_{j:1\in n} \left\{ \sqrt{F_{x,j}^2 + F_{y,j}^2 + F_{z,j}^2} \right\} \quad (2)$$

, where $F_{momentary}$ (N) is the momentary cutting force, F_x (N) is the radial, F_y (N) is the feed-directional and F_z (N) is the axial (passiv) component of the cutting force. As can be seen on the Fig. 4, on both tool's main effect diagrams, the feed rate has the most significant effect on the cutting force, followed by the cutting width. Furthermore, both factor increases the cutting force.

Analysis of variance (ANOVA) and interaction plots confirm that the two analysed factors have no considerable interraction terms. The response surfaces for the tools are shown in the Fig. 3. Both the increase of feed rate and cutting width results in rise of the cutting force. It can be seen that in each case, the maximum cutting force is awaked at maximum factor levels (v_f=1200 mm/min and a_e= 5 mm).

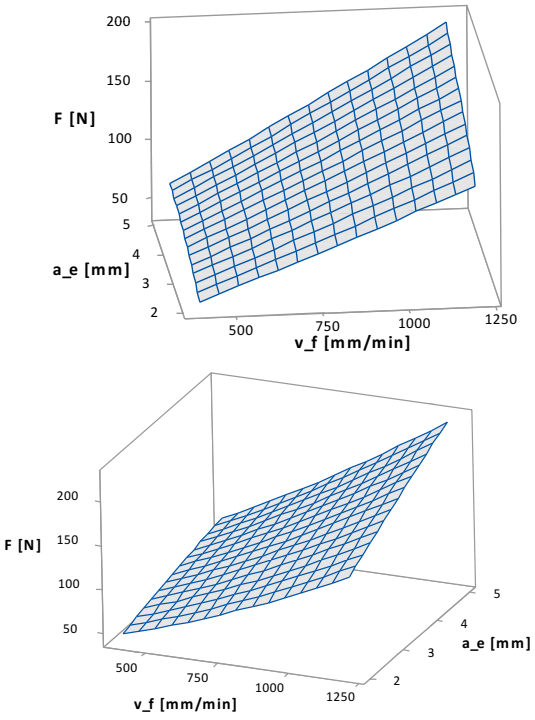


Fig. 3 Response surfaces of cutting force for tools 20340.450 and 20360.450, respectively.

Table 1 Experimental setting for the Fraisa 20340.450 tool, with parameters generadted by CCI design, and avareged *Ra* values, and the resultant *F* force

Nr.	Factors		Results				
	v_f (mm/min)	a_e (mm)	Ra (µm)	F_x (N)	F_y (N)	F_z (N)	F (N)
1	800	3.50	2.56	68.28	74.44	37.03	106.89
2	517	4.56	2.94	60.71	42.69	30.80	79.47
3	800	2.00	3.21	46.28	62.90	28.66	83.14
4	800	5.00	3.19	100.62	70.54	50.37	131.52
5	1083	4.56	2.67	120.53	98.34	65.27	166.09
6	400	3.50	1.73	43.34	33.75	21.73	57.58
7	1200	3.50	2.59	103.57	118.47	58.50	166.53
8	800	3.50	2.45	72.80	74.55	40.09	110.96
9	1083	2.44	2.81	72.00	97.25	44.94	126.88
10	800	3.50	2.39	76.34	76.31	43.24	112.87
11	800	3.50	2.37	72.87	74.15	38.67	109.77
12	517	2.44	2.40	39.76	40.63	20.38	59.38
13	800	3.50	3.06	73.52	73.77	38.08	109.05

Table 2 Experimental setting for the Fraisa 20360.450 tool, with parameters generadted by CCI design, and avareged *Ra* values, and the resultant *F* force

Nr.	Factors		Results				
	v_f (mm/min)	a_e (mm)	Ra (µm)	F_x (N)	F_y (N)	F_z (N)	F (N)
1	400	3.50	2.04	45.15	39.18	25.55	63.60
2	800	2.00	1.44	47.56	66.36	36.93	88.94
3	517	4.56	2.32	72.66	44.70	37.39	92.65
4	800	3.50	2.25	76.91	75.38	48.05	116.16
5	517	2.44	2.27	43.63	43.32	26.79	66.42
6	800	5.00	2.37	117.60	67.04	62.90	147.09
7	800	3.50	1.76	81.73	74.92	52.70	121.11
8	800	3.50	1.68	82.27	75.69	53.41	121.89
9	800	3.50	1.85	83.30	74.98	54.89	122.91
10	1083	2.44	2.38	84.54	99.07	61.18	141.52
11	1200	3.50	1.70	127.71	118.08	85.62	188.29
12	1083	4.56	1.73	140.59	101.59	85.51	190.25
13	800	3.50	1.80	83.25	75.18	52.06	121.73

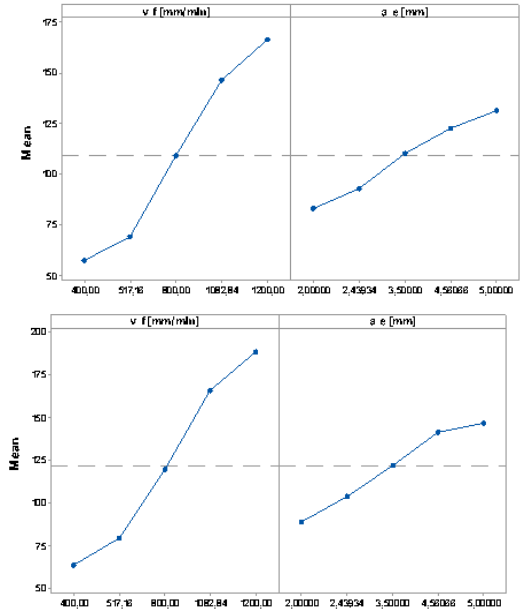


Fig. 4 Main effenct diagrams of cutting force for tools 20340.450 and 20360.450, as is

The developed models are shown by Eq. (3) and (4). According the models and the response surfaces, the compression end mill with coarse tooth is affected by up to 20% smaller force. The possible reason if this is, that the sufficient energy for starting chip splitting is higher than the amuont of energy needed for maintaining a cut. The tool with fewer edges starts new chips more often, in other words transmit more energy towars the workpiece, hence generates greater forces.

$$F = -20.8 + 0.0677v_f + 13.02a_e + 0.000008{v_f}^2 - 1.531{a_e}^2 + 0.01593v_f a_e \quad (3)$$

$$F = -5.8 + 0.0332v_f + 10.93a_e + 0.000035{v_f}^2 - 1.057{a_e}^2 + 0.01875v_f a_e \quad (4)$$

Moreover, F_z values are considerably lower than the other two components of the cutting force. It caused by the tool geometry in purpose. In this direction, the generated force on the neighbouring edges are opposed, as shown on the Fig. 5, thus resulting a smaller resultant force.

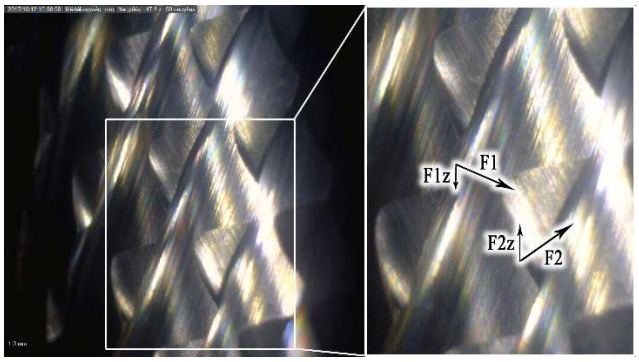


Fig. 5 Vector sum for z directional local cutting forces

3.2 Surface roughness

The surface roughness was measured five times along the surface, perpendicularly the toolpath, then average surface roughness (*Ra*), roughness depth (*Rz*) and their propotion (*Rz/Ra*) were calculated. The colleted data was filtered for deviant values. the examined values were obtained based on the the avarage of the five points. The response surfaces can be seen in the Fig. 6. It can be observed from the main effect diagrams, shown on the Fig. 7, that both factors have significant impact on the measured *Ra* values. Although, for the coarse tool the data is inconsistent. This was most likely caused by the amuont of uncut fibres along the surface, which is a common machining defect for CFRP [9], [13]. In the case of the coarse tool, the response surface forms a saddle surface. Based on the quadratic equation fitted on the data set, the optimal cutting width for a given feed rate, is 3.03 mm. This can be used for getting smoother surface along the joining points of the finished component.

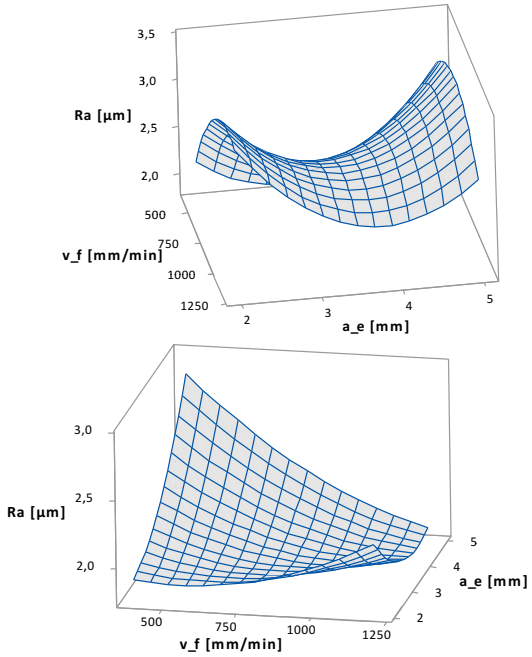


Fig. 6 Response sourfaces of average surface roughness (*Ra*) for tools 20340.450 and 20360.450, respectively

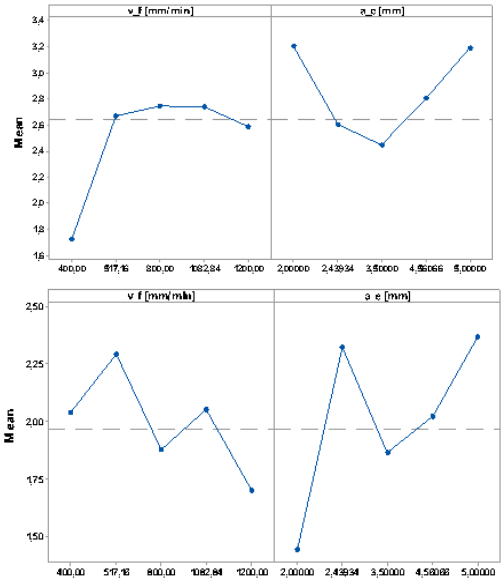


Fig. 7 Main effects diagram of average surface roughness for tools 20340.450 and 20360.450, respectively

As mentioned before, the amount of uncut fibres is a key parameter during machining of CFRP. We can get broader picture of this amount by inspecting the *Rz/Ra* ratio. Avarage surface roughness (*Ra*) is calculated as the arithmetical avarage value of all absolute differences from the centre line. This method tends to pay little attention for short high peaks, such as these fibres, or short deep valleys, like delamination on the surface. Roughness depth (*Rz*) is measured as the avarage distance from the highest peak to the lowest valley on five sampling lengths. *Rz/Ra* ratio gives us a proper value to represent the quantity of typical CFRP surface defects created during milling [7].

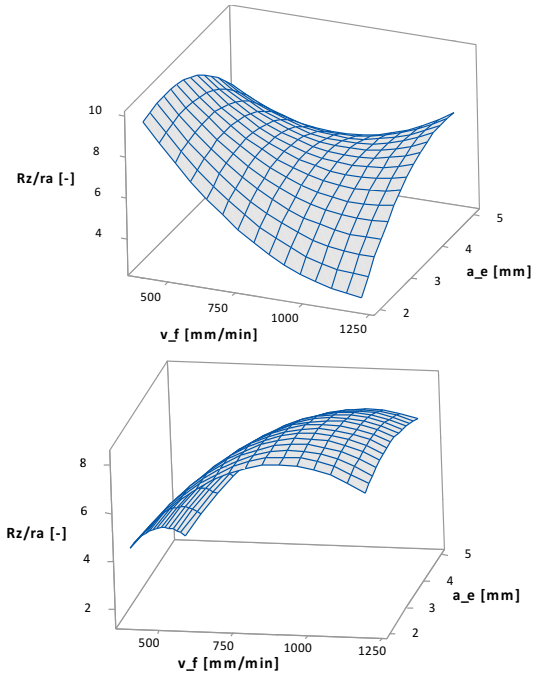


Fig. 8 Response sourfaces of Ra/Rz ratio for tools 20340.450 and 20360.450, as is

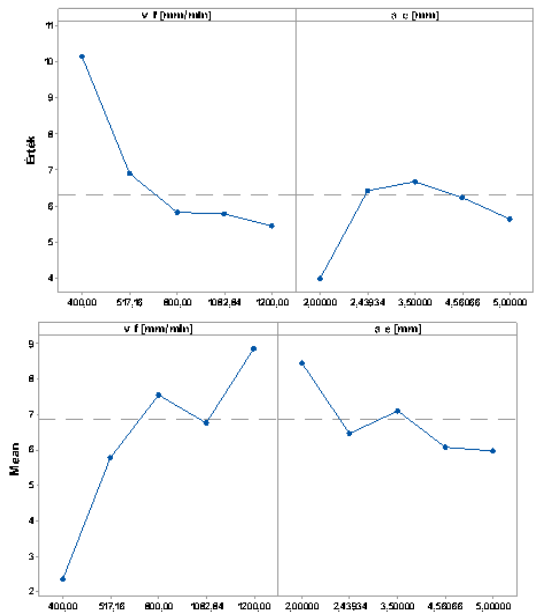


Fig. 9 Main effect diagram of Ra/Rz ratio for tools 20340.450 and 20360.450, as is

The response surfaces of the Rz/Ra ration are shown in the Fig. 8. On the basis of these and the ANOVA table, it's clear that the feed rate has by far more significant effect on the optimization parameter. Encrease of feed rate results in the decrease of this parameter. Therefore, it is advisable to use high feed near the joining points of the finished component.

4 Conclusions

In the present study, milling experiments were carried out in uni-directional CFRP using compression end mills in order to analyse and optimise process parameters. According to the present study, the following conclusions can be drawn:

- In the case of both compression end mills, both analysed factors (feed rate and cutting width) increase the cutting force, moreover the feed rate has the most significant effect on the cutting force, followed by the cutting width.
- RSM models were developed to analyse the influence of the factors on the cutting force. Cutting force were observably greater in the case of the compression tool with coarse tooth. This was possibly caused by the higher energy need of new chip formation.
- *Fz* (passiv) force component values are significantly lower than the other two components of the cutting force. It's caused by the tool geometry. The axial forces on the neighbouring edges are opposed, therefore these add up to smaller resultant passiv force.
- Both factors have significant impact on the measured *Ra* values. For the compression end mill with coarse tooth the optimal cutting width for any given feed rate, is 3.03 mm.
- Feed rate has by far more significant effect on the *Rz/Ra* ratio than the cutting width. Encrease of feed rate results in the decrease of this parameter. Therefore, use of high feed rates near the joining points during the finishing of the component leads to better surface quality, therefore better bonding.

Acknowledgement

The authors would like to acknowledge the support provided by the CEEPUS III HR 0108 project. This research was partly supported by the EU H2020-WIDESPREAD-01-2016-2017-TeamingPhase2-739592 project "Centre of Excellence in Production Informatics and Control" (EPIC). Furthermore, the authors acknowledge to prof. Gyula MÁTYÁSI and to the BSc students Csenge BÉKY, Kristóf SZOBODEK and Bertalan ZACHER for their participation in the experimental work.

REFERENCES

[1] M. Saleem, L. Toubal, R. Zitoune, and H. Bougherara, 'Investigating the effect of machining processes on the mechanical behavior of composite plates with circular holes', *Compos. Part Appl. Sci. Manuf.*, vol. 55, no. Supplement C, pp. 169–177, 2013.

[2] C. Soutis, 'Fibre reinforced composites in aircraft construction', *Prog. Aerosp. Sci.*, vol. 41, no. 2, pp. 143–151, 2005.

[3] C. Soutis, 'Carbon fiber reinforced plastics in aircraft construction', *Mater. Sci. Eng. A*, vol. 412, no. 1, pp. 171–176, 2005.

[4] R. Zitoune, V. Krishnaraj, and F. Collombet, 'Study of drilling of composite material and aluminium stack', *Compos. Struct.*, vol. 92, no. 5, pp. 1246–1255, Apr. 2010.

[5] L. Sorrentino, S. Turchetta, and C. Bellini, 'In process monitoring of cutting temperature during the drilling of FRP laminate', *Compos. Struct.*, vol. 168, no. Supplement C, pp. 549–561, May 2017.

[6] R. Voss, M. Henerichs, and F. Kuster, 'Comparison of conventional drilling and orbital drilling in machining carbon fibre reinforced plastics (CFRP)', *CIRP Ann.*, vol. 65, no. 1, pp. 137–140, 2016.

[7] N. Geier and T. Szalay, 'Optimisation of process parameters for the orbital and conventional drilling of uni-directional carbon fibre-reinforced polymers (UD-CFRP)', *Measurement*, vol. 110, no. Supplement C, pp. 319–334, 2017.

[8] H. Wang, J. Sun, J. Li, L. Lu, and N. Li, 'Evaluation of cutting force and cutting temperature in milling carbon fiber-reinforced polymer composites', *Int. J. Adv. Manuf. Technol.*, vol. 82, no. 9–12, pp. 1517–1525, Feb. 2016.

[9] M. K. N. Khairusshima, A. K. N. Aqella, and I. S. S. Sharifah, 'Optimization of Milling Carbon Fibre Reinforced Plastic Using RSM', *Procedia Eng.*, vol. 184, no. Supplement C, pp. 518–528, 2017.

[10] L. Lacalle, A. Lamikiz, F. Campa, A. FDZ. Valdivielso, and I. Etxeberria, 'Design and Test of a Multitooth Tool for CFRP Milling', *J. Compos. Mater. - J COMPOS MATER*, vol. 43, pp. 3275–3290, 2009.

[11] N. Geier, 'Machinability study of uni-directional CFRP using fractional factorial design', *Bp. Univ. Technol. Econ. TDK Study*, 2015.

[12] Norbert Geier and Gyula Matyasi, 'Machinability Study of Unidirectional CFRP Using Central Composite Design of Experiments', *Óbuda Univ. E-Bull.*, vol. Vol. 6, No. 1, 2016, 2016.

[13] R. Voss, L. Seeholzer, F. Kuster, and K. Wegener, 'Influence of fibre orientation, tool geometry and process parameters on surface quality in milling of CFRP', *CIRP J. Manuf. Sci. Technol.*, vol. 18, no. Supplement C, pp. 75–91, 2017.

Analysis of uncut fibres at machined holes in carbon fibre-reinforced plastics (CFRP) using digital image processing

Norbert Ibriksz, Norbert Geier

Department of Manufacturing Science and Engineering, Budapest University of Technology and Economics, 1111 Műegyetem rakpart 3. Building T 4th floor Budapest, Hungary

***Abstract* — Unlike metals, carbon fibre-reinforced plastics (CFRP) have anisotropic and inhomogeneous structure, in addition the reinforcements have strong wear-effect. Therefore those are difficult-to-cut materials. The main aim of this research is to find relation between the cutting tool diameter and the quality of the machined holes in CFRP. Milling experiments were designed using the full factorial design of experiments method. The experiments were conducted on a Kondia B640 machining centre. The machined surfaces were scanned with a digital microscope; the collected data were evaluated by digital image processing (DIP) techniques. The influence of tool-diameter and feed rate were examined and discussed in order to optimise the hole-machining process in CFRP.**

***Keywords*:** Carbon fibre-reinforced polymers, CFRP; machinability; digital image processing; uncut fibres

1 INTRODUCTION

Nowadays, in the high-tech industries, the use of carbon fibre-reinforced polymers (CFRP) is increasing, as it is shown in Fig.1. due to its good specific mechanical properties. Since the production technology of CFRP is often inaccurate or simply doesn't make it possible to produce any hole, their machining is necessary and essential in order to reach any required geometry. To minimize, or avoid any failure during machining special tools were designed, such as compression end mills or twist drills with special tip geometry. Although these tools are more suitable for machining CFRP materials compared to conventional tools, they cost often more. Hence this engineers often choose a cheaper conventional cutting tool. The main question is whether it worth to avoid buying special tools.

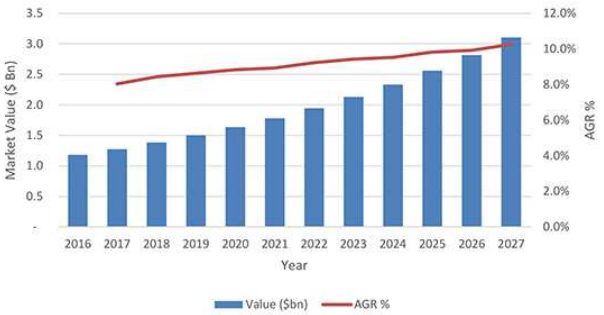


Fig.1 CFRP usage forecast in part of Europe [1] -$ Bn: billion dollar, AGR%: annual growth rate

1.1 PRELIMINARY KNOWLEDGE

Numerous earlier studies showed it is possible to machine hole in CFRP without special twist drill. One of these was written by *Geier and Szalay* [2]. *Sadek et al* [3] even proved it is possible to mill holes without any failure by using orbital drilling. These and several other researches assessed the fact, that feed rate has the most significant effect on the quality of the machined surface: regarding the average surface roughness, pulled out and uncut fibres (see Fig.3). Several article mention the so called „burr area" (see Fig.3) around 45° angle compared to the direction of the reinforce fibres, as can be seen in the Fig.2. Although delamination is also a known failure mode, during our experiments we did not take it into consideration.

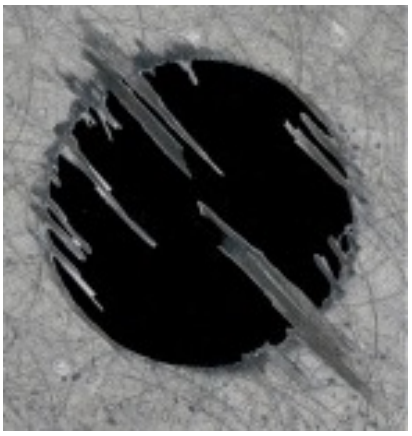


Fig.2 Uncut fibres [4]

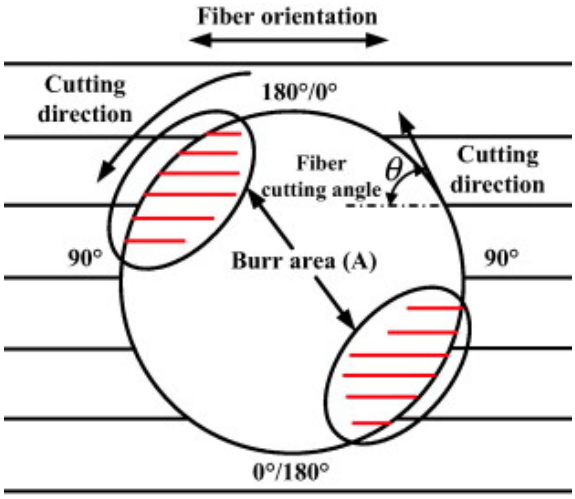


Fig.3 Burr area[5]

2 EXPERIMENT

2.1 DESIGN OF EXPERIMENT

2.1.1 APPLIED METHOD

The examined parameters (factors) were the tool diameter (D) and feed per tooth (fz) in this experiment. The values were chosen based on the recommendations of the tool manufacturer and preliminary knowledge. The factor levels can be seen bellow in Table 1. Since the number of the combination of the chosen values is few, it is possible to carry out full factorial experiments. This way experimental data loss can be decreased.

Table 1.Used parameters

D (mm)	4	6	8
f_z (mm/tooth)	0.01	0.04	0.07

2.1.2 MANUFACTURING STRATEGY

Previous researches proved, the climb milling results better surface, than conventional milling. Considering this fact, climb milling was used to machine holes Fig.4(b). The effect of lead-in Fig.4(a) and stand-off Fig4(c) strategy is excluded from the discussion of this experiment, so they are simple radial one, as can be seen in the Fig. 4.

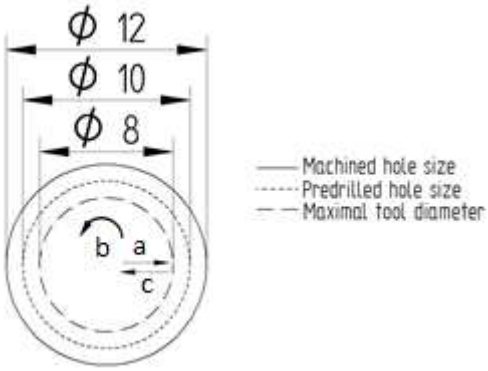


Fig. 4 Used manufacturing strategy. (a) movement is lead in, (b) is climb milling with feed rate and (c) is stand-off movement

2.1.3 EXPERIMENTAL SETUP

The experiments were carried out on a Kondia B640 machining centre. The tools were cemented carbide flute mills with one cutting edge, made by TIVOLY (ALU VHM P297), clamped in collet. For this experiment series a unique fixture was designed and manufactured, which ensure optimal material requirement and provides appropriate support resulting minimal delamination (laminated layer separation). In order to avoid the abrasive effect of carbon chips a Nilfisk GB 733 industrial vacuum cleaner was applied to remove them.

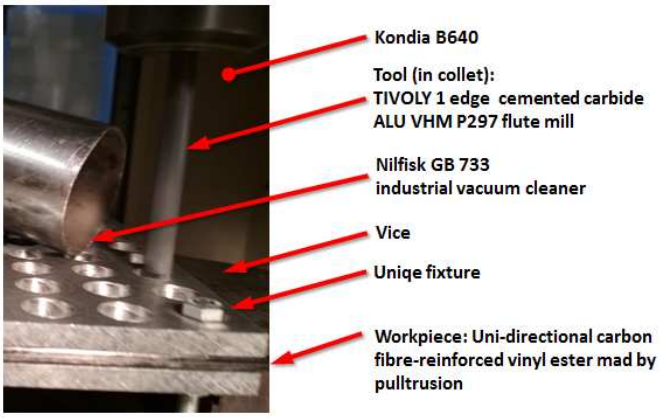


Fig. 5 Experimental setup

2.2 DATA COLLECTION

After machining, images were taken of the exit side of each hole, using Dino-Lite AD7013MZT digital microscope. These images were the base of the evaluation (explained below). Since the material was black, a white background was applied in order to increase the contrast of the images, thus increasing the accuracy of the evaluation process. The digital microscope station can be seen in the Fig.6.

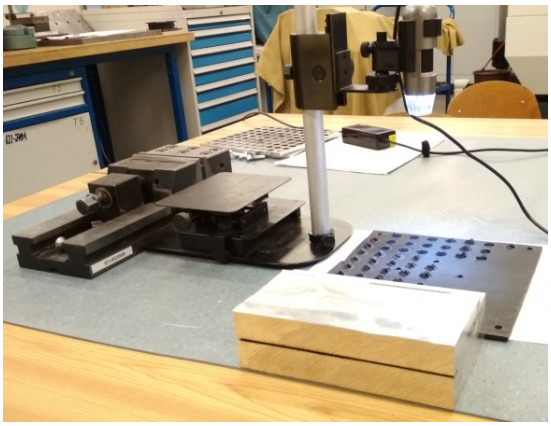


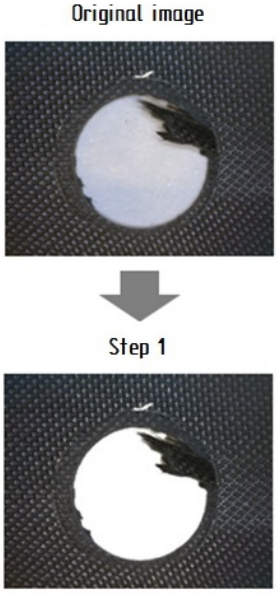
Fig. 6 Dino lite microscope during data collection

3 EVALUATION

3.1 USED METHOD

Digital image processing (DIP) was used to evaluate characteristics of uncut fibres. The images were binarized in three steps based on the picture's grey-scale histogram, as can be seen in the Fig. 7. In the first step was the white replacement, then the black replacement. The final step was removing the excess white pixels. During the image process the white pixels were counted. A reference value was measured on a computer drawn image. A see-through index (I) was determined as the ratio of the number of the white pixels on the picture (n_{pic}) and the reference number (n_{ref}). This is very similar to other commonly used area based method – for instance the one used for classifying delamination as *Faraz et al.* [6] did.

$$\underline{I} = \frac{n_{pic}}{n_{ref}} \tag{1}$$



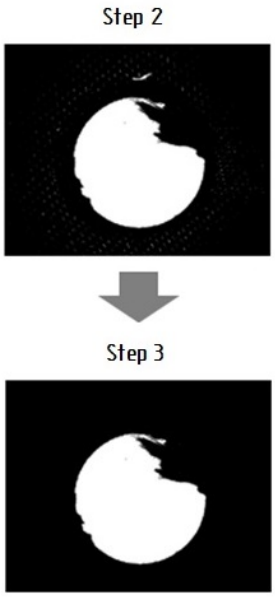


Fig. 7 Image processing of uncut fibres at the edge of drilled holes in CFRP

3.2 RESULTS

The method described above in was executed using Matlab and Mathematica software. Although both execute the same steps, the method used by them is different. As a result of this the returned values was different, but coherent. It means the returned value was not same for the same image, but since the reference value was also different it resulted only marginal differences in see-through index.

By analysing the indexes it became clear, the special drill is not necessary to make a good quality hole. It can be clearly seen in Fig. 9. This result confirmed our visual examination. This means it is possible to use general purpose conventional tool instead of special tool for CFRP manufacturing. Of course the machining parameters ought to be chosen carefully in this case, because of increased risk of causing failure in the material. With the proper settings the frequent defects can be avoided and the quality of the geometry will be also acceptable.

A chart is shown in Fig. 8 about see-through index of 22 holes made by the same drill under the same condition. After calculating the average value and the standard distribution (σ) of the given indexes we had to admit, the distribution is too big to consider these results exact, although the see-through index of manufactured holes reflects clear tendency.

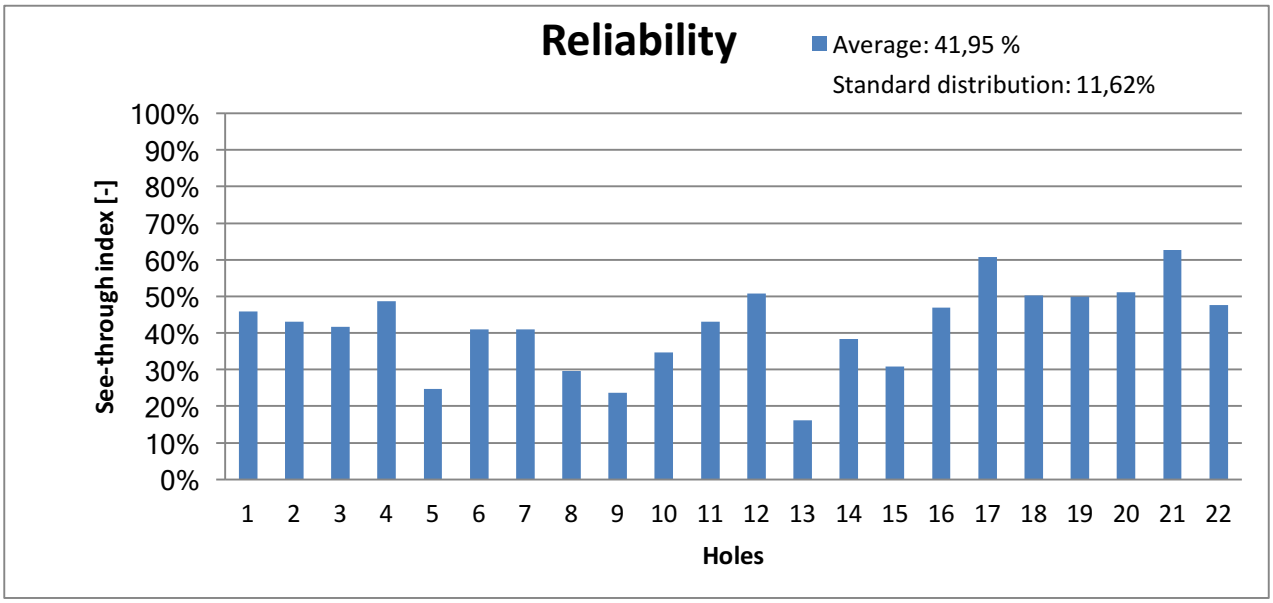
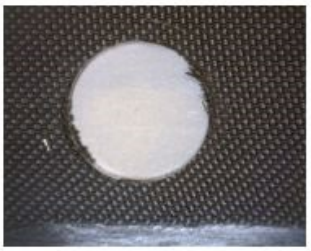
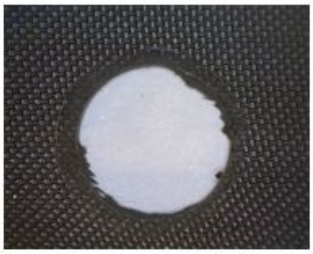


Fig. 8 Reliability of the processing



Special drill
I=77.51% σ=8.21%

Conventional drill
I=67.51% σ=4.81%



Drill
I=80.63% σ=7.84%

Fig. 9 Quality of holes –I: average see-through index, σ: standard distribution

4 SUMMARY

In conclusion the experiments confirmed our preliminary knowledge regarding the place of "burr area". Furthermore at low feed rate burning of the matrix polymer was noticeable. Some instance of fibre pull-out was also noticeable.

All in all in our opinion due to the inaccuracy (σ=11.62%) of the measurement no optimum can be settled, but it can be concluded, using a general purpose flute mill is also possible for machining good-quality holes in CFRP. Further analysis of the manufactured holes with more accurate devices or methods may reveal more specific relations.

5 REFERENCES

[1] https://www.visiongain.com/Report/1964/Carbon-Fibre-Reinforced-Plastic-(CFRP)-Composites-Market-Report-2017-2027

[2] N. Geier, T. Szalay (2017), Optimisation of process parameters for the orbital and conventional drilling of uni-directional carbon fibre-reinforced polymers (UD-CFRP), *Measurement*, 110, 319-334

[3] A. Sadek, M. Meshreki, M. H. Attia (2012), Characterization and optimization of orbital drilling of woven carbon fiber reinforced epoxy laminates, *CIRP Annals-Manufacturing Technology*, 61, 123-126

[4] Robert Voß, Marcel Henerichs, Stephan Rupp, Friedrich Kuster, Konrad Wegener (2016), Evaluation of bore exit quality for fibre reinforced plastics including delamination and uncut fibres, *CIRP Journal of Manufacturing Science and Technology*, 12, 56-66

[5] Jinyang Xu, Qinglong An, Ming Chen (2014), A comparative evaluation of polycrystalline diamond drills in drilling high-strength T800S/250F CFRP, *Composite Structures*, 117, 71-82

[6] Ali Faraz, Dirk Biermann, Klaus Weinert (2009), Cutting edge rounding: An innovative tool wear criterion in drilling CFRP composite laminates, *International Journal of Machine Tools and Manufacture,* 49, 1185-1196

A Hibamód- és Hatáselemzés alkalmazása napjaink autóiparában

Koncz Annamária[1]
[1]Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Magyarország
konczannamaria@gmail.com

Összefoglalás

A Hibamód- és Hatáselemzés (FMEA – Failure Mode and Effect Analysis) az autóipar (és az ipar) ismert minőségbiztosítási technikája. Használata az IATF 16949 autóipari szabványa (az ISO 9001 szabvány kiegészítő többletkövetelménye) alapján kötelező az autóiparban tevékenykedő vállalatok számára. Mindez érvényes az autógyártókra, illetve az egyes részegységeket előállító beszállítók számára is.
Munkánkban az FMEA-ra vonatkozó szabályokat, és az FMEA elkészítésének folyamatát, lépéseit mutatjuk be. Megmutatjuk a módszertan összefüggését a vállalatok minőségbiztosítási rendszerével (Control Plan, FMEA), elemezzük a módszer használatának előnyeit a beszállítókra, illetve az autógyártókra nézve.

Kulcsszavak: FMEA, Rendszer FMEA, Folyamat FMEA, Termék FMEA, funkcióháló, hibaháló

1 BEVEZETÉS

Napjainkban egyre nagyobb jelentőséget kap a minőség. A vállalkozások célja a fogyasztók számára egyre megbízhatóbb szolgáltatások, termékek előállítása, biztosítása, annak érdekében, hogy növeljék versenyképességüket.

A Hibamód-és hatáselemzés (FMEA:Failure Mode and Effect Analysis) metódusra az AIAG (Automotive Industry Action Group – Gépjárműgyártók Akciócsoportja), és a VDA (Verband der Automobilindustrie – Német Autógyártó Szövetség) is adott ki leírásokat. Ezenkívül az egyes autógyártók (Ford, GM, PSA) is kiadták a maguk előírását a tárgykörben. Ugyanakkor az FMEA módszertanra minden beszállító saját szabályozást alakíthat ki. Az FMEA kifejlesztése a 20. századra tekinthető (a módszer több, mint hetven éves), először az amerikai hadsereg írta le a negyvenes években 1], majd a NASA jegyezte le a metódust 1963-ban 2], de ugyanakkor az amerikai hadsereg is kiadta az erre vonatkozó előírását a nyolcvanas években (MIL-STD-1629 1980) [3].

A különböző iparágak fejlődése is életre hívta az FMEA szükségességét. A napjainkban is látványosan fejlődő autóiparban a sziszetmatikus elemzések segítik a gyártót. Példaként, az elektronikai fejlődésével még nagyobb jelentőséget kapott a hibák hatásának elemzése [4]. Azonban napjainkban nemcsak az autóelektronikai iparban használják az FMEA-t, hanem mechanikus alkatrészek előállításakor, sőt az élelmiszeriparban is [5].

Három különböző típusú FMEA-ról beszélhetünk: Rendszer FMEA-ról (System FMEA), Termék FMEA-ról (Design FMEA), és Folyamat FMEA-ról (Process FMEA). A három különböző fókuszú elemzés a teljes terméket lefedi, a rendszert, a terméket, és annak előállítási folyamatát. Abban az esetben, ha mindhárom elemzés szisztematikusan elkészül, feltérképezi a teljes késztermékét.

Az FMEA elemzés elkészítése során a potenciális hibákat vizsgáljuk- úgy, hogy hibahálóba helyezzük őket. Így a hiba összeköttetésbe kerül annak következményével, illetve okozójával is. Az FMEA rendkívül fontos eleme a minőségbiztosításnak, hiszen már konstrukciós szinten felfedheti az egyes nem –megfelelősségeket. Az elemzés felfedi a hibák lehetséges következményeinek súlyosságát, a hibaokok előfordulási gyakoriságát, illetve detektálásuknak lehetőségeit**.**

A Hibamód-és hatáselemzés a kockázatelemzés egyik eszköze, amely arra hivatott, hogy felmérje a termékekben, szolgáltatásokban, gyártási eljárásokban rejlő hibákat. Az FMEA ezáltal hasznos eszköze minden szolgáltató, és termelő vállalatnak.

A közlemény célja az FMEA eljárás bemutatása, annak lépéseivel, előnyeivel, és fejlesztési potenciáljával együtt. A tanulmányban felhasznált példák a Szerző tapasztalatai alapján előtérbe helyezik a folyamatszempontú megközelítést.

A tanulmány további részei: munkánk második fejezete az FMEA típusait írja le, majd a harmadik fejezet szemlélteti az elemzések lépéseit.

Tanulmányomban a negyedik fejezet bemutatja az FMEA kiindulási alapjait, az ötödik fejezet feltárja az FMEA eljárás szükségességét és előnyeit.

2 A HIBAMÓD-ÉS HATÁSELEMZÉS TÍPUSAI, FELÉPÍTÉSE

A Hibamód- és Hatáselemzés egy szisztematikus eljárás, amely a konstrukciókban, és a gyártási eljárásokban található hibák felfedésére, elemzésére és értékelésére, illetve azok elkerülésére alkalmas.

Az FMEA-t mindig csapatmunkában kell végezni [6]. Mivel minden lépés, és szint elemzésre kerül, ezért minden érintett területről szükség van szakemberre. Ugyanakkor nem szabad megfeledkezni arról , hogy minden FMEA projektre adott esetben külön csapat szükséges.

A csapatnak keresztfunkcionálisnak, és multidiszciplinárisnak kell lennie. Ez azt jelenti, hogy minden érintett területről szükség van közreműködésre, azonban minden területről különböző fukciókban dolgozó kollégákra is, hogy az elemzés ne legyen egyoldalú. Az FMEA-k komplexitása miatt szükséges egy FMEA moderátor alkalmazása is, akinek az a szerepe a csapatban, hogy irányítsa a résztvevőket. Az FMEA moderátornak a rendszertől, terméktől, folyamattól, szolgáltatástól függetlennek kell lennie.

Ahhoz, hogy az FMEA elemzés hatékony legyen, a résztvevőknek rendelkezniüknek kell a szükséges információkról a témában.

Ezek az információk lehetnek: az aktuális rendszer, termék, folyamat, szolgáltatás ismerete; képességadatok; információk a hiba előfordulásáról; és információk a bevezetendő intézkedésekről [7].

Az FMEA elemzések a sokoldalúságuknak köszönhetően sokrétűen használhatók az iparban, gyártó- és termelő vállalatoknál, valamint szolgáltatások esetén.

Alkalmazási területtől függően négy típusú FMEA beszélhetünk [7].

A Rendszer FMEA (System FMEA) rendszerek elemzéséhez használatos, a Termék FMEA (Design FMEA) [8] termékek elemzésénél használt, a Folyamat FMEA (Process FMEA) [8] folyamatok analíziséhez használt, a Szolgáltatás FMEA (Service FMEA) szolgáltatások elemzéséhez használatos.

Azonban nem szabad megfeledkezni arról, hogy a hibák egyszerre jelentkezhetnek rendszer-, termék-, folyamat- és szolgáltatás szinten. Ezért fontos, hogy a teljes előállítási láncra hozzunk létre FMEA-t [9].

2.1 Rendszer hiba-és hatásmód elemzés

A Rendszer FMEA-t többnyire a korai tervezési fázisban alkalmazzák, másként Koncepciós FMEA-nak is nevezik. Rendszerek, és alrendszerek elemzéséhez használatos.

Könnyen bemutatható a Rendszer FMEA és a Termék FMEA közötti összefüggés. Autóipari példával élve, ha a termék a fékvezérlő, akkor az alrendszer lehet a fékrendszer, a rendszer pedig maga a jármű.

A 1. ábra szemlélteti az említetett rendszer, alrendszer, termék kapcsolatot.

1. ábra Járművek rendszerei, alrendszerei [10]

A Rendszer FMEA a rendszer funkciók hibáira, nem teljesüléseinek felfedésére szolgál.

Kimenetei a Rendszer FMEA-nak a következők: RPN [11], [12] (Risk Priority Number: Hiba Prioritási Szám) számmal rangsorolt hibakép lista; egy lista a potenciális rendszer funkciókkal, amelyek detektálhatják a hibaképeket; valamint egy lista a potenciális dizájn intézkedésekről, amelyek csökkenthetik a hibaok előfordulásának gyakoriságát.

A Rendszer FMEA előnyei a következők lehetnek: segít megtalálni az optimális rendszer alternatívát; segít a redundancia meghatározásában; segít a rendszer diagnosztikai funkciók meghatározásában; növeli az esélyét a potenciális hibák felfedezésének, és segít a hibaképek alrendszerekkel összefüggésének meghatározásában [7].

2.2 Termék hiba-és hatásmódelemzés

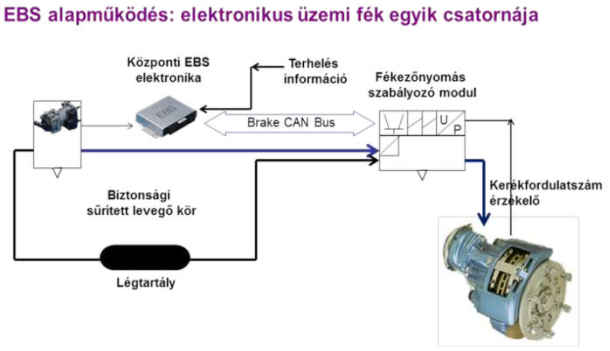
Termékek elemzésére szolgál, még a gyártásra felszabadítás előtt, a dizájnból eredő nem megfelelőségek felfedésével.

A példában a fékrendszer alrendszer része a fékvezérlő, amelyet a 2.ábra mutat.

A Termék FMEA a termék jellegéből adódóan több különböző típusú lehet [7]. Például egy elektronikai termék esetén lehet Szoftver FMEA, Elektronikus részegység FMEA, vagy Mechanikus FMEA.

Az ábránál a például vett elektronikus fékvezérlő (EBS) működési elvét láthatjuk.

(A pedálmodul fékezési jeladója elektromos jelként (két csatornás feszültség jel) adja meg a fékrendszer elektronikájának a vezető lefékezettségi igényét. Ebből az információból az elektronika meghatározza az egyes tengelyekhez kivezérelendő fékező nyomásokat és az erre vonatkozó parancs a gépkocsi CAN hálózatán keresztül jut el a nyomásmodulátorokhoz. Ezeknek az elektronikái fogadják a fékezési parancsot és ennek megfelelően működtetik az elektromágneses szelepeket, amelyek a megfelelő fékezőnyomást kivezérlik.)



2. ábra Intelligens fékrendszerek szerkezeti elemeinek analízise [13]

A Termék FMEA variációi a Gép-, Környezet-, és Tulajdonság FMEA, azonban ezeket jelen tanulmányunk keretein belül nem vizsgáljuk [7].

A Termék FMEA és a Rendszer FMEA összefüggéseit a fentiekben bemutattuk. Ugyanilyen összefüggés fedhető fel a Termék FMEA és a Folyamat FMEA között.

Minden termék előállítására lehet alkalmazni a Folyamat FMEA-t. A két elemzés a gyakorlatban úgy függ össze, hogy a Termék FMEA hibakövetkezményeit összhangba kell hozni a Folyamat FMEA hibaképeivel. Ez egy úgynevezett FMEA interfészen keresztül valósul meg, amely tartalmazza az egyszerűség kedvéért a releváns következményeket.

Így a Folyamat FMEA hibaképei az $RPN = SOD$egyenlőségnek megfelelően az S szorzótényezőt a Termék FMEA-ból nyerik.

A Termék FMEA kimenetei a következők: potenciális termék hibák listája; potenciális különleges jellemzők listája; dizájn intézkedések, amely a hibák előfordulásának csökkentésére fókuszálnak, valamint paraméterlista, a vizsgálandó, tesztelendő jellemzőket tartalmazza,

A Termék FMEA előnyei a következők: prioritást a termék dizájn javító akcióknak; dokumentálja a változások szükségességét; információkkal szolgál a termék teszteléséhez, verifikálásához, éssegít azonosítani a potenciális biztonsági kockázatait [7].

2.3 Folyamat hibamód-és hatáselemzés

A Folyamat FMEA elsősorban termékek gyártási folyamatainak elemzésére szolgál [8]. Ebben az esetben a funkciók a folyamat optimális működését mutatják be.

A Folyamat FMEA összefügg más minőségügyi módszerekkel, eljárásokkal. Legfontosabb megemlíteni a Control Plan-t és a *8D* eljárást [14].

A Control Plan magyarul Szabályozási Tervet jelent. A Szabályozási Tervben szerepelnie kell a gyártás minden lépésének, a meghatározott jellemzőikkel együtt. Ezeknek az FMEA és a Control Plan dokumentumok között meg kell egyezniük minden esetben. Ezt gyakorta úgy érik el a gyártó vállalatok, hogy ugyanazt a szoftvert használják a két eljárás eszközéül.

A Control Plan, az FMEA elemzéshez hasonlóan, szintén az IATF 16949 szabvány kötelező eleme az autóipari vállalatok számára.

A 8D egy minőségbiztosítási technika, amely egy hiba gyökér okait (gyártási hiba gyökér okait) hivatott megkeresni 8 lépésben. A 8D lehet külső (vevői jelzés alapján), és belső (szervezeten belüli) [4].

Mindkét esetben a 8D elemzésben meghozott azonnali, és hosszútávú intézkedéseket implementálni kell a Folyamat FMEA intézkedései közé. (Természetesen, ha a hibakép, és hibaok nem ismert, akkor szükséges azokat is szerepeltetni.)

A Folyamat FMEA kimenetei a következők: potenciális hibák listája, *RPN*[10][11] számmal rangsorolva; kritikus, és különleges jellemzők listája;

-potenciális intézkedések listája, amelyek a jellemzők biztosítását szolgálják.

A Folyamat FMEA előnyei között említhető, hogy korrektív intézkedési tervvel szolgál; továbbá fejleszti a Szabályozási Terveket; priorizálja a megelőző intézkedéseket; segít elemezni a gyártási, szerelési folyamatokat, és dokumentálja a változások szükségességét [7].

2.4 Szolgáltatás hibamód-és hatáselemzés

Szolgáltatások elemzésére szolgál, mielőtt azokat a vevők tapasztalnák. A Szolgáltatás FMEA a folyamatbeli nem megfelelőségekre fókuszál.

A Szolgáltatás FMEA kimenetei között találjuk a potenciális hibák listáját; a kritikus feladatokat és folyamatok definícióját; valamint a feladatokban, és folyamatokban jelölt szűk keresztmetszeteket.

A Szolgáltatás FMEA előnyei, hogy segít a munkamegosztás elemzésében; segít a szolgáltatás folymatának elemzésében; valamint azonosítja a kritikus, és szignifikáns folyamatokat; ezen kívül prioritást ad a javító intézkedéseknek; és dokumentálja a változások szükségességét [7].

3. A HIBAMÓD- ÉS HATÁS ELEMZÉSEK LÉPÉSEI

Az FMEA eljárás minden esetben négy főbb lépésből áll. Elsőként ábrázolunk egy struktúrát, majd funkciókat társítunk a struktúraelemekhez. A funkciókhoz végül a hibákat társítjuk, egy hibaelemzés keretein belül. Ha az FMEA váza rendelkezésre áll, akkor következik az intézkedések meghozása, és azok értékelése. A következőkben a részfolyamatokat mutatjuk be.

3.1 *Struktúra elemzés*

Az FMEA eljárás során először létrehozzuk a struktúrát, egy struktúra elemzés keretében. Ekkor meghatározzuk a rendszer elemeit, amelyet vizsgálni szeretnénk. A struktúra elemzés lehet egy blokk diagram, vagy egy egyszerű folyamatábra.

Rendszer esetén szükséges a rendszert részelemeire bontani, termék esetén alkotóelemekre, folyamat esetén részfolyamatokra, szolgáltatás esetén pedig részelemekre.

3.2 Funkcióelemzés

A struktúra elemzés után következik a funkcióelemzés, amelynek során a rendszer elemeihez funkciókat határozunk meg. Ez Rendszer FMEA esetén az adott

rendszer funkcióit jelöli, a Termék FMEA esetén a termék funkcióit, Eljárás FMEA esetén pedig az eljárás funkcióit. A funkcióelemzés azt jelenti, ha a rendszer optimálisan működik, akkor milyen funkciókat kell ellátnia, ha a termék megfelelő, akkor milyen funkciót lát el, valamint ha a folyamat megfelelően működik, akkor milyen feladatokat lát el [7].

3.3 Hibaelemzés

A funkcióelemzés után következik a hibaelemzés, amely során egy úgynevezett hibahálót hozunk létre. A hibák a funkciókból vezethetők le, azok nem-teljesülését jelentik.

A hibaháló középpontjában a hibakép áll, amelynek eredménye a hibakövetkezmény, és oka a hibaok. A hibaháló elemei a következőképp kapcsolódnak egymáshoz: hiba következmény-hibakép-hibaok.

Az FMEA elemzés során előfordul, hogy ismétlődnek jellegüknél fogva a következmények, hibaképek, vagy pedig a hibaokok. Mindez eredményezi a hibahálók komplexitását, hiszen, ismétlődés esetén nem szükséges újra felvenni a súlyosságokat, hibaképeket, vagy hibaokokat [7].

3.4 *Intézkedések meghozatala*

Az FMEA elemzések során a hibaokokat szükséges kielemezni.

Az intézkedések következők alapján hozhatók meg:

- Ha a kockázat elhanyagolható, nincs szükség intézkedések meghozására (azonban a gyakorlat azt mutatja, hogy ezt a vevők nem tolerálják).
- Ha közepes a kockázat, szükséges intézkedések deifiniálása.
- Ha magas a kockázat határozott akciókra van szükség (validálás, és kiértékelés is szükséges lehet).
- Ha kritikus a kockázat, akkor szintén határozott akciókra van szükség (ezenkívül változtatni szükséges a rendszeren, termék dizájnon, folyamaton, vagy szolgáltatáson).

Az egyes szabványok, valamint az autógyártók, és beszállítók kézikönyvei tartalmaznak úgynevezett értékelési katalógust, amiben meghatározzák egy-egy rövid definició mellett az egyes tényezők értékeit.

Az intézkedések elemzése két szempont alapján történik: ez a megelőzés és a detektálhatóság [7].

3.5 Megelőző intézkedések az FMEA-ban

A megelőzés azt mutatja, hogy mely intézedésekkel lehet elkerülni a hibaok kialakulását. Folyamat FMEA esetén a következőképpen lehet meghatározni a megelőzés szerepét.

Ha a hiba (például:sérülés a terméken) oka az, hogy az operátor más szerszámot használ az adott művelethez, akkor megelőzés lehet az, hogy a szerszám kódolt, így a másik állomáson használt szerszámot fizikailag nem lehet használni a művelethez.

Számszerűsíteni a megelőzés hatékonyságát az *O* (Occurance: Gyakoriság) tényezővel lehet [10]. A korábban említettek alapján a megelőzés 1-10-ig terjedő értéket kaphat, ahol az 1 a legritkább gyakoriság, a 10 pedig a leggyakrabban előforduló hibaok [15].

A gyakoriság értékének meghatározásában, segítséget ad, ha rendelkezésre állnak ppm értékek is. A ppm (Part Per Million: Hibaszám egy millióból) pontosabb közelítést ad a hibagyakoriság megadásához [7].

3.6 Detektáló intézkedések meghozása

A detektálás azt mutatja, hogy mely intézkedésekkel lehet detektálni az esetleges hibákat. Folyamat FMEA esetén a következőképpen lehet meghatározni a detektálás szerepét.

Ha a hiba -például a termék csatlakozó pinjei túl hosszúak- akkor automa detektálás lehet egy kamera rendszer, amely a csatlakozók pinhosszát méri. Ebben az esetben a detektálás jó értéket kap, mivel embertől független, objektív a hibafelismerés.

Abban az esetben, ha egy opretárnak kell vizuálisan vizsgálnia a terméket, úgy a detektálás értéke rosszabb lesz, mivel ez szubjektív vizsgálat. Azonban ha az operátor idomszerrel vizsgálja a pinhosszat, és ez az eszköz Poka Yoke megoldás, úgy a detektálás ismét jó értéket kaphat.

A megelőzés hatékonyságát a *D* (Detection:Detektálás) tényezőjével lehet mérni[10].

Ha a detektálás értékelése 10-es skála alapján történik, úgy a legjobb, leghatékonyabb detektálás 1, a 10 pedig a legrosszabb hatékonyságú detektálás.

Abban az esetben, ha a hibaokot nem tudjuk detektálni, úgy detektálhatjuk a hibaképet magát is. Például, ha az előbb említett kamera rendszer meghibásodik, és nincsen másodlagos detektálás, úgy csak azt a tényt tudjuk detektálni, hogy a pinek hosszabbak a megengedettnél. Ebben az esetben azonban a detektálás a legrosszabb értékeket fogja kapni, mivel a detektálás valószínűsíthetően már a vevőnél következik be [7].

3.7 *Tényezők értékelése*

Az FMEA elemzés utolsó lépéseként következik az egyes tényezők értékelése.

Az FMEA elemzés során használt mérőszám az RPN [10], [11]. Az RPN három tényező szorzatából áll.

Az *S* tényező a hiba következményének súlyosságát jelöli, az O hibaok gyakoriságát, a D a hibaok detektálhatóságát [10]. Mindhárom tényező maximális értéke 10, így az RPN szorzat eredménye maximálisan 1000.

A súlyosság esetén a legsúlyosabb hiba pontértéke 10, ezt abban az esetben kaphatja a hiba, ha halálos, életveszélyes következményekkel jár [16].

A gyakoriság esetén a legyakrabban bekövetkező hibaok 10-es értékelést kap, a legritkábban előforduló1-est (ha Poke Yoke eljárásról beszélünk).

A detektálás esetében a legkevésbé detektálható hibaok 10-es értékelést kap, a legjobban detektálható pedig 1-est,

abban az esetben, ha automatikus hibadetektálásról van szó.

Az RPN szorzat tényezőinek meghatározása történhet kvalitatív és kvantitatív módon.

Munkákban a kvantitatív meghatározással foglalkozunk. Ebben az esetben az adatoknak jól meghatározottak, egzaktak. Ezek az adatok lehetnek aktuális (gyártási) adatok, és/vagy hasonló rendszerből vett helyettesítő adatok az értékeléshez [17].

4. KIINDULÁSI ALAPOK HIBAMÓD-ÉS HATÁS ELEMZÉSEK ELVÉGZÉSE ESETÉN

A következőkben ismertetem az FMEA elemzések során használható kiindulási alapokat. Egyértelmű, hogy az FMEA elemzés annál tényszerűbb, és helytállóbb, minél több valós, bizonyított információ áll rendelkezésre.

A szükséges információkat FMEA típusonként szerepeltetjük.

4.1 Kiindulási alapok rendszer esetén

Abban az esetben, ha a rendszer hasonló egy más rendszerhez, vagy pedig elérhetőek a korábbi adatok használható korábbi statisztikai adatok, vagy a helyettesítő rendszerből kinyert információk, akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, és a matematikai modellezések eredményei.

Abban az esetben, ha rendelkezésre állnak korábbi hibaadatok, magáról a rendszerről, vagy egy helyettesítő rendszerről, használhatók korábbi statisztikai adatok, vagy a helyettesítő rendszerből kinyert információk (képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei, a korábbi hibák adatati, vagy kummulált hibaadatok).

Abban az esetben, ha a rendszer új, és nem állnak rendelkezésre kvantitatív adatok, az FMEA csoport határozza meg az S,O,D értékeket [17].

4.2 Kiindulási alapok termék esetén

Ha a termék dizájn hasonló más termékhez, vagy pedig elérhetők korábbi adatok akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei.

Abban az esetben ha rendelkezésre állnak a termék, vagy ahhoz hasonló helyettesítő termék hibaadatai, használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei,a korrábi hibák adatati, vagy kummulált hibaadatok.

Abban az esetben, ha a termék új, és nem állnak rendelkezésre kvantitatív adatok, az FMEA csoport határroza meg az S,O,D értékeket [17].

4.3 Folyamat esetén a következőkből indulhatunk ki

Ha a folyamat statisztikailag szabályozott, akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei.

Abban az esetben, ha a folyamat ismert, vagy létezik helyettesítő folyamat, akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei.

Abban az esetben, ha rendelkezésre állnak a folyamat, vagy ahhoz hasonló helyettesítő folyamat hibaadatai, használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei,a korrábi hibák adatati, vagy kummulált hibaadatok.

Abban az esetben, ha a folyamat új, és nem állnak rendelkezésre kvantitatív adatok, az FMEA csoport határozza meg az S,O,D értékeket [17].

4.4 Kiindulási alapok szolgáltatás esetén

Ha a szolgáltatás statisztikailag szabályozott, akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei az elemzéshez.

Abban az esetben, ha a szolgáltatás ismert, vagy létezik helyettesítő szolgáltatás, akkor használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei.

Abban az esetben, ha rendelkezésre állnak a szolgáltatás, vagy ahhoz hasonló helyettesítő szolgáltatás hibaadatai, használhatók a képességvizsgálatok eredményei, aktuális eloszlások, megbízhatósági adatok, matematikai modellezések eredményei,a korrábi hibák adatati, vagy kummulált hibaadatok.

Abban az esetben, ha a szolgáltatás új, és nem állnak rendelkezésre kvantitatív adatok, az FMEA csoport határozza meg az S,O és D értékeket [17].

5. A HIBAMÓD-ÉS HATÁSELEMZÉS ELŐNYEI, SZÜKSÉGESSÉGE

A Hibamód- és Hatáselemzés, abban az esetben, ha megfelelően használják, egy rendkívül hatásos eszköz a hibafaktorok kiküszbölésében. Hatékony eszköz továbbá a belső hibakeresésre, és a vevőkkel való kommunikációra (főleg (8D eljárás esetén).

5.1 Az eljárás előnyei

Az FMEA megjelenése előtti minőségügyi szemlélet a problémák megoldására fókuszált, a veszteségek felmérésére és a megbízhatóság számszerűsítésére. Az FMEA eljárás megjelenésével egy új szemlélet alakult ki az ipar minőségbiztosításában. A hangsúly áthelyeződött a hibák megelőzésére, a veszteség eliminilására valamint a megbízhatóság növelésére.

Az FMEA segít a gyártmány tervezés kezdeti szakaszában nagy megbízhatósággal és biztonsággal a megfelelő alternatívák kiválasztásában; javítja a vállalat versenyképességét, és imidzsét; valamint növeli a vevői elégedettséget; továbbá csökkenti a termékfejlesztési cikulus idő- és költségigényét. Ezen kívül segít az

optimális dizájn kiválasztásában; a rendszer redundanciájának meghatározásában; diagnosztikai eljárások meghatározásában; meghatározni kritikus, illetve jelentős jellemzőket (karakterisztikákat); új gyártási- illetve szerelési eljárások elemzésében; valamint a feladatok elemzésében, sorrendiség és szervíz tekintetében.

AZ FMEA eljárás továbbá prioritást ad a termék dizájn javításának; a hibák előfordulásának megelőzésére helyezi a hangsúlyt; segít a korrekciós intézkedések meghozatalában; biztosítja, hogy az összes szignifikáns hiba kivizsgálásra került; felsorolja a hibákat és meghatározza a hatásuk mértékét; biztosítja a fejlesztési- és a validációs fázis tesztlépéseit; valamint fejleszti a korai kritériumokat a gyártás, eljárás, szerelés, és szervíz esetén.

Az FMEA egyértelműen segíti a vállalatot. Mivel versenyelőnyt teremt, növeli a szervezet teljesítő képességét, és fejleszti a vállalati kultúrát.

Ennek megfelelően egy jól elkészített FMEA azonosítja az ismert, és potenciális hibaképeket; meghatározza minden hibakép okát, és következményét; és rangsorolja az hibaképeket, az RPN szám alapján [18].

5.2 Az eljárás szükségessége

Alapvetően minden tervezési folyamatot megelőzően (legyen az rendszer, termék, folyamat, vagy szolgáltatás) vagy párhuzamosan szükséges FMEA készítése, azonban vannak speciális esetek, amikor a már létező elemzéseket módosítani szükséges. Módosítás szükséges, ha a termék, gyártási eljárás, szolgáltatás módosításra kerül;

- a Control Planek (Gyártási Szabályozási Tervek) módosítása esetén;
- amikor fejlesztési potenciálok fedezhetők fel a rendszer, termék, folyamat, szervíz esetében;
- hibaelemzések készítése esetében;
- periodikusan a termék, eljárás, szolgáltatás életciklusában;
- vevői visszajelzések esetén (például reklamációk);
- 8D hibakereső eljárások adatainak implementálása esetén (lehet az belső, vagy külső 8D);
- ha a felelősök személye megváltozik;
- ha a meghozott intézkedések változást idéznek elő a folyamatban (például változik a gyakoriság, könnyebbé válik a detektálás); illetve
- ha a meghozott intézkedések határidejét módosítani szükséges [18].

6. ÖSSZEGZÉS

A cikkben az FMEA módszertan szakirodalmi bemutatása volt a tanulmányunk célja. Az FMEA egy rendkívül sokoldalú eszköz a hibák felfedésére, eliminálásra, abban az esetben, ha kellő energia ráfordítással jár a kezdeményező fél részéről. Minden rendszerre, termékre, folyamatra és szolgáltatásra használható. Ezért a nem az autóiparban tevékenykedő vállakozások számára is rendkívül előnyös.

Későbbiekben a szerző célja az FMEA szubjektivitásának vizsgálata, gyakorlati példákon keresztül [19], valamint az egyes FMEA típusosok bővebb vizsgálata [17], [20].

IRODALOMJEGYZÉK

[1.] Christian Spreafico, Davide Russo , Caterina Rizzi: A state-of-the-art review of FMEA/FMECA including patents, Computer Science Review, Volume 25, August 2017, Pages 19-28, 2017

[2.] Hossein Sayyadi Tooranloo, Arezoo sadat Ayatollah: A model for failure mode and effects analysis based on intuitionistic fuzzy approach, Applied Soft Computing, Volume 49, December 2016, Pages 238-247,2016

[3.] Koji Komita,Tomohiko Sakao, Yoshiki Shimomura: A failure analysis method for designing highly reliable product-service systems, Research in Engineering Design, April 2018, Volume 29, Issue 2, pp 143–160, 2018

[4.] C.J. Price , N.S. Taylor: Automated multiple failure FMEA, Reliability Engineering & System Safety, Volume 76, Issue 1, April 2002, Pages 1-10, 2002

[5.] Antonio Scipioni , Giovanni Saccarola, Angela Centazzo, Francesca Arena, FMEA methodology design, implementation and integration with HACCP system in a food company, Food Control, Volume 13, Issue 8, December 2002, Pages 495-501, 2002

[6.] Kwai-Sang Chin , Ying-Ming Wang , Gary Ka Kwai Poon , Jian-Bo Yang: Failure mode and effects analysis using a group-based evidential reasoning approach, Computers & Operations Research, Volume 36, Issue 6, June 2009, Pages 1768-1779, 2009

[7.] D. H. Stamatis: Failure Mode and Effect Analysis: FMEA from Theory to Execution, 2003

[8.] P.C. Teoh , Keith Case: Failure modes and effects analysis through knowledge modelling, Journal of Materials Processing Technology, Volumes 153–154, 10 November 2004, Pages 253-260, 2004

[9.] Ying-Ming Wang , Kwai-Sang Chin , Gary Ka Kwai Poon , Jian-Bo Yang: Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean, Expert Systems with Applications, Volume 36, Issue 2, Part 1, March 2009, Pages 1195-1207

[10.] Közúti járművek szerkezeti felépítése, http://kozlekedes.bme.hu/wp-content/uploads/2016/09/JKL_Rendszerek_KozutiJarmuvek_2.pdf, 2016

[11.] H. Arabian-Hoseynabadi , H. Oraee , P.J. Tavner: Failure Modes and Effects Analysis (FMEA) for wind turbines, International Journal of Electrical Power & Energy Systems, Volume 32, Issue 7, September 2010, Pages 817-824, 2010

[12.] Kyungmee O. Kim , Ming J. Zuo: General model for the risk priority number in failure mode and effects analysis, Reliability Engineering & System Safety, Volume 169, January 2018, Pages 321-329,2018

[13.] Intelligens fékrendszerek szerkezeti elemeinek analízise, http://www.mogi.bme.hu/TAMOP/kozuti_jarmurendszerek_szerkezettana/math-ch16.html, 2017

[14.] Koncz Annamária: A 8D problémamegoldó technika http://epa.oszk.hu/02600/02694/00069/pdf/EPA02694_rtk_2015_03.pdf, 2015

[15.] Saptarshi Mandal, J. Maiti: Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach, Expert Systems with Applications, Volume 41, Issue 7, 1 June 2014, Pages 3527-3537

[16.] Seung J. Rhee , Kosuke Ishii: Using cost based FMEA to enhance reliability and serviceability, Advanced Engineering Informatics, Volume 17, Issues 3–4, July–October 2003, Pages 179-188

[17.] Szilágyi Gábor, Lukács Krisztián, Szamosi Barna, Pokorádi László: A QS 9000 és a VDA szerinti hibamód és -hatáselemzések összehasonlítása , http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-33-0115_Szilagyi_Gabor_et_al.pdf, 2014

[18.] Failure Mode and Effect Analysis, http://asq.org/learn-about-quality/process-analysis-tools/overview/fmea.html, 2017

[19.] Szamosi Barna-Pokorádi László:Az interszubjektivitás hatása az FMEA-ban, http://epa.oszk.hu/02600/02694/00067/pdf/EPA02694_rtk_2015_1_073-080.pdf, 2015

[20.] Lázár-Fülep Tíme, Pokorádi László: Reliability in Automotive Engineering by Fuzzy Rule-Based FMEA, https://link.springer.com/chapter/10.1007%2F978-3-642-33805-2_64,2012

A szennyvíz vizsgálata az energiabiztonság szemszögéből

The examination of wastewater from the perspective of energy security

Bakos Imre
Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Budapest, Magyarország
bakos.imre@bgk.uni-obuda.hu

***Összefoglalás* — Az energiabiztonság az egyik legfontosabb téma, ami az egész Földet érinti. Hazánkban az '90-es évek óta jelent növekvő problémát. Ebből kifolyólag szükséges az alternatív energiaforrások, -mint például a biomassza - lehetőségeit felkutatni. A szerves anyagok anaerob fermentációja során biogáz termelődik, ami értékes energiahordozó. Ilyen jelentős mennyiségű szerves anyag halmozódik fel a szennyvíztisztító telepeken.**

A Dél-pesti Szennyvíztisztító telep környezetbarát és bevált tisztítási technológiák alapján működik. Ugyanakkor felhasználják az iszap és a szilárd hulladék energiapotenciálját. A telepen biogáz előállítására szilárd és folyékony szerves hulladékot kezelnek a szennyvízkezelésből származó iszapokkal együtt. Így közel 40 ezer m^3 biogázt állítanak elő naponta a szennyvízből és a beszállított hulladékokból. [1]

***Kulcsszavak*:** szennyvíztisztító telep, biogáz termelés, energiabiztonság

***Abstract* — The safety of energy is the one of the most important topic all over the world. This problem was growing up from the '90 in Hungary. We have to looking for the alternative energy sources for example biomass. The anaerobic fermentation's of the organic material produce biogas, wich is a valuable energy carrier. Large amount of organic matter haveaccumulated in wastewater plants.**

The wastewater treatment plant is operated on the basis of environment-friendly proven cleaning technologies at the south of Budapest. It making use of the energy potential of sludge and solid waste at the same time. At the plant, for the purpose of producing biogas, solid and liquid organic waste is managed together with sludge originating from wastewater treatment. Thus nearly 40 thousand m^3 of biogas is produced daily from sewage and wastes transported from outside. Give a short description about the research work.

***Keywords*:** wastewater plan, biogas product, energy security

1 BEVEZETÉS

Az Európai Unió tagállamai közül Németországban a legkiemelkedőbb a biogáz-termelés. 2013 végén az Európai Biogáz Szövetség adatai szerint a térségben egészen pontosan 14572 biogáz termelő üzem működött (mezőgazdasági, ipari, szennyvíztelepi és depónia alapon), amiből 9035 üzemmel Németország rendelkezett. Olaszország áll a második helyen, ahol 1391 üzemel. [2]

Magyarországon napjainkban közel 50 biogáz telep működik, melyek együttes villamosenergia-termelő kapacitása 37 MWe. (Magyarország összes energiaigénye 6000- 6500 MW) A hazai biogáz telepek több, mint a fele mezőgazdasági üzemben található, a kapacitásuk 21 MWe -ot tesz ki. Ilyen létesítmény például a szarvasi üzem, mely a baromfivágásból származó hulladékokat hasznosítja, vagy a kaposvári üzem, ami a cukorgyártásból származó mezőgazdasági hulladékokra épült.

Hazai viszonylatokban jelenleg is a legnagyobb kapacitással a nyírbátori Bátortrade Kft. biogáz üzeme rendelkezik, mely mezőgazdasági, valamint baromfivágásból származó hulladékokat hasznosít. A telep kapacitásának megduplázásával már 3,6 MWe előállítására képes. [3][5]

Szennyvíz iszap felhasználására 23-25 létesítményt építettek, amelyek teljesítménye 12-13 MW. Ilyen üzemek közé tartozik a Szegedi Vízmű Zrt. szennyvíztelep is a két, egyenként 4000 m^3-es mezofil rothasztó tornyukkal. A 36-38°C fokos üzemi hőmérsékleten, több mint 20 nap alatt megy végbe a rothasztási folyamat, azaz a biogáz termelése. Éves szinten 2 millió m^3 (5.600 m^3/nap) biogáz keletkezik, melynek metánkoncentrációja 63%. [4] A zalaegerszegi szennyvíztisztító telep biogáz előállítása pedig átlagosan napi 130-150 m^3 kevert iszap rothasztásából valósul meg, melyből 1000-1500 m^3 biogáz keletkezik. [4][6][7]

Budapesten a Fővárosi Csatornázási Művek Zrt két nagy kapacitású biogázüzemet – egyet a Dél-pesti Szennyvíztisztító telepen (1. ábra), és egyet az Észak-pesti Szennyvíztisztító telepen - működtet, melyek a hulladékként jelentkező szennyvíziszapot hivatottak hasznosítani, egyenként mintegy 3 MWe kapacitással.

1. ábra: Dél-pesti Szennyvíztisztító Telep [9]

Az üzemekben nemcsak, hogy környezetkímélő módon ártalmatlanítják a szennyvizet, és ezzel környezetvédelmi tevékenységet látnak el, hanem a beszállított szervesanyag tartalmú élelmiszer hulladékból zöldenergiát termelnek. A folyamatos kutatások, fejlesztések eredménye a telepen magyar szabadalommal megvalósult Organica élőgépek rendszer (2. ábra), mely a tisztítás hatásfokát élőnövényzet gyökérzetével igyekszik növelni. [8]

A rendszeres nyílt napok, diákcsoportok fogadása, a felelősségteljes, környezettudatos gondolkodásmód kialakulását segítik elő az idelátogatókban, ami szintén pozitívan hathat az energiabiztonságra. Az ilyen programok rávilágítanak a környezetvédelem, a hulladékgazdálkodás és a biogáz előállítása kapcsán az észszerű energiahordozó gazdálkodás szoros összefüggéseire.

2. ábra Organica élőgépek rendszer [10]

Az Óbudai Egyetem Gépész és Biztonságtechnikai karán 2008-ban létesült biogáz laboratórium, és azóta folynak vizsgálatok, mérések és kutatás az oktatási intézményben. A kezdetben mezőgazdasági hulladékokból származó biogáz kísérletekhez a Fővárosi Csatornázási Művek Zrt. biztosította az oltóanyagot. Az azóta eltelt időszakban nagyon konstruktív kapcsolat alakult ki az Egyetem és a Dél-pesti Szennyvíztisztító telep között.

A szennyvíztisztító jelenleg mintegy 300 ezer lakost szolgál ki. Célul tűztem ki, hogy megvizsgálom az itt keletkező biogáz mennyiség ismeretének birtokában, azt hogy egy Magyarország méretű – az egyszerűbb számítás kedvéért 9 millió fő – szennyvíz keletkezésekor mennyi biogáz keletkezhetne. Ennek a földgázra történő egyenértékűsítése után, összehasonlítom hazánk aktuális földgáz exportjával.

Áttekintem ezáltal annak a lehetőségét, hogy egy ideális állapotban – melyben az ország összes keletkező szennyvízéből megvalósítjuk a biogáz termelést – milyen pozitív hatással lehetne az energiabiztonságának alakulására.

2 A SZENNYVÍZTELEPI BIOGÁZTERMELÉS JELLEMZŐI

A keletkezett biogáz felhasználásának legáltalánosabb megoldása, a helyben, gázmotorban történő elégetés, kapcsolt energiatermelés (hő és elektromos áram termelés). Másik lehetséges megoldás a földgáz rendszerbe történő betáplálás, de ez egyelőre a hazai műszaki és jogszabályi környezetben túl nehézkesnek tűnik.

A gázmotorok esetében az áramtermelési hatásfok (a bemenő gáz energiatartalmához viszonyítva) legfeljebb 40%, de emellett jelentős mennyiségű hő is jelentkezik. Gondot jelent továbbá, hogy az így keletkezett hőenergia nem mindenhol hasznosítható, így az a rendszer hatékonyságának értékét nem növeli.

Egy m^3 biogázból átlagosan 2-2,5 kWh elektromos áram és 2,5-3 kWh hőenergia keletkezik. Nyári időszakban a hőenergiát esetenként vészhűtővel kell elvezetni. A termelt áram hálózatra történő táplálása a jelenlegi garantált átvételi ár mellett csúcs- és völgyidőszakban gazdaságos lehet, bár a táplálást lehetővé tevő berendezések létesítése költségekkel jár.

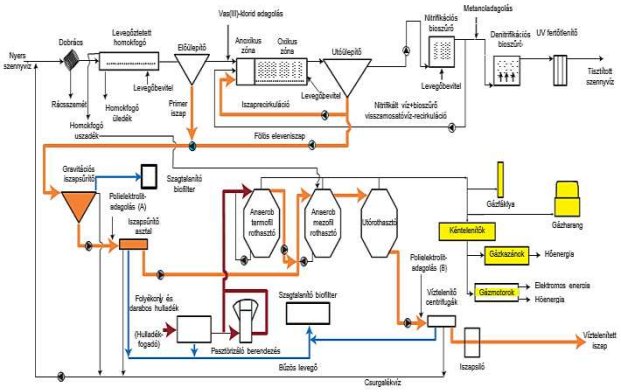
Nem célszerű a mélyvölgy-időszakban (hajnali 3 és 6 óra között) külső hálózatra termelni, mert az átvételi ár ekkor igen alacsony. Ekkor belső használatra érdemes áramot termelni, vagy a biogáz tárolását kell megoldani. A termelt gáz csak fűtésre történő felhasználása nem gazdaságos, ilyen esetben – különösen a nyári időszakban – nagy mennyiségű gázt kell elfáklyázni. [7]

3 A DÉL-PESTI SZENNYVÍZTELEP BIOGÁZ ELŐÁLLÍTÁSÁNAK PARAMÉTEREI

A Dél-pesti Szennyvíztisztító telep, -melynek távlati felvételét mutatja az 1. ábra -, Magyarország első szennyvíztisztító telepe, amely 1966 óta üzemel. [8]

Naponta átlagosan 53 ezer m^3/nap szennyvizet tisztít meg, amit aztán a Kisdunába engednek vissza. Kapacitása napi 80 ezer m^3, évi 22 millió m^3 [8]. A szennyvíztisztítás melléktermékeként keletkezeik kb. 500 m^3/nap mennyiségű nyersiszap és eleveniszap. Ehhez adódik hozzá a telepre zárt rendszerben beszállított kb. 100 m^3/nap szilárd, zsírszerű és folyékony hulladék. [7]

A szennyvíztelep felépítését, elvi elrendezését mutatja be a 3.ábra.



3. ábra: A szennyvíztelep felépítése [12]

1989-től megkezdődött a biogáz hasznosítás, ami segítségével a gázmotorok által előállított energia biztosítja az eleveniszapos rendszer légfúvóinak működését.

Az igen bonyolult, számos baktériumtörzs szimbiotikus kapcsolatán keresztül történő folyamat a telepen elhelyezett 1 db termofil és 4 db mezofil rothasztó toronyban- melyeket a 4. ábra mutat - megy végbe. A szilárd alapanyag, homogenizálását és pasztörizálását követően betáplálásra kerül első lépésként a termofil anaerob (üzemi hőmérséklet 55 ^oC, hasznos térfogat 2000 m^3), majd második lépésként mezofil anaerob (üzemi hőmérséklet 35 ^oC, hasznos térfogat: 3 x 2600 m^3) fermentorokba. (4. ábra)

4 . ábra Dél-Pesti Szennyvíztisztító telep, fermentorok [10]

A termelt mennyiség többször megközelíti a 40 ezer m^3/nap termelt energiahordozót a 3 db gázmotorban - Jen Bacher JMS 312, Jen Bacher JMS 316 és Caterpillar 1,2 MW (5. ábra) gyártmányú egységekben - égetik el. Ezek elektromos teljesítménye 625, 836 és 1200 KW értéket képvisel, amit a technológia, a gyártelep és a kiszolgáló épületek saját energiafelhasználásra hasznosítanak.

A gázmotorok üzemeléséből adódó hőenergia pedig hőcserélő segítségével a fűtési rendszer támogatja.

5. ábra Az 1,2 MW-os Caterpillar konténeres gázmotor [10]

Jelentősen növelte a termelési hatékonyságot, a 2014-ben megépült membrános gáztároló (6. ábra). Ennek üzembehelyezésével lehetőség nyílt arra, hogy optimális időszakban történhessen a felhasználás, valamint tervszerű vagy meghibásodás miatti gázmotor leállás esetén is megoldottá vált a nagyobb mennyiségű biogáz átmeneti tárolása. A közeljövőben újabb gáztároló megépítése várható az üzem területén.

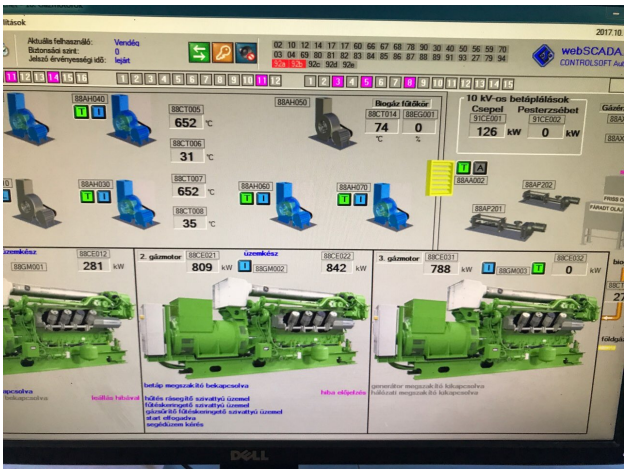
Mivel a szennyvíztisztító telepeken a rothasztó berendezések közel azonos nyers-és fölös iszap és egyenletes terheléssel üzemelnek, ezért célszerű megvalósítani az üzembe szállított további hulladékok segítségével a kofermentációt.

A kommunális (szerves) hulladéklerakás jelenleg hazánkban még jelentős szerepet kap, amiben változás várható az Uniós szabályozásnak betartása miatt. Ez alapján a biológiailag lebomló szerves anyagok lerakásra kerülő mennyiségét a jövőben adott szabályok szerint 35%-ára csökkenteni kell.

6. ábra Dél-Pesti Szennyvíztisztító telep, membrános gáztároló [10]

Itt meg kell említeni, hogy a globális felmelegedés visszaszorítása szempontjából fontos, hogy a lerakógázt gyűjtsük és felhasználjuk. A fel nem használt depóniagázt el kell fáklyázni, mert a levegőbe kerülő metán okozta üvegházhatás a széndioxidhoz képest húszszorosan káros következménnyel jár. [11]

A Dél-Pesti szennyvíztisztító telepen üzemelő két gázmotor, és a konténeres gázmotor működését, teljesítményét, aktualitását egy erre a célra kiépített irányító központból követik figyelemmel, a telephelyen belül. Az itt megfigyelt, rögzítésre kerülő adatok - mivel elektronikus formában jelentkeznek -, akár távoli elérést is lehetővé tesznek a felhasználók számára. Az irányító központ számítógépének kijelzőjét az 7. ábrán mutatom be.



7. ábra Az irányító központ kijelzője [10]

Ezzel a technikával a termelés teljes megfigyelését biztosíthatják a napok 0-24 órájában kényelmes keretek között. Ez azonnali beavatkozást tesz lehetővé, ami mind termelékenységi, mind biztonságtechnikai szempontból kedvező.

4. MAGYARORSZÁGI ENERGIAFÜGGŐSÉG CSÖKKENTÉSÉNEK KALKULÁCIÓJA A SZENNYVÍZTELEPI BIOGÁZ ÜZEMEK LÉTESÍTÉSE ÁLTAL

Magyarország energiafüggősége, az Európai Uniós átlagnál magasabb. Földgáz behozatali szükségletünk is meghaladja az éves felhasznált mennyiség 80%-át.[13] Ez olyan mérvű kiszolgáltatottságot ad országunknak, mely ellen folyamatosan keresni kell a megoldási lehetőségeket, és erre nyújthat egy alternatívát az összes keletkező szennyvízből (és megsemmisítendő szerves anyagú hulladékból) származó biogáz termelés.

A telep vonzáskörzetéből, 300.000 Lakos Egyenértékből éves szinten 8,6 millió m^3 biogáz keletkezik. Ez napi átlagban 23,56 ezer m^3 –t jelent. A biogáz tisztítása – azaz CO_2 és egyéb összetevők kivonása - nem okoz technológiai problémát. Így a folyamat eredményeként a földgázhoz hasonló, magas metántartalmú (kb. 98%) energiahordozót nyerhetünk. A kapott biometán a földgázzal megegyező energiaértékkel bír.

A keletkező biogáz metántartalmát átlagosan 60%-ra felvéve, és a 100%-os metántartalommal rendelkező földgázhoz vonatkoztatva elvégzem az egyenértékesűtísést. Tulajdonképpen meghatározásra kerül az, hogy mennyi „földgáz" keletkezik. Ezt pedig már tudjuk viszonyítani, az éves földgáz exportunkhoz. A számolás eredményeit az 1. táblázat tartalmazza.

Meg kell jegyezzem, hogy a fermentorok fűtéséhez nagy mennyiségű energia felhasználás szükséges, de mivel erre vonatkozóan pontos adatokkal nem rendelkezem, így ezt itt nem vettem figyelembe. A teljesen valós értékek meghatározásához viszont ezt nem lehet figyelmen kívül hagyni, csakúgy, mint a karbantartási és megvalósítási költségeket.

1. táblázat: Éves földgázimport csökkentésének kalkulációja a szennyvíziszapból termelt biogáz által hazánkban

	Dél-pest Szennyvíztelep	**Magyarország**
Lakos egyenérték [LE] 10^5	3	90
Termelt biogáz [m^3/nap] 10^4	23.56	706.86
Éves termelt biogáz [m^3/év] (átlag 60% metán) 10^6	8.6	258.0
Az éves termelt biogáz földgáz egyenértékűsítés [m^3/év] (100% metán) 10^6	5.59	167.7
5,7 milliárd m^3 földgáz export (2016) csökkentése [%]	0.098	2.942

Jól lehet a földgáz energiafüggőség csökkentésének értéke mindössze 3% körüli értékre adódik az alkalmazott fermentációs technológiával, de jelentősen védhetjük a környezetünket, hulladékot kezelünk és újrahasznosítunk.

5. A KOFERMENTÁCIÓ, MINT ENERGIABIZTONSÁG NÖVELŐ ELJÁRÁS

Különböző keverék anyagok (például a települési szennyvíziszap, mezőgazdasági, élelmiszeripari) közös rothasztásakor a biogáz képződés lényegesen javítható. A nagyobb szervesanyag koncentrációjú szubsztrát sokféleség hatására a rothasztó térfogata is jobban kihasználható

A kofermentációs eljárás során alapvető követelmény, hogy a hulladék ne legyen toxikus, hiszen az magát a lebontási folyamatot gátolná.

A beszállított hulladékok bevizsgálása speciális vizsgálatokat igényel, amelyek gyakran kifejezetten a hulladékok előtesztelésére alkalmasak. A különböző hulladéktípusok anaerob lebontásakor képződő biogáz metántartalma csak sok eszközt igénylő, bonyolult bonthatósági vizsgálatok során határozható meg. Ezen vizsgálatok elvégzése mind az időt, mind az anyagi ráfordítást tekintve gazdaságtalan. Kevés laboratórium vállal ilyen méréseket és drágán. Egy közös kísérlet alkalmával az Óbudai Egyetem és a Délpesti szennyvíztisztító telep együtt vizsgálta a telepre rendszeresen beszállított magas szervesanyag tartalmú hulladékok hatását azok rothasztására. (8. ábra)

Az egyetemen végzett kísérlet során több beszállított alapanyag biogázhozamát, és annak metántartalmát állapították meg.

8. ábra Az Óbudai Egyetem fermentációs reaktorai [10]

A szennyvíztisztítótelep laboratóriumában az OxiTop®-rendszerrel a homogenizált zöldhulladékból, a moslékból (étkezési maradék), burgonyapépből, papírhulladékból, sajtból (ömlesztett), lisztből, fűszenázsból (fűkaszálék), az egyetem laboratóriumában pedig Batch-rendszerrel cellulózból, élelmiszerszuszpenzióból, zsíriszapból, száraz kutyatápból készült szuszpenzióból („Csont 2") és vinaszból keletkező gázt vizsgáltak. [14]

Néhány alapanyag metántartalom eredményét ismerteti az 2. táblázat.

2. táblázat: Magas szervesanyag tartalmú hulladék típusok rothasztása során keletkezett biogáz %-os metántartalmának megállapítása laboratóriumi kísérlet elvégzése segítségével [14]

Szerves hulladék	**Metántartalom [%]**
Szennyvíziszap	60
Zsíriszap	66
Kutyatáp	80
Moslék	75
Élelmiszer szuszpenzió	72
Sajt	67

A táblázatból kiolvasható, hogy a szennyvíziszap 60%-os metántartama alatta marad hozzákevert kísérleti anyagok metántartalom értéke alatt .

A kísérlet eredményei alapján azt a következtetést vonhatjuk le, hogy a szennyvíziszap mellé betáplált, hulladékként definiált alapanyagok ezirányú energetikai hasznosítása nagy perspektívát jelenhet a rothasztás során nyert energiahordozó kapcsán.

6. Következtetés

A bevezetésben célul tűztem ki, hogy a Dél-pesti Szennyvíztisztító telep működésének eredményeit felhasználva, megvizsgálom, hogy egy ideális szennyvíztisztítási rendszerben, ahol az összes lakossági szennyvíztisztítás során keletkező biogáz hasznosításra kerül, az milyen hatással lehet az energia biztonságra.

Közelítő számításaim alapján ez – a hazai adatokra számítottan - közel 3%-os földgáz export csökkenést okozhat. Ez olyan mértékű, ami megfontolást igényel, főleg egy olyan nagy energiafüggőséggel rendelkező ország számára, mint hazánk.

További lehetőségeket rejt a szennyvíztelepek esetében a kofermentáció. A magas szervesanyag tartalmú – a megsemmisítés céljából – beszállított hulladékanyagok és a szennyvíziszap együttes rothasztása jelentősen javíthatja az üzem hatékonyságát. A biogáz hozam növelése és a kapott gáz %-os metántartalmának növelése biztosítja az előállított energiahordozó értékének növelését. Ezzel tovább csökkenthető az általam korábban számított hazai export energia igény is, ahol átlag 60%metántartalomat vettem alapul.

Ugyanakkor a szennyvíztelepi kofermentáció biztos alkalmazására körültekintő előzetes vizsgálatokra van szükség. Az egyes alapanyagok anaerob fermentációra tett hatásának pontos megállapítására laboratóriumi, félüzemi, majd több éves üzemi kísérletekre van szükség.

De a távoli jövőben megoldásként felmerülhet, mint alternatív energiatermelési lehetőség, például egy idegen bolygón kialakítandó űrtámaszpont számára.

Köszönetnyilvánítás

Szeretném megköszönni a Fővárosi Csatornázási Művek Dél-pesti Szennyvíztisztító telep munkatársainak – Kulcsár Zoltán technológusnak és Bezsenyi Anikó mikrobiológusnak, - hogy segítséget nyújtott a tanulmány elkészítésében.

Irodalomjegyzék

[1] http://fcsmzrt.hu/hu/kereses/?q=40+ezer+biog%C3%A1z
letőltés ideje: 2017. Szeptember 11.

[2] www.biogas.hu.
letőltés ideje: 2017 Július 1.

[3] Bai Attila (szerk.): A biogáz, Száz Magyar Falu Könyvesháza Kht., 2007

[4] http://www.szegedivizmu.hu/ceginformacio/tevekenysegi_kor/biogaz_termeles_es_hasznositas/
letőltés ideje: 2017. Január 10.

[5] Dr. Hajdú József: Biogázüzemek Magyarországon, 2012 http://agraragazat.hu/cikk/biogazuzemek-magyarorszagon
letőltés ideje: 2016. Október 4.

[6] https://www.zalaviz.hu/index.php/rolunk/szennyviz-elvezetes
letőltés ideje: 2017. December 8.

[7] Az anaerob iszapkezelésben rejlő eneegia-termelés és hasznosítási lehetőségei Palkó györgy
http://docplayer.hu/7860879-Az-anaerob-iszapkezelesben-rejlo-energia-termelesi-es-hasznositasi-lehetosegek-palko-gyorgy-olah-jozsef-szilagyi-mihaly-fcsm-rt.html
letőltés ideje: 2017. November 1.

[8] http://www.fcsm.hu/szolgaltatasok/szennyviztisztitas/delpesti_szennyviztisztito_telep
letőltés ideje: 2017. November 1.

[9] https://www.google.hu/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjAoIW8kcXYAhXKaFAKHeSpAMIQjRwIBw&url=https%3A%2F%2Forientpress.hu%2Fcikk%2Fnyilt-nap-a-del-pesti-szennyviztisztito-telepen&psig=AOvVaw0mXVNA0bBuKPU03fRdZYpt&ust=1515389742516784
letőltés ideje:2018. Január 8.

[10] A szerző saját felvétele
A kép elkészítésének helye: A Dél-pesti Szennyvíztisztító Telep1238 Budapest, Meddőhányó u. 1
A kép elkészítésének ideje: 2017. Junius

[11] Garai György: Szennyvíztistító telepek energiakérdései, energiaellátás és automatizálás kapcsolata A Magyar Szennyvíztechnikai Szövetség Lapja 2006, November-December pp 3-7.
http://docplayer.hu/3989105-Hir-csatorna-tartalom.html
letőltés ideje:2017. December 1.

[12] Növekedett Magyarország földgázbehozatala , Magyar Nemzet, Gazdaság, 2017.
https://mno.hu/gazdasag/novekedett-magyarorszag-foldgaz-behozatala-2402102
letőltés ideje: 2017. június 6., kedd 18:05, frissítve: kedd 18:31

[13] Bakosné Diószegi Mónika: A magyarországi energiabiztonság növelésének okai In: Dr Csibi Vencel-József (szerk.) OGÉT 2013 XXI Nemzetközi Gépészeti Találkozó. Konferencia helye, ideje: Arad, Románia, 2013.04.25-2013.04.28. Kolozsvár: Erdélyi Magyar Műszaki Tudományos Társaság (EMT), pp. 28-31.

[14] Csibrik Enikő: Nagy szervesanyag-tartalmú hulladékok előzetes felmérése biogázüzemekben
Óbudai Egyetem Rejtő Sándor Könnyűipari és Környezetmérnöki Kar, Környezetmérnöki Intézet Szakdolgozat, Budapest, 2017.

A személy- és vagyonbiztonság adaptálása korunk kihívásaira

Adaptation of the Safety of Persons and Property for Current Challanges

Szakali Miklós
Óbudai Egyetem, Budapest, Magyarország
mszakali@hotmail.com

Összefoglalás

Napjaink megváltozott biztonsági körülményei szükségessé teszik a széleskörű összefogást az emberi élet, a kultúránk, hagyományaink és életstílusunk védelmében. Az állampolgárok védelme alapvetően állami feladat, amelyet a hivatalos szervek látnak el, azonban nem mondhatunk le a civil személy- és vagyonbiztonság területén meglévő képességekről sem biztonságunk fokozása érdekében. Véleményem szerint csak akkor érhetünk el tartós eredményeket, ha a biztonsági kihívások legveszélyesebb formáit, a terrorizmust és a hibrid hadviselés hasonló elemeit komplex módon kezeljük és felhasználunk minden rendelkezésre álló forrást a támadások megelőzésére, elhárítására, illetve esetleges következményeinek kezelésére.

Cikkemben azt vizsgálom, hogyan lehetne a civil személy- és vagyonbiztonság elemeinek fejlesztésével, illetve az elemek közötti együttműködés javításával növelni biztonságunkat valamint segíteni a hatóságok terrorelhárító tevékenységét egy komplex biztonsági hálót létrehozásával.

Kulcsszavak: *biztonsági környezet, személy- és vagyonbiztonság, terrorizmus, biztonsági rendszer, együttműködés*

Abstract

Nowadays the changed security environment makes it necessary to introduce wide range of cooperation in order to defend our life, culture, traditions and general lifestyle. It is basically a state-responsibility to defend its citizens with the assigned authorities; however, in favour of our enhanced security we cannot exclude those capabilities which exist at the civil security services. I think that we can only achieve firm results against the most dangerous forms of the current security challenges – terrorism and the similar elements of the hybrid warfare - if we treat them in a complex way using all the available resources to prevent and to defend against attacks or to manage the consequences of an eventual event.

In this article I examine the possibilities how we can develop some elements of the safety of persons and property and to increase the cooperation among them in order to enhance our security and to assist anti-terrorism activities of the authorities contributing to a complex security system.

Keywords: *security environment, civil security and safeguarding, terrorism, security system, cooperation*

1. BEVEZETÉS

A személy- és vagyonbiztonság kiterjedt felelősségi kört foglal magában, a témakörbe tartozik a természeti jelenségek (vihar, eső stb.) által, továbbá az emberi hibából vagy véletlen meghibásodásból bekövetkező események (tűz, robbanás, gázömlés, egyéb ipari katasztrófa, stb.) elleni védelem is. Ezek az események is veszélyeztethetik az ott tartózkodó személyek életét, testi épségét, egészségét, valamint anyagi kárt okoznak a tulajdonban is. Ebből adódóan a személy- és vagyonbiztonsági rendszer egyik feladata, hogy ezeket is megelőzze, elhárítsa, vagy káros hatásait mérsékelje, enyhítse. Azonban cikkemben csak a megváltozott biztonsági környezet néhány eleméből következő, a személyes biztonságra veszélyes szándékos emberi tevékenység elleni megelőzés és védelem kérdéseivel foglalkozom.

Napjainkban jelentősen megváltozott a biztonsági környezet, amely hatással van mindennapi életünkre és biztonságunkra is. Eddig főleg a vagyon elleni cselekmények voltak a meghatározóak, amelyek ellensúlyozására létrejöttek a különböző civil biztonsági, őrző-védő vállalkozások. Ugyan az illegális anyagi haszonszerzésre való törekvések indokolttá teszik a civil biztonsági vállalkozások hagyományos alkalmazását, azonban világszerte megjelent a személyes biztonságra sokkal veszélyesebb jelenség, a terrorizmus. Magyarországon ugyan még nem történt a nyugat-európai támadásokhoz hasonló esemény, de véleményem szerint időben fel kell készülni annak megelőzésére és esetleges következményeinek kezelésére. Cikkemben azt vizsgálom, hogy jelenleg működő személy- és vagyonbiztonsági rendszer egyes elemeit hogyan lehet adaptálni annak érdekében, hogy növelje az állampolgárok személy- és vagyonbiztonságát, valamint valós segítséget nyújtson az állami szerveknek a terrorizmus elleni harcban. Véleményem szerint nem szabad egy kiképzett, őrzés-védelmi tapasztalatokkal rendelkező jelentős létszámú civil állományt figyelmen kívül hagyni, amikor emberéleteket veszélyeztető cselekményekkel szemben kell fellépni és biztonságunkat szavatolni.

2. A BIZTONSÁGI KÖRNYEZET VÁLTOZÁSA

A biztonság köznapi értelmezése kapcsán mindenki saját életének egy-egy területére (anyagi, egzisztenciális, egészségügyi, baleseti, stb) gondol, amely által leginkább veszélyeztetve érzi személyes életét, biztonságát. A felsorolt néhány példából is kellően érzékelhető, hogy a biztonság minden esetben egy állapotot takar, egy olyan állapotot, melyet esetenként valami más és más dolog veszélyeztet. A biztonság tehát csak valami veszélyeztető tényezővel együtt értelmezhető.

A biztonságot közvetlenül két tényező határozza meg. Az egyik a veszélyeztetés, azaz a szándékos jogellenes magatartások, melyek negatívan befolyásoljak a biztonságot. A másik az alkalmazott védelmi erőforrások mennyisége és minősége. Minél nagyobb erőt, hatékonyabb őrzést és védelmet alkalmazunk, annál nagyobb biztonságot érhetünk el. Ugyanis az alkalmazott védelmi erőforrások a szándékos jogellenes magatartásokkal szemben hatnak, azt akadályozzak. Azonban tudatában kell lennünk, hogy maximális törekvéseink ellenére sem érhetünk el teljes körű, abszolút biztonsági állapotot. [1]

A rendszerváltás következtében Magyarország társadalmi és gazdasági berendezkedése jelentős változáson ment keresztül. Megszűnt a társadalmi tulajdon, a tervutasításos gazdasági rendszer helyét átvette a magántulajdonra épülő piacgazdaság. A privatizációs folyamatok következtében a társadalmi tulajdon szerves részét képező vagyontárgyak (termelőüzemek, gyárak, épületek, stb.) ismét magántulajdonba kerültek. A Polgári Törvénykönyv szerint pedig a tulajdonos egyik alapvető joga a birtokvédelem. Így a magántulajdon növekedésével természetes módon felmerült az igény ennek külső személlyel, szervezettel történő megvédésére is, mert erre a tulajdonos önmagában már nem képes. Ráadásul a privatizáció következtében sok munkahely megszűnt, nőtt a munkanélküliség, a megnövekedett magántulajdon pedig csábító lehetőségnek tűnt a kieső jövedelem illegális pótlására, ami a vagyon elleni jogsértések számának ugrásszerű növekedéséhez vezetett.

A kisebb tulajdon elleni jogsértések mellett, ebben az időszakban jelentek meg hazánkban a szervezett bűnözés első jelei is. Több esetben fordultak elő robbantások, lövöldözések, maffia jellegű leszámolások a nyílt utcán. Az világosan látszott, hogy a megváltozott társadalmi berendezkedésben az államnak a belső rend, közbiztonság fenntartása is nehézségeket okoz, így – megfelelő kapacitás hiányában – nem tudja és nem is akarja a személy- és vagyonvédelmi feladatokat teljes körűen ellátni. Az egyéneknek viszont a személyiségfejlődés során kialakul a biztonság iránti igénye, amit az államtól nem kaphattak meg. Így a megfelelő tőkével rendelkező magánszemélyek és a gazdasági élet különböző szereplői között felmerült az igény arra, hogy személyük és értékeik védelméről a privát szférán belül, magánjogi jogviszony keretében gondoskodjanak. Így alakultak ki - és működnek az óta is - hazánkban a vagyonvédelmi vállalkozások.[2]

Mint látjuk egy gyökeres belpolitikai-társadalmi változásra való reagálás volt a magán biztonsági, személy-, és vagyonvédelmi szektor kialakulása, amely tevékenységét a megváltozott biztonsági körülmények és a fizetőképes biztonsági igények határoztak meg.

Napjainkban ismét tanúi és részesei lehetünk egy gyökeresen változó biztonsági környezetnek, amely alapjaiban fenyegeti személy- és vagyonbiztonságunkat. Sajnos a fenyegetettek körét nem lehet társadalmi, gazdasági és egyéb egzakt jellemzők alapján behatárolni, mivel a fenyegetés sokkal általánosabb és kiszámíthatatlanabb. Ezt az általános fenyegetést a terrorizmus és a hibrid hadviselés egyes elemei jelentik, melyek jól érzékelhető félelmet és bizonytalanságot keltenek a lakosság körében. Az egyre pusztítóbb terrorista merényletek jelentik az első számú fenyegetést a polgári lakosság élet-, és vagyonbiztonságára világszerte. Természetesen Európa sem kivétel ez alól, itt sem érezheti magát biztonságban senki sem, mivel ezek a támadások mindennapi életünk általános színtereit veszik célba, amelyeket mindannyian használunk. A továbbiakban bemutatok néhány olyan eseményt, amelyek alapján könnyen belátható, hogy meghatározó változások történtek a biztonsági környezetben, amelyek szükségessé teszik a személy- és vagyonvédelem, valamint a polgári biztonsági szakma alkalmazkodását is a megváltozott körülményekhez a társadalom biztonsági igényeinek kielégítése érdekében.

A terrorizmus lényegéből adódik, hogy a terroristák az úgynevezett könnyű célpontokat részesítik előnyben. A támadások főleg a fegyvertelen, védekezésre felkészületlen éppen ezért arra képtelen nagy létszámú csoportokat veszik célba, amelyek esetében jelentős személyi áldozat és anyagi károkozás várható. A támadások legnagyobb hatása – talán a konkrét merényleteknél is nagyobb - a csoportos félelem, a tehetetlenség érzése és a pánik, amelyek az agressziót követően átjárják az embereket és tudatosul bennük, hogy ez velük is bármikor megtörténhet és ők védtelenek ezzel szemben.[7; 16-35. o.]

Röviden felidézek néhányat a közelmúltban történt támadások közül ezzel is érzékeltetve, mennyire kiszámíthatatlan és reális veszély egy terrortámadás:

2013. április 15-én a Boston Marathon futóverseny résztvevői és nézői ellen két robbantásos merényletet követtek el. Öt ember életét veszítette, 280 személy megsérült.

2014. május 24-én Brüsszelben egy fegyveres személy tüzet nyitott egy múzeumnál meggyilkolva három embert, illetve súlyosan megsebesített egy negyediket.

2015. január 7., Párizs – Terrortámadás a Charlie Hebdo szerkesztősége ellen. Két fegyveres 12 embert, köztük 2 rendőrt agyonlőtt, társaik január 8-án megöltek egy rendőrnőt és 4 túszt egy kóser boltban.

2015. június 26., Szúsza (Tunézia) – Tengerparton pihenő turistákat támadtak meg és 39 vendéget lőttek agyon, 40 személyt megsebesítettek.
2015. november 13., Párizs – 150 halálos áldozatot követelt a terrortámadás-sorozat, 200 ember megsérült, köztük 80-an súlyosan. A nyolc terrorista – AK–47-es gépkarabélyokkal és testükre erősített bombákkal támadott. 112 emberrel végeztek a XI. kerületi Bataclan koncertteremnél az Eagles of Death Metal koncertjén. További öt helyszínen érte támadás a francia főváros lakóit és a turistákat: a La Belle Équipe kávézóban, a Le Carillon bárnál, a Bonne Bière kávézóban, Petit Cambodge étteremben, illetve a Comptoir Voltaire bárban, itt összesen 38 ember vesztette életét.
2016. március 22., Brüsszel – 34 halálos áldozatot és több mint 200 sérültet követelő merényletsorozat. Reggel 2 robbantás (és egy besült) történt a brüsszeli Zaventem reptéren, később pedig az Európai Parlamenttől nem messze lévő metróállomáson történt egy robbanás.

Amíg a terrortámadás főleg a szélsőséges vallási-, és politikai csoportokhoz és szervezetekhez köthetők, addig a másik fő veszélyforrás, a hibrid hadviselés az államok hadviselési eljárása. Lényege, hogy egy adott közösség minden elemét (politikai, gazdasági és társadalmi) támadja a kormányzati és rendfenntartó szervek megbénítása, a törvényes rend szétzilálása, valamint a társadalmi feszültségek és bizalmatlanság keltése érdekében.

A hibrid hadviselés [8; 120-137. o.] eszköztárából két elemet emelek ki, amelyek különösen alkalmasak a fenti hatások elérésére. Az egyik az információs műveletek, amelyek által megtévesztő információkat sugároznak a kiválasztott célcsoport felé, elégedetlenséget, haragot és félelemérzetet keltve a célcsoportban. Ezzel is bizalmatlanságot ébresztve a kormányzati, rendfenntartó szervekkel vagy más társadalmi csoportokkal szemben, amely akár erőszakos cselekményekhez is vezethet.

A másik fő elem pedig a helyi szimpatizáns csoportok (proxik) alkalmazása, amelyek akár terrorista jellegű támadásokkal, akár erőszakos, köztörvényes bűncselekményekkel keltenek félelmet a kiválasztott célcsoportban vagy a lakosság szélesebb köreiben, megkérdőjelezve a rendfenntartó szervek alkalmasságát, aláásva a lakosság és a hivatalos szervek kapcsolatát. Nem ritka, hogy a proxi csoportok kiképzésére és a felforgató műveletek irányítására a szembenálló fél reguláris erőit, különleges műveleti csoportjait vetik be.

Mint látjuk mind a terrorizmus, mind a hibrid hadviselés egyes elemei valós fenyegetést jelentenek élet- és vagyonbiztonságunkra. Ez elöl a fenyegetés elől nem térhetünk ki, mivel az életformánkat, illetve annak általános szintereit vették célba, amelyek feladása történelmünk, kultúránk és identitásunk feladását jelentené. Nem tehetünk mást, hatékony választ kell adnunk ezekre a biztonsági kihívásokra alapvető értékeink szem előtt tartásával.

A fenti külföldi példák alapján bárki megkérdezheti, hogy miért foglalkozunk ezzel a témával, amikor Magyarország nem érintett benne. Célszerűbbnek tartom időben megtenni a szükséges intézkedéseket és felkészülni egy esetleges esemény bekövetkezésére, mint tétlenül várni és utólag bánkódni az – egyébként talán elkerülhető- veszteségek miatt.

3. A BIZTONSÁGI HÁLÓ KITERJESZTÉSE

A biztonsági környezet változásával tudomásul kell vennünk, hogy a biztonság szavatolásának személyi, jogi és eszközrendszere is változni fog. Lényeges, hogy a jogellenes magatartások elleni fellépés továbbra is alapvetően állami feladat marad és ezt az államilag intézményesített szervek: rendőrség, nemzetbiztonsági szolgálatok, ügyészség, bíróságok stb. végzik.

Annak ellenére, hogy Magyarországon eddig nem történt a fenti példákhoz hasonló támadás az Országgyűlés 2016. júliusában elfogadta az Alaptörvény módosítását, amelyben a terrorveszélyhelyzetet beemelte az Alaptörvény 51/A cikkeként. [3] A törvény felhatalmazza a Kormányt a sarkalatos törvényben meghatározott rendkívüli intézkedések bevezetésére, valamint lehetővé tette a Magyar Honvédség hazai alkalmazását terrorveszélyhelyzet idején, ha a rendőrség és a nemzetbiztonsági szolgálatok alkalmazása nem elegendő. Tehát a magyar politikai vezetés is elég fontosnak ítélte a terrorizmus kérdését ahhoz, hogy módosítsa az Alaptörvényt és lehetővé tegye a Honvédség alkalmazását. Ez azért jelentős, mivel a Magyar Honvédség alapvető feladataként az ország függetlenségének, területi épségének és határainak katonai védelme volt meghatározva nem pedig a közbiztonság és közrend fenntartása, illetve helyreállítása.

Ugyanakkor azt is könnyű belátni, hogy minden kulturális és szórakoztató intézmény biztonságát nem felügyelhetik az állami szervek és a közelmúlt eseményei tükrében a népszerű szórakozóhelyek potenciális veszélyeztetettsége megnőtt. Amíg az eddig veszélyeztetettségi értékelések szerint az éttermek, kávézók, színházak nem igényeltek őrzés-védelmet, addig ez a fenti példák alapján jelentősen megváltozhat.

Szükségesnek tartom növelni a kulturális, sport és egyéb szórakozóhelyek biztonságát, azonban természetesen nem lehet azonos elvárásokat támasztani minden, a fenti kategóriába tartozó intézménnyel szemben. Itt látok lehetőséget az állami és a civil biztonsági szolgálatok és szervezetek szakmai bevonására az egyes intézmények (objektumok) biztonsági kockázatának meghatározásában és az arányos őrzés-védelmi rendszer kialakítására való javaslattételben. Ezt a tevékenységet a tulajdonossal együttműködésben, annak érdekeltté tételével tudom csak elképzelni, egyébként ellenkezést és ellentétes hatást válthat ki.

Úgy gondolom, hogy a fenti objektumok biztonságának fokozása érdekében sincs szükség az objektumőrzés és védelem kapcsán megfogalmazott klasszikus elvi megközelítés és eszközrendszer felülírására.

Jelenleg is helytállónak tartom azt a meghatározást, miszerint *„ Az objektumőrzés egy olyan folyamatos vagyonbiztonsági tevékenység, mely során élőerővel és technikai eszközökkel, valamint rendszabályokkal késleltetik, esetleg megakadályozzák az objektum rendeltetésszerű működését, illetve a vagyont veszélyeztető szándékos jogellenes magatartás bekövetkeztét, es ha szükséges biztosítják az objektumvédelem sikeres végrehajtását."*[1; 96-97. o.] Azonban fontosnak tartom az eszközrendszer minőségi fejlődését követni és a jelenlegi helyzethez igazítani.

A nemzetközi védelmi ipar foglalkozik a kihívással, illetve az ikertornyok-, majd pedig a közelmúltban Franciaországban elkövetett terrorcselekmények után új lendületet vettek az intelligens kamerarendszer [4] fejlesztések és telepítések. Ezek a fejlesztések különösen fontosak, mivel nem csak az események rögzítését teszik lehetővé, de jogellenes cselekmények felismerésére és megelőzésére is nagyobb esélyt adnak.

Példaként néhány a teljesség igénye nélkül:

– Viselkedés elemző algoritmus.

Magasabb kockázati kitettségű területeken célszerű olyan okos rendszerek telepítése, amelyek a szokatlan/nem életszerű magatartásokat képesek detektálni. A technológia azonnal figyelmeztet, ha valaki lerakja és ott hagyja a kézi-, vagy hátizsákját, de a hirtelen irányváltás, és bármilyen feltűnő viselkedés azonnal az operátor látókörébe hozhatja a célszemélyt.

– Testhőmérséklet változások kiszűrése.

A Francia Állami Vasúttársaság (SNCF) kísérleti jelleggel már rendszerbe állított intelligens kamerarendszereket megelőzése céllal.

– Arcfelismerő algoritmus.

A hatóságok által előre beprogramozott képi információk alapján a technológia körözött bűnözőket, illetve már nyilvántartásba vett terroristákat is képes beazonosítani.

– Mobil arcfelismerés.

Már egy IPhone készülékre telepített "szkenner" is megjelent, amely képes a szem, arcvonások, hang és ujjnyomat azonosítására. A rendőri erők egyszerűen és gyorsan képesek ellenőrizni, hogy az adott személy szerepel-e a bűnügyi/körözési nyilvántartásban.

A példák alapján láthatjuk, hogyan fejlődik a biztonságtechnikai feltételrendszer, azt azonban talán még fontosabbnak tartom, hogy a high-tech eszközök ne elszigetelten működjenek, hanem rendszerbe foglalva biztosítsák az időbeni információáramlást és ezzel a lehetőséget a beavatkozásra és az esemény megelőzésére.

A legintelligensebb kamera sem hasznos, ha nem megfelelően helyezik el, ha nem továbbít - vagy nem a megfelelő helyre – információt és nem kapcsolódik egy reagáló erőhöz. Ezért nélkülözhetetlennek tartom a technikai eszközök hálózatban történő alkalmazását és egy műveleti központba (állami vagy civil) történő bekötését. Ennek azonban előfeltétele az interoperabilitás kialakítása, amely magában foglalja az azonos alkalmazási elveket, az eszközök kompatibilitását, az operátorok azonos követelmények szerinti felkészítését és egy egységes eljárási (riasztási, döntéshozatali, beavatkozási) protokoll alkalmazását.

A technikai feltételrendszer mindig csak a lehetséges megoldás egyik oldalát jelenti, ugyan is a legfejlettebb technika sem nélkülözheti az emberi szakértelmen és tapasztalatokon alapuló döntéshozatalt. Optimális helyzetnek az ember (élőerős) és technika egymást kiegészítő alkalmazását tekinthetjük.

Az interoperabilitás megteremtését a személyi állomány kiválasztása, oktatása – kiképzése és alkalmazása során is szem előtt kell tartani. Ezért egységes követelményrendszer szükséges a kiválasztás, valamint az oktatás-képzés, továbbképzés területén is. A legkiválóbb egyéni képességekkel rendelkező személy- és vagyonőr is csak elriasztja a gyanús egyéneket vagy idő előtti cselekvésre készteti őket, ha egyedül próbál megoldani egy speciális szakértelmet és csapatmunkát igénylő helyzetet. Így csak a növeli a kockázatot és veszélyezteti saját és munkatársai valamint az objektumban tartózkodók testi épségét és életét.

Eddig az objektumok őrzésébe és védelmébe bevonható civil őrző-, védő vállalkozások technikai és élőerejének, interoperabilitásának és hálózatban történő alkalmazásának lehetséges előnyeit vizsgáltam. Azonban a lényegi előrelépést az állami szervek (rendőrség, TEK, nemzetbiztonsági szolgálatok, stb) és a civil biztonsági cégek szabályozott együttműködése, a biztonsági háló kiterjesztése jelenthetné.

Figyelembe kell venni, hogy nagy tapasztalat és komoly tudásanyag halmozódott fel az elmúlt évek során a személy- és vagyonvédelem körében, amelyre alapozva és azt kiegészítve meg lehet találni a megoldást az új biztonsági kihívás kezelésére. Véleményem szerint meg kell fontolni a személy- és vagyonvédelmi szakma bevonását a terrorizmus elleni megelőző és következménykezelési feladatokba.

A terrorelhárítás állami feladat, amelynek megvannak a megfelelően széles jog- és hatáskörökkel ellátott szervei, azonban még így is képtelenség teljes körű biztonsági hálót létrehozni. Egyrészt szükség van a különböző állami szervek (rendőrség, nemzetbiztonsági szolgálatok, stb) együttműködésére ugyanakkor nem engedhető meg az a luxus, hogy egy szakmailag képzett, jelentős tapasztalattal és eszközrendszerrel bíró civil őrző-védő állományt nem vonunk be mindannyiunk biztonságának szavatolásába. Ilyen pusztító következményekkel járó fenyegetettség ellensúlyozására szükség van egy összefüggő biztonsági háló kiépítésére, amelynek az állami szerveken kívül a személy- és vagyonvédelemi szakma is részét képezi.

Egy közös koncepció alapján szervezett biztonsági háló lényegesen nagyobb lefedettséget biztosítana, illetve a szabályozott és célirányos információáramlás nagyban hozzájárulna a hatékonyság növeléséhez. A civil biztonsági cégek jelentős támogatást nyújthatnának a technikai eszközeik és az információszolgáltatás célirányos biztosításával az állami szervek tevékenységéhez. A civil személy- és vagyonvédelmi

szakma bevonása a biztonsági feladatok szélesebb körű kezelésébe nem példa nélküli, mivel az USA-ban a 9/11-es terrortámadásokat követően bevonták a civil biztonsági szervezeteket is a terrorizmus elleni feladatokba főleg a megelőzés, valamint a következmények kezelése területén.

Visszatérve a javaslatra el kell ismerni, hogy ez egy kényes sok vitát kiváltó kérdés, milyen mértékben lehet bevonni és milyen jogosultságokkal lehet felruházni civil személy- és vagyonvédelmi cégeket, úgy, hogy az valóban hatékony legyen és erősítse a biztonságot, ugyanakkor ne jelentsen indokolatlan jogi felhatalmazást, amely alkalmas ad visszaélésekre és a személyiségi jogok megsértésére.

A 2005. évi CXXXIII. törvény [5] (a továbbiakban: Vagyonvédelmi törvény) szigorú személyi követelményeket és foglalkozási titoktartási kötelezettséget fogalmaz meg a személy- és vagyonőri tevékenységet végzőkkel szemben, amelyek alapját képezhetik egy ilyen bizalmai feladatrendszerben való részvételnek. Mindezek nem azt jelentik, hogy a törvény ezen rendelkezéseit nem lehetne felülvizsgálni és még jobban a feladathoz igazítani beleértve a rendszeres időközönként történő hatósági ellenőrzéseket is.

A lehetséges együttműködés és a jogkörök bővítésének vékony határvonalát gondosan kell szabályozni a későbbi zökkenőmentes gyakorlati alkalmazás érdekében, ugyanakkor állampolgári oldalról is nagyobb társadalmi elfogadottságra és személyes belátásra van szükség saját biztonságuk védelme érdekében. A társadalmi elfogadottságot jelentősen elősegíthetné egy átgondolt kommunikációs stratégia, valamint a tényszerű, rendszeres tájékoztatás és a lakosság szélesebb rétegeit megszólító figyelemfelkeltő, oktató, bemutató programok és előadások.

A tevékenység jogi kereteinek meghatározása ugyan alapvető fontosságú, azonban ennél összetettebb feladatról van szó. Először a szakmai alapokat kell meghatározni, amely átfogja a teljes tevékenységet, beleértve a személyi állomány kiválasztási, képzési és foglalkoztatási követelményeit, az alkalmazható mechanikai és elektronikai eszközök, valamint az eljárások körét és rendjét csakúgy, mint az állami és a civil szervek közötti együttműködés szabályait. A szakmai alapok kidolgozását követően lehet azokat jogszabályi szintre emelni.

Felvetődik az a kérdés is, hogy mennyiben igényel más megközelítést egy terrortámadás megakadályozása vagy kivédése, mint személy- és vagyonvédelem témaköréhez kapcsolódó jogellenes tevékenységek elhárítása. A válasz elég egyszerű, a személy- és vagyonvédelemhez köthető tevékenységek alapvetően egy objektum, vagyontárgy vagy egy meghatározott személy, csoport őrzésére-védelmére koncentrálnak.

Ezt a feladatot akár fegyvertelenül, határozott fellépéssel, meggyőzéssel vagy társak segítségül hívásával is végre lehet hajtani. Még egy fegyveres rablótámadás esetén is az anyagi haszon megszerzése a cél, melynek az elérését az áldozatok ejtése csak megnehezítené és súlyosbítaná a cselekmény büntetőjogi megítélését. A terrorista célja viszont az azonnali és általános pusztítás, nem anyagi haszonszerzés és nem feltétlenül egy konkrét személy vagy csoport megtámadása vezérli, hanem a sok áldozattal járó, brutalitásával és könyörtelenségével megdöbbenést és félelmet okozó, nagy médiafigyelmet vonzó gyilkolás.

Éppen ezért a fenti példák is mutatják, hogy a fegyveres terrortámadásokat a biztonsági személyzet – már, ahol volt – nem tudta megakadályozni vagy elhárítani. Legjobb esetben is csak a megtámadottak menekítését, rejtését-bújtatását tudták segíteni.

Ezek alapján levonhatjuk a következtetést, hogy bár a terrortámadás elhárításának céljai összhangban vannak a személy- és vagyonvédelem céljaival, vagyis:

- a személyek személyes biztonságának,
- a személyek, szervezetek jogos érdekeinek,
- a személyek, szervezetek jogos tulajdonát, vagy ezek kezelésében, használatában levő más vagyontárgyak megóvásával, azonban a célok azonossága önmagában nem segíti elő egy terrortámadás sikeres megakadályozását vagy elhárítását.

Speciális eszközrendszerre, ismeretekre, kiképzésre és eljárásrendre van szükség ahhoz, hogy egy civil cég emberei a siker reményében vehessék fel a harcot egy támadással. Pontosabban fogalmazva a célnak a támadás megelőzésének kell lennie, egyébként – különösen fegyvertelenül – nagyon kevés esély van egy terroristák semlegesítésére és így a túlélésre is.

Elgondolásom szerint - a teljesség igénye nélkül - a következő szakterületekre és témakörökre terjedhet ki az együttműködés:

1. Szakképzés (a Vagyonvédelmi törvény szerint a kamara feladata, de az együttműködés szükségszerű)
   - a terrorveszély megelőzése, reagálás és a következmények kezelése támadás esetén témakör bevezetése képzési tárgyként,
   - az elméleti és gyakorlati anyagok kidolgozásához szakmai útmutatás biztosítása,
   - a „train the trainer” elv jegyében elméleti és gyakorlati felkészítés biztosítása a civil oktatók részére,
   - alkalmanként oktatók-kiképzők biztosítása,
   - a képzés ezen részének szakmai ellenőrzése,
   - elméleti és gyakorlati továbbképzés az időszerű változások bemutatására.
2. Szaktanácsadás
   - a veszélyeztetettség felméréséhez, elemzéséhez,
   - a biztosítás, őrzés-védelem megszervezéséhez,
   - az élőerő célszerű felállítási helyéhez és tevékenységéhez,
   - a mechanikai eszközök és elektronikai jelzőrendszerek elhelyezéséhez, működtetéséhez, álcázásához,

- az adott helyszínre jellemző eljárási protokoll kidolgozásához.

3. Műveleti együttműködés

- az információcsere és megosztás rendjének és szabályainak kidolgozása,
  - kőrözött, vagy terroristagyanús személyek fényképe, személyleírása,
  - az objektum felmérésére, a biztonsági rendszer felderítésére utaló jelek, magatartás,
  - a biztonsági személyzet vagy rendszer tesztelésének gyanúja,
  - a biztonsági személyzet kommunikációs és informatikai felszerelése iránti érdeklődés.

4. JOGI SZABÁLYOZÁS AKTUALIZÁLÁSA

Az előző fejezetben hivatkoztam a Vagyonvédelmi törvényre, amellyel az állam beavatkozik a biztonságvédelembe úgy, hogy meghatározza az állami és a civil szereplők kapcsolatát és feladatait. Ez egy határvonal meghúzását jelenti, amelyen belül bizonyos fokú szabadságot biztosít a magánbiztonság védelmére, amíg az nem zavarja az állam működését.

Tekintve, hogy egy 12 éve hatályban lévő törvényről van szó, miközben a biztonsági környezet lényegesen megváltozott, úgy gondolom, hogy a vagyonvédelmi törvény aktualizálását is úgy kell végrehajtani, hogy az adekvát kereteket biztosítson a korunk legnagyobb kihívásainak kezelésére.

Nagyobb hangsúlyt kell, hogy kapjon a személyes biztonság védelme, mint az anyagi javak védelme. Figyelembe véve a közelmúlt terroreseményeiről szóló rövid felsorolást megfontolandónak tartom kötelezettségként előírni a bizonyos vendégszám (20-50?) fölötti befogadásra képes kulturális- és szórakozóhelyek részére a látogatók személyes biztonságáról való gondoskodást.

Bár a törvény egy helyen (31. § (3) bekezdés b) pontja) megemlíti a terrorcselekmény és közveszélyokozás megelőzését, de csak a rögzített kép- és hangfelvételek megsemmisítésével kapcsolatban, amelyet a rögzítést követő 30 nap eltelte után határoz meg. Ugyanakkor különösnek találom, hogy a vagyonvédelmi céllal készült kép- és hangfelvételek megsemmisítési határideje a rögzítéstől számított 60 nap eltelte. Vagyis fontosabbnak tekinti a vagyonbiztonságot, mint a személyi biztonságot.

Álláspontom szerint külön fejezetet kell szentelni a terrorveszély megelőzésének, esetleges támadás bekövetkezése esetén való tevékenységnek és következmények kezelésének. Ez a fejezet alapvetően a megelőzésre fókuszálna, szabályozná az állami szervekkel való együttműködés rendjét a felek jogosultságait és kötelezettségeit, valamint a tevékenység ellátásának főbb kereteit és szabályait.

Fontosnak tartom megjegyezni, hogy itt nem a felelősségi körök összemosásáról, vagy a civil biztonsági személyzet hatósági jogkörrel való felruházásáról, illetve az állami szervek átfogó kontrolljának bevezetéséről (rendőrállam) van szó, hanem egy pontosan szabályozott együttműködésről, amely az állampolgárok személyes biztonságát szolgálja, azok felesleges és túlzott zavarása nélkül.

5. ÖSSZEGZÉS

Nem kétséges, hogy a biztonsági környezet megváltozott, a legnagyobb elővigyázatosság mellett sem érezhetjük magunkat biztonságban egy esetleges terrortámadással szemben.

A terrorelhárítás állami feladat, viszont a kulturális- , sport és szórakozóhelyek őrzés-védelme a civil személy- és vagyonvédelmi szektor alapvető területe, azonkívül az állami szerveknek nincs kapacitásuk ezekre a feladatokra.

Javaslom egy egységes koncepció alapján létrehozott biztonsági háló kidolgozását a civil személy- és vagyonvédelmi szakma bevonásával, támogató és kiegészítő feladatok végrehajtására.

Véleményem szerint egy nagyon hasznos hiánypótló tevékenység valósulhatna meg ezzel az együttműködéssel.

Egy kiképzett, komoly tapasztalatokkal, élőerővel és technikai eszközökkel rendelkező erőt nem hagyhatunk figyelmen kívül, amikor biztonságunk forog kockán.

Az együttműködésnek a megelőzésre és az esetleges támadás következményeinek kezelésére és felszámolására kell irányulnia.

Ki kell dolgozni azokat a szakmai területeket és szabályokat, amelyek a legnagyobb szakmai eredményt, hozadékot biztosíthatják, majd pedig szakmai alapokon felülvizsgálni és módosítani a vonatkozó törvényt.

Különös figyelmet kell fordítani az alkalmassági feltételek, az oktatás-továbbképzés felülvizsgálatára és az új kihívásoknak megfelelő módosítására.

Javaslatom nem a személy- és vagyonvédelem profilváltására irányul, hanem az eredeti profil meghagyása mellett egy új feladatba történő bevonásra vonatkozik.

IRODALOMJEGYZÉK

[1] Dr. BEREK L.- Dr. BEREK T.- BEREK L.: *Személy- és vagyonbiztonság; Budapest 2016.*

[2] *2.94.05 Kerettanterv a XXXVIII. Rendészet Ágazathoz, Fegyveres szervek és vagyonvédelem I. tantárgy* http://mrszki.hu/images/docs/rendeszetiagazati/segedanyagok/vagyonved/vagyonvedelem_9_10_szeged.pdf (letöltve: 2017. 11. 12.)

[3] *Magyarország Alaptörvénye*,

[4] *Terrorelhárítást szolgáló intelligens kamerarendszerek.* http://steve4security12.blog.hu/2016/09/27/segithetnek-e kamerarendszerek_a_terror_elharitasban#more8522998 (letöltve: 2017. 11. 10.)

[5] 2005. évi CXXXIII. *törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.*

[6] RÁCZ L.: Objektumvédelem, különös tekintettel a szállodavédelemre; Hadmérnök VI. 1. (2011) http://www.hadmernok.hu/2011_1_racz1.php (letöltve: 2017. 10. 14.)

[7] DR. KIS-BENEDEK J. – DR. KENEDLI T.: *A terrorfenyegetettség új tendenciái és lehetséges válaszlépések; Szakmai szemle 1. (2015) 16-35. o.*

[8] KOÓS G. – DR. SZTERNÁK GY.: *A katonai műveletek új formája – a hibrid műveletek; Szakmai szemle 1. (2015) 120-137*

Atomerőmű, mint a kritikus infrastruktúra egy elemének veszélyeztetése, őrzésének és védelmének fő feladatai

The Nuclear Power Plant, the main tasks of guarding and protecting the vulnerability of a component in the critical infrastructure.

Jurás Zsolt
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
zsoltjuras@gmail.com

Összefoglalás: ***Napjainkban a biztonságtudomány területén dolgozó, kutató szakembereknek számos természeti, civilizációs katasztrófát illetve szándékos terrorcselekményekből származó veszélyeztetettséget kell tudniuk számításba venni a kritikus infrastruktúrák őrzésének és védelmének fő feladatainak meghatározásánál. Ismerni kell a veszélyeztetettség csökkentése érdekében történő védekezés módszereit és feladatait. Az ismert legsúlyosabb következményekkel járó civilizációs katasztrófák egyike a nukleáris katasztrófa, ahol a bekövetkezése esetén óriási természeti és civilizációs károkkal lehet számolnunk. Cikkemben a szándékos károkozás, „szabotázsból" származó veszélyeztetés csökkentésére irányuló őrzési és védelmi fő feladatokat mutatom be.***

Kulcsszavak: *Atomerőmű, biztonság, fenyegetettség, kritikus infrastruktúra, védelem*

Abstract: *Nowadays researching and working professionals in the field of safety sciences must be able to consider vulnerability from many natural and civilizational catastrophes as well as intentional acts of terror when determining the main tasks of guarding and protecting critical infrastructures Protection methods and tasks by decreasing vulnerability must be recognized. One of the known civilizational catastrophes with the worst consequences is the nuclear catastrophe, where an occurrence would cause huge natural and civilizational damage. In my article will present the main tasks of guarding and protecting to reduce danger from willful misconduct "sabotage".*

Key Words*: Nuclear Power Plant, safety, vulnerability, critical infrastructure, protection*

1. BEVEZETÉS

Az energiatermelésben előre láthatóan még hosszú távon meghatározó szerepet játszanak majd az atomerőművek. Elég csupán arra gondolni, hogy Magyarországon a paksi atomerőmű bővítésével a hazai nukleáris alapú energiatermelés a duplájára nő. Az atomerőművek működése a technológiából adódóan veszélyesnek mondható, mivel az energiatermelési folyamatot különböző sugárzások kísérik. A sugárzás élettani hatásai miatt, ezek kiküszöbölésére és a nukleáris kockázat csökkentésére különböző berendezések, rendszerek, eljárások kerültek beépítésre, alkalmazásra. Az atomerőmű biztonsága egy összetett, bonyolult folyamat eredménye, ami a tervezéstől az üzemeltetésig tart. A magas szinten tartott nukleáris biztonság egy hatékony és tiszta erőforrást végeredményez. További jellemzője, hogy egy telephelyen több energiatermelő reaktort üzemeltetnek, a paksi atomerőmű esetében 4·500MW beépített villamos teljesítményű blokkokról van szó, ez az ország pillanatnyi energiafogyasztásának az 50%-át is elérheti.

A nukleáris alapú energiatermelési szektorban nagy figyelmet kell fordítani az energiatermelő létesítmények őrzésére és védelmére, ezt indokolja a terrorcselekmények egyre növekvő száma. Éppen ezért kritikus jelentőségű, hogy hazánkban a kiemelten magas szinten tartott nukleáris biztonság folyamatosan biztosított, valamint az ország nukleáris veszélyeztetettsége alacsony szintű legyen.

A terrorcselekményekkel kapcsolatban a 2016 tavaszán megrendezett Washingtoni nukleáris biztonsági csúcstalálkozón David Cameron volt brit miniszterelnök felszólalása hívja fel a figyelmet arra, hogy -véleménye szerint- a terroristák bármit alkalmaznak, amit csak meg tudnak szerezni.

Cameron így fogalmazott: „hihetetlenül fontos a nukleáris anyagok biztonsága mindazon országok számára, amelyeknél futnak atomprogramok, hogy biztosak lehessünk abban, hogy biztonságban vannak ezek az anyagok, nemcsak Nagy-Britanniában, hanem szerte a világon. A brüsszeli támadások felerősítették a félelmeket, miután az öngyilkos merénylők megfigyelték egy belga nukleáris létesítmény egyik vezetőjének az otthonát. Brit kormányzati források ugyanakkor azt mondták, nincs tényszerű bizonyíték, hogy a terroristák brit célpontokra támadnának." [1]

Az ország nukleáris veszélyeztetettsége nagyon sok tényezőtől függ, még a szomszédos országokban elhelyezkedő nukleáris létesítmények (erőművek, tárolók, kutatórektorok stb.) számától is, de első sorban a hazai objektumok telephelyein lévő reaktorok számától és teljesítményétől, tárolok esetében a tárolt nukleáris anyag mennyiségétől.

A két új paksi blokk megépítésével hazánk veszélyeztetettségének mértéke mindenképpen megváltozik, valamint a terroristák számára is új célpont lehet, ezért érdemes a biztonságtudománnyal foglalkozó szakembereknek erre a területre vonatkozó objektumvédelmi és őrzési feladatok összefüggéseit, szabályozásait felülvizsgálni a kritikus infrastruktúrák középpontba állításával.

2. ATOMERŐMŰ, MINT KRITIKUS INFRASTRUKTÚRA?

A kritikus infrastruktúrák meghatározásánál minden esetben figyelembe kell venni az adott ország, illetve valamilyen szervezet, közösség szemszögéből létfontosságú infrastrukturális elemeket.

Rácz László István tudományos cikkében a következőképpen fogalmazott a témával kapcsolatban: „A kritikus infrastruktúrák vonatkozásában meg kell határozni az infrastruktúrához igazodó vizsgálati módszert. Ennek segítségével fel kell tárni a kritikus infrastruktúra körébe tartozó rendszereket és elemeket. Ezeket prioritásuk, a gyakorolt hatásuk szerint be kell sorolni, el kell készíteni az üzemeltetői biztonsági tervet.” [2]

A 90-es évek második felétől generálódott a létfontosságú infrastruktúrák meghatározásának és védelmének igénye, koncepcionális kérdésként való meghatározása. Több szervezet is, de elsőként az USA foglalkozott a tématerülettel műszaki biztonsági aspektusból megközelítve, majd az amerikai terrorcselekmények után biztonságpolitikai és védelmi szempontok mentén. A későbbi európai terror események után sorra az ENSZ, a NATO és végül az Európai Unió is fokozott figyelmet fordított a létfontosságú infrastruktúrák meghatározására és védelmére.

A fent leírtak alapján lehetséges az, hogy nincs egy általánosan elfogadott egzakt kifejezés vagy definíció a létfontosságú infrastruktúrák területén. Szeretnék a következőkben példálózó jelleggel bemutatni néhány kritikus infrastruktúra definíciót:

Az USA Kritikus Infrastruktúra Védelmi Elnöki Bizottsága a következőképpen fogalmazta meg: „Ember alkotta rendszerek és eljárások hálózata, amelyek szinergikusan együttműködve arra törekszenek, hogy folyamatosan alapvető termékeket és szolgáltatásokat állítsanak elő és terjesszenek".

A NATO Polgári Védelmi Bizottsága által az alábbiak szerint került megfogalmazásra a fogalom: „Kritikus infrastruktúra azokat a létesítményeket és információs rendszereket jelenti, amelyek olyan létfontosságúak a nemzetek számára, hogy működésképtelenné válásuknak vagy megsemmisülésüknek gyengítő hatása lenne a nemzet biztonságára, a nemzetgazdaságra, a közegészségre, a közbiztonságra és a kormány hatékony működésére.” [2]

Hazai szabályozás szerinti megfogalmazás: „Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.” [3]

A nem teljesen egybevágó megközelítés, megfogalmazás ellenére a nemzetközi együttműködések és a hazai előkészítő munkák eredményeként megszülettek a hazai nemzeti szabályozások, amelyek rögzítik a Nemzeti Kritikus Infrastruktúrák Védelmére (NKIV) vonatkozó irányelveket.

A szabályozók közül a kutatás szempontjából a kettő irányadó jogszabály a 2012. évi CLXVI. törvény A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, valamint a 65/2013. (III. 8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

Az jogszabályokban megfogalmazott rendelkezések alapján a kritikus infrastruktúrákat ágazati csoportokba lehet sorolni, melyek a következők:

- energiaipar;
- közműellátás nélkülözhetetlen szektorai;
- közlekedés, szállítás;
- távközlés;
- bankrendszer;
- élelmiszer alapellátás;
- egészségügyi ellátás;
- folyamatos kormányzás feltételrendszere;
- rendvédelmi szervek működésének feltételrendszere;
- tömegtartózkodási helyek.

Az ágazati besorolás mellet további felosztása is lehetséges a kritikus infrastruktúráknak, méghozzá a horizontális kritériumok mentén. Így a következő csoportok alakíthatók ki:

- a veszteségek kritériuma
- gazdasági hatás kritériuma
- társadalmi hatás kritériuma
- politikai hatás kritériuma
- környezeti hatás kritériuma

A kritikus infrastruktúrák meghatározásánál az ágazati besorolás és a horizontális kritériumok alapján történő felosztás mellett fontos megemlíteni 5 alapvető tulajdonságot, ami a kritikus infrastruktúrát jellemezheti:

- interdependencia – rendszerek egymástól való függősége;
- informatikai biztonság – kiemelt terület, automatizált FIR-ek, munkafolyamatok;
- üzemeltetés – sajátosságok, egyedi jelleg;
- dominóelv – láncreakciószerű sérülés/károsodás;
- leggyengébb láncszem – összekapcsolódó hálózatok stabilitása a leggyengébb elem erősségétől függ.

A hazai szabályozás mentén az atomerőműveket az energia szektoron belül a villamosenergia-rendszer létesítményi közé kell sorolni, és vizsgálni a horizontális kritériumok mentén.

Ennél a vizsgálatnál figyelembe kell venni az atomerőművek telepítési konfiguráció gyakorlati megvalósításának a sajátosságait, amit az egy telephelyen létesített energiatermelő blokkok nagysága és száma, valamint az egy blokk/országos alapfogyasztás hányadosa erősen befolyásol.

Jelenleg Magyarországon egy atomerőműi blokk hozzávetőlegesen az országos átlagfogyás 10%-át adja, amiből egyenesen következik, hogy egy blokk üzemzavara esetében is már érzékelhető hatást fejt ki a gazdaságra. Értelmezésem szerint a számítások részletezése nélkül a gazdasági hatás kritériuma az egy blokk 22,5 napos termeléskiesése vagy a 4 blokk egyidejű 6 napos termeléskiesése estén teljesül. További kritériumok teljesüléséhez már az egyszerű üzemzavaron túlmutató eseménynek kell bekövetkeznie, ami lehet nukleáris szennyezéssel együtt járó üzemzavar is.

Két alapvető kritikus infrastruktúrára jellemző tulajdonságot ki kell emelni az atomerőművek vizsgálata szempontjából, melyek az interdependencia és az üzemeltetési sajátosságok.

Interdependencia: Az atomerőmű energiatermelésének kiesésekor a villamos-energiaellátó hálózati rendszerben, okozhat olyan mértékű teljesítménylengést, ami a hálózat összeomlásához, Black Out-hoz vezethet. A hálózat teljes összeomlása egy igen bonyolult összetett kérdés, több egyéb befolyásoló tényezőtől függ, amiről Dr. Prof. Berek Lajos és Vass Attila „Gázturbinás erőműi objektum védelme” című tanulmányukban nyújtanak teljes képet.

Üzemeltetési sajátosságok, egyedi jelleg: Az atomerőmű a fizikai létezésével és üzemelésével eleve egyedinek tekinthető, az ott alkalmazott technológia és különféle tudományok alkalmazásának a sokszínűségével. Szintén a technológia sajátosságból adódik, hogy egy blokk energiatermelésének megkezdéséhez úgynevezett idegen gőzös indítására van szükség. Az első blokk létesítésekor ezt a feladatot egy indító kazánház látta el. A második és a többi blokk indításánál már az üzemelő blokkok valamelyike vette át ezt a feladatot. Tehát a négyblokkos kiesés, leállás esetén újból szükség lenne az indító kazánházra, ami már nem áll rendelkezésre. Fontos megjegyezni, hogy az elmúlt 34 éves üzemidő alatt még soha nem fordult elő a blokkok egyidejű teljes leállítása.

Összegezve, több szemszögből is vizsgálva az atomerőműveket mindenképpen a kritikus infrastruktúrák közé sorolom. Ezt a megállapítást azért teszem, mert hazánkban is hosszabb folyamat eredményeként azonosításra, kijelölésre kerültek a létfontosságú rendszerek és létesítmények a 2012. évi CLXVI. törvényben, ugyanakkor a törvény 1. számú melléklete szerint a rendelkezései alól kivételt képeznek az atomerőmű nukleáris biztonságára és sugárvédelmére, fizikai védelmére, valamint biztosítéki felügyeletére vonatkozó szabályozás hatálya alá tartozó rendszerek és rendszerelemek.

3. NUKLEÁRIS LÉTESÍTMÉNYEK VESZÉLYEZTETETTSÉGE.

Az atomerőművek, nukleáris létesítmények okozta katasztrófák általi veszélyeztetettség mértékének kutatásánál, a katasztrófát kiváltó okokat tekintve 3 fő veszélyeztető tényezőt vettem számításba:

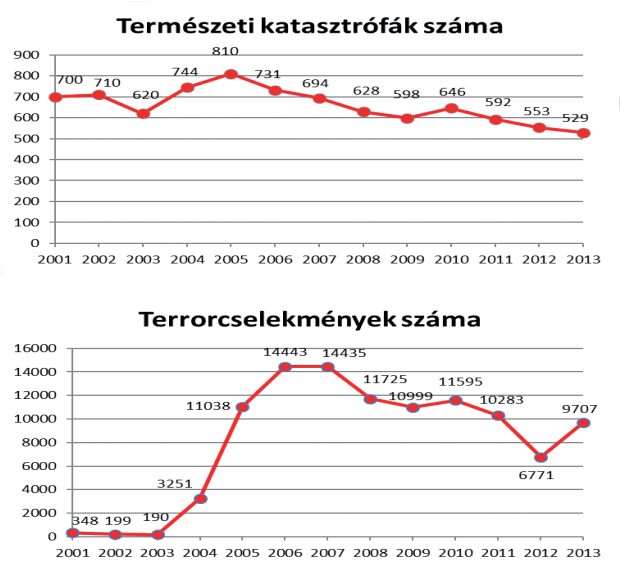
- Természeti katasztrófa
- Üzemzavar (ipari katasztrófa)
- Szándékos jogellenes cselekmények, terrorcselekmények

A különböző eredetű katasztrófák elleni védekezéshez más-más védelmi koncepció, akcióterv kidolgozására van szükség.

A természeti katasztrófák okozta károk és az üzemeltetéssel összefüggésben (technológiai, emberi mulasztás) keletkező meghibásodásból származó károsodások kialakulásának megakadályozására, már a létesítmény tervezésekor nagy figyelmet kapott a biztonsági rendszerek kidolgozása. Az első energiatermelő reaktor üzembehelyezése több mint 50 éve történt és azóta összesen 2 darab nagy nukleáris szennyezéssel együtt járó természeti katasztrófa történt a Csernobili atomerőműben emberi mulasztás miatt, és a Fukusimai atomerőműben tervezési határon túli cunami következtében.

Véleményem szerint az atomerőművek nukleáris biztonsági szempontból magas műszaki színvonalat képviselnek, amit rendszeresen hazai és nemzetközi atomenergiai szervezetek ellenőriznek. Napjainkban nagyobb energiaráfordítást a szándékos cselekmények elleni védelem területén kell alkalmazni a megnövekedett terrorcselekmények száma miatt. A természeti katasztrófák és a terrorcselekmények száma a következő ábrán látható módon alakult az elmúlt években.

A két diagram igazán jól szemlélteti, az elmúlt években nagyságrendekkel megnövekedett a terrorcselekmények száma a világban, és a természeti katasztrófák száma, ha nem is nagymértékben, de azért valamelyest csökkent.



1. ábra: A világ eseményeinek gyakorisága a természeti és terrorcselekmények arányában [4]

3.1 Nukleáris létesítmények elleni terrorcselekmények

A terrorcselekmények változását szemléltető diagram értelmezésekor fontos, figyelembe venni, hogy az adatok az összes terrorcselekményt tartalmazzák, és ennek csak nagyon kis hányada irányult nukleáris létesítmény ellen. Ezek közül én két tanulságos támadást emelek ki röviden összefoglalva:

Behatolás az Oak Ridge-i urántárolóba 2012-ben, ahol fegyver minőségű uránt tárolnak, kezelnek és dolgoznak fel. A nukleáris létesítmény az Y-12-es katonai komplexum (Manhattan-projekt) területén épült 2001. szeptember 11. után. A támadást 3 behatoló hajtotta végre: Michael Walli (65); Megan Rice (84); Greg Boertje-Obed (54). Kerítéseket átvágták, különböző akadályokon áthatoltak, a tároló falát kalapáccsal ütötték, emberi vérrel lelocsolták és jelszavakat festettek rá. A támadás célja a nukleáris fegyverek elleni tiltakozás volt. [5]

A másik eseményről kevesebb információ áll rendelkezésre, ami viszont már üzemelő atomerőmű elleni támadását célozta meg. Oroszországban 2005 októberében Csecsen lázadók öt alkalommal kíséreltek meg repülőgép eltérítést, melyek során különböző oroszországi célpontokat szándékoztak támadni, melyek között szerepelt egy erőműi reaktor is.

A két esemény elkövetésének az indítéka, célja teljesen különböző volt. „Az Oak Ridge-i Környezetvédelmi Békeszövetség elnevezésű szervezet közlése szerint a csoport célja nem az volt, hogy demonstrálja az objektum sebezhetőségét, hanem az, hogy az általuk "háborús bűnnek" minősített nukleárisfegyver-gyártás ellen tiltakozzanak.” [5]

Az oroszországi tervezett cselekménynél viszont egyértelműsíthető a háborús helyzetben, belső zavargásokat gerjesztő Csecsen lázadók terroristatámadása volt, amivel nukleáris katasztrófát akartak előidézni. A második ábrán az Oak Ridge-i elkövetők, a harmadik ábrán pedig felfegyverzett Csecsen katonák láthatóak.

2. ábra: Oak Ridge-i elkövetők [5]

3. Ábra: Csecsen katonák [6]

Számomra nagyon tanulságos az Oak Ridge-i behatolás, mert az aktivisták szándéka csak a tüntetés, tiltakozás volt, de magával a szabotázs végrehajtásával felhívhatták a figyelmét a nemzetközi terrorszervezeteknek arra, hogy egy fokozottan őrzött nukleáris objektum területre milyen egyszerűen be lehetett jutni.

Fontos itt megjegyezni, hogy az incidens után az amerikai kongresszus és az energiaügyi minisztérium vizsgálatot indított melynek eredményeként biztonsági vezetőket és a biztonsági szolgálatot ellátó őrzés-védelmi céget leváltották.

A két eseményt összegezve elmondható, hogy a tüntetéstől a terrorcselekményekig nagyon sokféle céllal hajthatnak végre nukleáris létesítmények ellen irányuló támadásokat, aminek a sokszínűségét az 1966 és 2007 közötti támadások felsorolása is megmutatja.

3.2 Nukleáris létesítmények ellen irányuló támadások 1966-tól 2007-ig

1966 - 1977: Európa - 10 nukleáris létesítmény ellen elkövetett terrortámadás

1968 - 1974: USA - 32 károkozással járó cselekményt, ill. szabotázs gyanúját észlelték különböző nukleáris létesítményekben

1978: Spanyolország - bomba robbant a lemonizi atomerőmű gőzfejlesztőjénél

1982: Franciaország – 4 páncéltörő rakétát lőttek ki a creys - malville-i nukleáris létesítményben elhelyezkedő Super Phénix kutatóreaktorra

1982: Dél-Afrikai Közt. - robbantásokat hajtottak végre az épülő koebergi atomerőműnél

1987: USA - bomba robbant a Sandia Nemzeti Laboratórium parkolójában

1992: Oroszország - 3 atomerőmű ellen irányuló fenyegetést regisztráltak

2004: Ausztrália - terrortámadást terveztek Sydney-ben a Lucas Heights kutatóreaktor ellen

2005: Lashkar - e - Toiba (Igazak Hadserege) terrorszervezet tagjai a kihallgatásuk során beismerték, hogy a célpontok között szerepelt az indiai Kaiga atomerőmű

2007: Dél-Afrikai Közt. - 4 felfegyverzett támadó behatolt a pelindabai fokozottan őrzött nukleáris létesítménybe

A nukleáris létesítmények jellegétől, a szabotázs szándékától, a földrajzi elhelyezkedéstől, a veszélyeztetettség mértékétől, de a terület identitásától is függhet az adott objektum ellen irányuló támadások valószínűsége. A valós veszélyek felmérése mellett az elképzelhető támadások sikeres kivitelezésüket kell megakadályozni komplex védelmi megoldások megvalósításával.

4. Atomerőművek őrzésének és védelmének fő feladatai

Az atomerőművek fizikai biztonsági rendszerének üzemeltetése összetett bonyolult feladat, mert a létesítmény működésének teljes időtartama alatt illeszkednie kell a társaság gazdasági céljaihoz, hazai jogszabályi előírásokhoz, a hatósági elvárásokhoz, útmutatókhoz és a nemzetközi követelményekhez.

A nukleáris anyagok, nukleáris létesítmények, radioaktív sugárforrások és radioaktív hulladékok elleni terrorcselekmények vagy szabotázsok elkövetésének fenyegetésével szemben a fizikai védelemnek kell biztonságot nyújtani. A fizikai védelem – az atomenergiáról szóló 1996. évi CXVI. törvény 2. § 33. bekezdése alapján – „azon belső szabályozás, technikai eszköztár és élőerős elhárítás összessége, amely a nukleáris védettség részeként a nukleáris létesítményekkel, valamint nukleáris és más radioaktív anyagokkal szemben elkövetendő jogtalan eltulajdonítás és szabotázs észlelésére, elrettentésére, késleltetésére és elhárítására irányul.” [7]

A nukleáris létesítmények, nukleáris és más radioaktív anyagok fizikai védelmével kapcsolatos előírásokat többek között az atomenergiáról szóló 1996. évi CXVI. törvény, az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 190/2011. (IX. 19.) Kormányrendelet, valamint hatósági és nemzetközi útmutatók tartalmazzák.

Hazánkban a nukleáris létesítmények fizikai védelmi rendszerének alkalmasnak kell lennie a tervezési alapfenyegetettség hatékony és időbeni észlelésére, késleltetésére és elhárítására. A tervezési alapfenyegetettség a fenyegetettség állam által meghatározott azon szintjét jelenti, amely ellen a hatékony fizikai védelmet az atomenergia alkalmazója biztosítja. A tervezési alapfenyegetettséget meghaladó mértékű fenyegetés esetén állami eszközökkel egészül ki a védelem [7]. A tervezési alapfenyegetettséggel szemben a hatékony fizikai védelmi rendszer tervezéséért, létrehozásáért és folyamatos működtetéséért az atomenergia alkalmazója a felelős.

Az atomerőművek fizikai védelmi rendszerével szemben támasztott törvényi követelményeket kielégítésére biztonságtechnikai eszközöket és technikákat kell alkalmazni. Az alapvető technikák alatt az előerős védelem, a mechanikai védelem és az elektronikai vagyonvédelmi rendszerek összességét értjük, amit más néven komplex védelmi rendszernek is hívhatunk.

A továbbiakban felvázolt őrzési-védelmi feladatok megvalósítására készített javaslatom egy általános megoldási lehetőséget kínál az atomerőművek részére, nem a Paksi atomerőmű jelenlegi kialakítását tükrözi.

A komplex védelemi technikákat a biztonságtechnikai alrendszerek mentén mutatom be:

Élőerős védelem alkalmazott erőforrásai:

- Fegyveres Biztonsági Őrség (FBŐ) 27/1998. (VI. 10.) BM rendelet alapján
- Őrszolgálat – a 2005. évi CXXXIII. törvény. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól. szóló törvény alapján
- TEK Terror Elhárítási Központ a tervezési alapfenyegetettséget meghaladó cselekmények elhárítására

Mechanikai védelem

- Kerítésvédelem (mechanikus védelem elektronikus fedővédelemmel)
- Beléptetési pontok és zónahatárok forgókapui, zsilipjei
- Rácsok, szögesdrótok
- Zárak

Elektronikus rendszerek

- beléptetőrendszerek
- CCTV-rendszerek (látható és infratartomány)
- fokozott védelmet igénylő helyiségek kiegészítő védelme
- kommunikációs hálózat (biztonságos kommunikáció, alternatív megoldások)
- monitorközpont (kijelzések, vezérlések, irányító központ)
- kültéri mozgásérzékelők
- biometriai azonosítók
- röntgengépek (csomag)
- fémdetektáló kapuk
- sugár kapuk
- robbanóagyag detektáló berendezések

5. ŐRZÉSI ÉS VÉDELMI FELADATOK MEGVALÓSÍTÁSI JAVASLATA

Élőerős védelem megtervezésénél a három szervezetileg egymástól elkülönült egységek alapvető feladatainak a többségét a vagyonvédelmi törvény hatálya alá tartozó őrszolgálati feladatok elvégzésével megbízott szervezetnek kell végrehajtania.

Az atomerőmű folyamatos működéséből adódóan az élőerős védelmet 0-24 órás váltóműszakos rendben kell megvalósítani. A szervezetnek el kell látnia az erőművet üzemeltető, karbantartó és egyéb személyzetének a folyamatos ki és beléptetését. A ki és beléptetés során ellenőrizni kell a beléptető pontokhoz érkező személyek jogosultságát, illetve a teherportán a gépkocsikat is. A beléptetési jogosultság ellenőrzését követően az áthaladó forgalom által ki és beszállított eszközök vizsgálatát és a nem személyi használatú tárgyak esetén azok engedélyezését. A beléptető pontokon üzemeltetni kell a fémkapukat, a sugárkapukat és az automata tolókapukat.

Tekintettel a veszélyes ipari üzem mivoltára, el kell rendelni az üzemeltető személyzet területre való belépéskori véletlenszerű alkoholszondás és drogtesztes ellenőrzést.

A területet fel kell osztani különböző zónákra a technológia berendezések és a veszélyeztetettség figyelembevételével. Egy úgynevezett nyomottvizes atomerőművet példaként véve jól el lehet határolni a nukleáris folyamatot fenntartó technológia helyiségeket (primer kör, reaktor és berendezései) és a villamos energia előállításában közvetlen résztvevő technológiai berendezések (szekunder kör, turbó gépcsoport és berendezései) helyiségeit, amelyek önmagukban képezhetnek egy zónát.

További zónák lehetnek még irányítótermek, önálló autonóm egységet képező kiszolgáló technológiák valamint általános területi zónák. A zónahatároknál zsilipes illetve forgókeresztes beléptető rendszereket kell kialakítani, amelyek segítségével akár egy adott személy területi mozgása is meghatározható.

A fokozottan őrzött védelmi zónába történő átlépés esetén, az FBŐ szolgálatot kell megbízni az őrzési védelmi feladatokkal a 27/1998. (VI. 10.) BM rendelet alapján, és a veszélyeztetés mértékének függvényében, a fegyveres biztonsági őrség rövid lőfegyvertől eltérő nagyobb hatótávolságú, puskákat, karabélyokat kell rendszeresíteni.

Általánosságban mondható, hogy a kiemelten fontos pontokon, illetve területen felállított őrt kell alkalmazni. Az erőműben felállított őrök által nem biztosított körzetét járőrözéssel kell ellenőrizni. [8] Az őrök éberségének fenntartása érdekében az őrzési, ellenőrzési pontokon a személyzet folyamatos 2 óránkénti rotációs váltásával kell lefedni a 0-24 órás szolgálati időt. A járőrözés hatékonyságát mindenképpen járőrellenőrző rendszer kiépítésével és a lefedetlen területeknél zárt láncú kamerarendszer alkalmazásával kell támogatni.

További fő feladatként deklarált a különböző funkciókat ellátó elektronikai rendszerek, mint például a fémkapuk üzemeltetése a területre való fegyverek bejutatását megakadályozó, illetve azok detektálását szolgáló rendszer.

A javaslat figyelembevételével egy tervezett atomerőmű biztonsági rendszerének a kialakításakor ellenálló komplex védelmi megoldást lehet megvalósítani. Természetesen a fő feladatokat további alfeladatokra kell bontani az aktuális környezeti tényezőkhöz igazodva. Megállapítható, hogy védelmi rendszerek kialakítása összetett feladat, ami nagy odafigyelést és széleskörű szakmai ismereteket igényel.

IRODALOMJEGYZÉK:

[1] David Cameron nyilatkozata http://vs.hu/kozelet/osszes/piszkos-bomba-veszelyere-figyelmeztet-david-cameron-0401

[2] Rácz László István: Kritikus infrastruktúra védelem hazai és nemzetközi szabályozási rendszere, 2012. *Hadmérnök*, http://hadmernok.hu/2012_2_racz.pdf

[3] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[4] Vass Attila – Dr. Maros Dóra – Prof. Dr. Berek Lajos: Az interdependencia kérdése az energetikai rendszer és a híradástechnika esetén a kritikus infrastruktúra biztonsága védelmében, 2015. *Bolyai szemle,* http://uni-nke.hu/uploads/media_items/bolyai-szemle-2015-03.original.pdf

[5] https://www.partyzoo.hu/magazin/2014-02-20-tobb-ev-bortonre-iteltek-egy-84-eves-apacat-mert-behatolt-egy-nuklearis-letesitmenybe

[6] Ábra 3. http://ic.c4assets.com/brands/terror-in-moscow/42e804af-85ec-481b-9759-51f5f178f37d.jpg?interpolation=progressive-bicubic&output-format=jpeg&output-quality=90%7B&resize%7D

[7] 1996. évi CXVI. törvény az atomenergiáról

[8] Prof. Dr. Berek Lajos - Vass Attila: Gázturbinás erőműi objektum védelme, 2014. *Hadmérnök*, http://hadmernok.hu/142_01_berekl.pdf

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Nukleáris üzemanyag közúti szállításának kivitelezhetősége fizikai védelmi szempontból

The feasibility of transporting nuclear fuel from the point of view of physical protection

Viplak Armand Máté, Prof. Dr. Berek Lajos
* Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
viplak@haea.gov.hu, berek.lajos@bgk.uni-obuda.hu

***Összefoglalás* — Az atomerőművekben felhasznált nukleáris üzemanyagot többféle módon szállítják, hazánkban a legelterjedtebb a vasúton történő, illetve az utóbbi időben megjelent légi szállítás is. Az eddigi tapasztalatok alapján megjelent a szakmai igény a közúti szállításra is. Az újféle módozatot esetén vizsgálni kell a jogszabályi feltételeket és előírásokat, illetve a megfelelő fizikai védelmet biztosító műszaki megoldásokat, az élőerős biztosítást és az útvonalválasztás feltételeit is. A cikk ezek vizsgálatán túl kitér a megálló helyekkel kapcsolatos megoldásokra és az emelt szintű fizikai védelem bevezetésekor meghozható intézkedésekre.**

***Kulcsszavak*:** nukleáris, üzemanyag, szállítás, fizikai védelem

***Abstract* — There are many ways to transport fresh nuclear fuels into nuclear power plants, in Hungary the most usual way is by train, but during the latest times the aerial transport also occurred. Based on previous experiences, there is a demand for the road transport method. In case of this new mode, it is necessary to examine the legal conditions and regulations, technical solutions that provide adequate physical protection, the possibilities of response and the selection method of the transport routes. In addition to this, the article addresses the approaches to stopping points and the actions to be taken when introducing elevated level of physical protection.**

***Keywords*:** nuclear, fuel, transport, security, physical protection

1 BEVEZETÉS

Az atomerőművek reaktoraiban lezajló láncreakciókhoz szükség van valamilyen fajtájú hasadóanyagra. A nukleáris anyagok, a hazánkban is található, nyomottvizes atomreaktorokban urán-dioxid pasztilla formájában használtak. A pasztillák az úgynevezett üzemanyag pálcákban találhatóak meg és a pálcák alkotják az üzemanyag kazettákat, amelyek más néven fűtőelemnek vagy fűtőelem kötegnek is szoktak nevezni. A még reaktorban fel nem használt üzemanyag a friss vagy nem kiégett kazetta, amely alacsony radioaktív sugárzást bocsájt ki. A friss fűtőelemek a gyártótól egyenesen az atomerőművekbe kerülnek, ahol több évre elegendő mennyiséget halmoznak fel belőlük. A két végpont közötti szállításkor a nukleáris anyag védelmét biztosítani kell szabotázs vagy jogtalan eltulajdonítás ellen, nemcsak a szállított anyag radioaktív és nukleáris mivolta miatt, hanem mert a kazetták nagy anyagi értéket jelentenek az üzemeltetőknek. Egy esetleges sikeres elkövetői akciót követően számítani lehet a lakosságban kialakuló pánikra és az atomenergia használat elfogadottságának csökkenésére is.

A nemzetközi gyakorlatban a földi (vasúti és közúti), a vízi (elsősorban tengeri) és a légi szállítási módok, illetve ezek kombinációi használtak. Hazánkban a Paksi Atomerőműbe eddig kétféle módon történt fűtőelem szállítás: teljes hosszában vasúton, illetve, 2014-től, az ország területére légi úton érkező és a repülőtértől vasúton történő kombinált eljárás szerint. [1] A vasúti szállítás előnye, hogy egyszerre nagyobb mennyiségű kazettát is lehet szállítani a biztosítást adó kísérettel együtt. Hátránya, hogy a korlátozott útvonalszám miatt nagyobb kerülőket kell tennie a szerelvénynek, többször olyan pályaszakaszt érintve, amely nem kétvágányú és nem húzódik mellette közút. Ennek problémája, hogy egyrészt nehezen juttatható el szükség esetén megerősítő erő a szerelvényhez, másrészt, ha műszaki hiba lép fel, vagy valamelyik vagon felborul, akkor nem tud mellé olyan daru állni, ami képes lenne a vagont a vágányra visszaemelni. Az útvonalat nem lehet úgy összeállítani, hogy ne érintsen lakott települést vagy a közforgalom által is használt vasútállomást, illetve szükség lehet többszöri mozdony és mozdonyvezető váltásra is. Vannak olyan nem megkerülhető szakaszok, amelyeken történő bármilyen műszaki hiba azt eredményezheti, hogy a szerelvénynek mindenképpen meg kell állnia és várakoznia kell a hiba elhárításáig, valamint a Paksi Atomerőmű egyetlen, egyvágányú vasútvonalon keresztül közelíthető meg. Mindez azt eredményezi, hogy a szállítás hosszú idejű, amely akár el is húzódhat, illetve a biztosítása nagyszámú rendőri erőt köt le országos szinten.

Az eddig tapasztalatok alapján jelent meg az a szakmai igény hazánkban, hogy a friss üzemanyag kazettákat az államhatártól vagy pedig a repülőtértől közúton lehessen eljuttatni a Paksi Atomerőműbe. Ennek megvalósításához nemcsak a jogszabályi háttér, hanem az érvényes műszaki előírások és a kivitelezés vizsgálata is szükséges.

2 A SZÁLLÍTÁSRA VONATKOZÓ ELŐÍRÁSOK

Az olyan veszélyes anyagok közúti szállítására, mint amilyen a friss nukleáris üzemanyagé, többféle jogszabályi és műszaki előírások vonatkoznak. Ezek nemcsak a szállító járművet és a kíséretét szabályozzák, de az útvonalakat és a megállóhelyeket is, illetve azokat a különleges időszakokat, amikor a szállítmány fenyegetettsége megnő és kiegészítő védelmi intézkedésekre lehet szükség.

2.1 Vonatkozó hazai jogszabályok a szállítás fizikai védelmére, a lehetséges résztvevő szervezetek

A nukleáris anyagok szállításának fizikai védelmének jogszabályi hátterét elsősorban az atomenergiáról szóló 1996. évi CXVI. törvény (a továbbiakban Atomtörvény vagy röviden Atv.) és az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 190/2011. (IX.19.) Kormányrendelet (a továbbiakban Kormányrendelet vagy röviden FVr.) alkotja. Az Atomtörvény 30.§-a határozza meg a szállítás során a fizikai védelmi rendszer, azaz a nukleáris védettség célját, amely „a nukleáris és más radioaktív anyagok jogtalan eltulajdonításának, a Btk. szerinti radioaktív anyaggal visszaélés (250. §), a szabotázs, valamint a nukleáris vagy más radioaktív anyaggal való közveszély okozása, környezetkárosítás elkövetésének megelőzését" [2], illetve kijelöli, hogy a nukleáris védettségért felelős hatóságokat, jelen esetben az Országos Atomenergia Hivatal (OAH), mint az atomenergia-felügyeleti szerv, és az Országos Rendőr-főkapitányság (ORFK), és azok feladatait. A fizikai védelmi rendszer tervezésekor és üzemeltetésekor az Atv. 31.§-ban meghatározott irányelveket kell követni. [2]

Az Atomtörvényben foglalt alapelveknek megfelelően a 2011-ben elfogadott Kormányrendelet határozza meg a műszaki tartalomra és az eljárásrendekre vonatkozó előírásokat. Az FVr. megadja a védendő nukleáris és radioaktív anyagok kategorizálásának módját. Az anyag kategóriája és a vele tervezett folyamat (alkalmazás, tárolás vagy szállítás) alapján meghatározható, hogy A-tól D-ig milyen védelmi szintet kell biztosítani, és hogy az egyes szinteknél milyen elkövetői szándék ellen kell felkészülni (szabotázs, jogtalan eltulajdonítás). A Kormányrendelet definiálja a fizikai védelmi rendszer funkcióit: elrettentés, detektálás, késleltetés, elhárítás és ezek megvalósításának szabályait. Az egyes védelmi szintekhez tartozó konkrét előírásokat a rendelet mellékletei tartalmazzák. [4]

Az FVr. kiköti, hogy radioaktív anyag szállítása engedélyköteles. Az engedélykérelemhez, kivéve, ha az anyagnak D védelmi szintet kell biztosítani, egy Fizikai Védelmi Tervet kell készíteni és csatolni. Az engedély C szintű szállítás esetén 5 évig érvényes, korlátlan mennyiségű szállításra, B szint esetén viszont csak egy adott szállításra lehet engedélyt kérni. A Fizikai Védelmi Tervben kell az engedélyt kérőnek bemutatnia, az adminisztratív adatokon és elérhetőségeken túl, hogy a radioaktív anyagot tartalmazó konténer és az azt szállító gépjármű milyen műszaki megoldásokkal elégíti ki az előírásokat, illetve a szállítás milyen elsődleges és tartalék útvonalakon valósulna meg, hogyan épül fel a biztosítás és milyen eljárások vannak a rendkívüli események kezelésére. A Védelmi Terv pontos tartalmi előírásait a Kormányrendelet 4. melléklete tartalmazza. Az engedélykérelmet eljáró hatóságként az OAH bírálja el, az ORFK szakhatósági segítségével. Az FVr. egyedi előírásokat is állapít meg a nukleáris iparban alkalmazott fegyveres biztonsági őrség tagjaival szemben: iskolai végzettség és fizikai erőnléti előírások teljesítése. [4]

Bár szigorúan véve nem szabályozója a nukleáris védettségnek a veszélyes anyagok közúti szállításának biztonságát szabályzó ADR jogszabály, de a benne meghatározottak kötelező érvényűek a szállítás tervezése és végrehajtása során, illetve befolyásolja a Védelmi Tervben levő műszaki megoldásokat és eljárásokat. Például, egy esetleges baleset vagy veszélyhelyzet esetén a kíséret és a gépjármű vezető feladatait az ADR szerinti teendőkkel is össze kell hangolni.[5] A Kormányrendelet 5.§ értelmében a „fizikai védelmi rendszernek az I. és II. kategóriába tartozó nukleáris anyag, 1. kategóriába tartozó radioaktív sugárforrás és radioaktív hulladék szállítása során biztosítania kell a szabotázs elleni védelmet az azokra vonatkozó, jogszabályban meghatározott szállítási biztonsági követelmények teljesítése útján"[6], azaz ha a szállító konténer megfelel az ADR előírásainak, akkor nem kell igazolni azt, hogy ellenállna egy szabotázs akciónak is.

A jelenlegi gyakorlat szerint a rendőrség is biztosítja a friss nukleáris üzemanyagok szállítását. [7] Erre jogi alapot az atomenergia alkalmazásával összefüggő rendőrségi feladatokról szóló 47/2012. (X. 4.) BM rendelet 5.§-a adhat, amely kimondja, hogy az Atv. 31. § (4) bekezdése szerinti esetben, azaz amikor a fenyegetettség megnövekedése miatt szükségessé válik az állami szervek bevonása a nukleáris védettség fenntartásához, a rendőrség részt vesz az I. és II. kategóriájú nukleáris anyagok szállításának biztosításában. Közúti módozat esetében oszlopvezető és záró gépjárművet ad, valamint elvégzi a szükséges a forgalomszabályozó feladatokat. Vasúti szállítás esetén működteti a szerelvény rádióhíradását, készenlétben tartja a területileg illetékes beavatkozó egységeket és fokozottan felügyeli a tervezett megállóhelyeket. [8] Ahhoz, hogy a jövőbeni közúti szállítások megfelelő rendőri biztosítása jogilag megalapozott legyen, szükséges ennek a paragrafusnak a megváltoztatása. Egyrészt a rendőri biztosítási feladatokat abban az esetben is kötelezővé kellene tenni, amikor nem áll fenn az Atv. 31. § (4) bekezdése szerinti eset. A szállított nukleáris anyag mennyisége miatt egy támadás pánikot kelt a lakosság körében, illetve szélsőséges esetben fennakadást okozhat az atomerőmű termelésében, ezzel veszélyeztetve a lakosság ellátását. Másrészt a vasúti szállításhoz tartozó rendőri feladatokat a közúti módozatnál is elő kellene írni: a területi beavatkozó egységek készenlétben tartásával rövidebb idő alatt tudna a rendőrség olyan eseményekre reagálni, amelyek csapaterős jelenlétet igényelnek, és amelyek veszélyeztethetik a szállítási folyamatot (például demonstráció az útvonalon), a megállóhelyek biztosításával pedig egyszerűbben meg lehet felelni az FVr. megállókra vonatkozó feltételeinek. További változtatás, bár ez nem feltétlenül ebben a BM rendeletben kell megjelennie, hogy a Terrorelhárítási Központ (TEK) is vegyen részt a szállítmány útvonalának biztosításában a műveleti és felderítési tevékenységeivel.

A szállításban résztvevő szervezetek közül az elsődleges az engedélyt megkapó és az FVr. szempontjából kötelezett, esetünkben az MVM Paksi Atomerőmű Zrt.. A teljes végrehajtás során a nukleáris anyagok védettségéért és biztonságáért elsősorban a kötelezett felelős, illetve ő biztosítja a szállítmány dozimetriai felügyeletét is. A konvojt biztosító reagáló erő lehet az erőmű saját fegyveres biztonsági őrségének csapata vagy pedig szerződés útján megbízhatja, a nagyértékű pénzszállítások kíséréséhez hasonlóan, a rendőrséget vagy a TEK állományát. Mindkét szervezetnek nagy tapasztalata van védett személyek és szállítmányok kísérésében, illetve az útvonalok biztosításában. A rendőrség területi erőin túl elsősorban a Készenléti Rendőrség egységei vehetők igénybe, akik a pénzszállítmány kíséréseket, illetve a Tűzszerész Szolgálaton keresztül a gépjármű és terület ellenőrzéseket végzik. A konvojban helyet kaphat a hivatásos katasztrófavédelmi szerv állománya is, illetve az OAH és

az ORFK hatósági ellenőrei, akiknek a teljes folyamat alatt ellenőrzési jogosultsága van.

2.2 Szállító gépjárműre vonatkozó előírások

A szállítójármű vagy járművek méretének meghatározásakor figyelembe kell venni a szállítandó anyagot: a VVER-440 reaktorokban használt fűtőelemek 215 kg tömegű [9], 3217 mm magas, szabályos hatszögalakú kazetták, amelyek kulcsmérete 145 mm. [10] A szállítás során minden kazetta egyedileg egy szállítókonténerbe kerül, amely biztosítja az ADR szerinti védelmét a nukleáris anyagnak. A konténereket az 1. ábrán látható módon lehet a raktérben elhelyezni. A rakteret lehet ponyvával vagy pedig merev burkolattal takarni. Fontos a kialakításnál, hogy a daruzhatósági lehetőség biztosítva legyen a könnyebb rakodás végett. A kazetták tömege miatt olyan szcenárióval nem kell számolni, hogy az elkövetők gyalog tulajdonítanák el őket. Vagy a szállítójárművel együtt próbálják meg elvinni, vagy pedig át kell rakodniuk egy más járműre.

1. ábra: Üzemanyag szállító konténerek rögzítése a szállító jármű rakterében. [11]

A gépjármű tervezésekor figyelni kell rá lehetőleg, hogy ne legyen túlméretes a szállítmány, hiszen ekkor útvonalengedély szükségessége, sebesség korlátozások és egyéb előírások lépnek fel. Túlméretes a közúti szállítmány, ha a jármű össztömege meghaladja a 40 tonnát vagy az összmérete rakománnyal együtt nagyobb, mint:

−Pótkocsi nélküli tehergépjármű hosszúság 12,00 m;

−Nyerges járműszerelvény hosszúság 16,50 m;

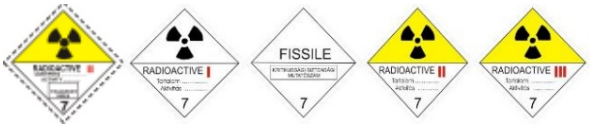
−Pótkocsis járműszerelvénynél hosszúság 18,75 m;

−A jármű szélessége 2,55 m, magassága 4,00 m. [12]

A gépjármű fizikai védelmi rendszere tervezésekor figyelembe kell venni, hogy a szállított nukleáris anyag B védelmi szintbe tartozik. A rendszer tervezését az FVr. 29.§ (5) bekezdése alapján csak érvényes vagyonvédelmi tervezői igazolvánnyal rendelkező személy végezheti. [13] A rendszernek az Atomtörvényben lefektetett alapelvek mentén kell működnie. Ezek a fokozatosság elve, azaz minden anyagot a kategóriájának megfelelően kell csak védeni, a mélységi védelem elve, azaz a védelemnek több szintből kell állnia és meg kell felelnie a rendszereknek az egyszeres hibatűrés követelményének, az egyenlő védelem elve, amely kimondja, hogy függetlenül az elkövetés módjától, helyétől, idejétől és a fennálló külső-belső körülményektől, az őrzött anyagnak mindig azonos védelmet kell biztosítani. [2] A gépjármű védelmi rendszerének, a kísérettel együttvéve, biztosítania kell az elrettentés, detektálás, késleltetés és elhárítás funkciókat. [4]

A gépjárműben helyet kell tudjon foglaljon a sofőr mellett még egy fő, ugyanis B szintű szállítás esetén mindig minimum 2 főnek kell lennie a szállítójárműben. Biztosítani kell a vezető részére olyan kommunikációs eszközt, amelyen keresztül tartani tudja a kapcsolatot a kísérettel. A kíséretben egy arra kijelölt feladata, hogy időszakosan ellenőrizze a kapcsolatot a szállítmány vezetőjével, a területileg illetékes hatóságokkal, a kiinduló és végállomással és a szállítást felügyelő őrségközponttal. A kommunikációs vonalak elvesztésének kezelésére rendelkezniük kell eljárással. [4] A szállítójármű vezetőfülkéjét érdemes lövedékállóként kialakítani. Ennek előnye, hogy egy támadás esetén a sofőr és a kísérő biztonságban lehet, fel tudják venni a kapcsolatot a szükséges szervekkel, illetve megnehezíti a gépjármű eltulajdonítását is. Egy esetleges olyan belső elkövető ellen, aki bejutott a fülkébe és megpróbál elhajtani a kazettákkal, a szerző látott már olyan megoldást, hogy a motortér oldalán elhelyezett ajtón keresztül a motor kívülről blokkolható a reagáló erők által. Ezzel még idejében, komolyabb erőbehatás nélkül megállítható a jármű, nem kell a fűtőelemek sérülésével számolni.

A rakodóteret berakodás után a szállítókonténerek elrejtése miatt célszerű lefedni. Ez megtehető ponyvával vagy pedig egy merevebb, erősebb anyagból készült felépítménnyel. Ha a takarás megfelelő erősségű, akkor egy hosszabb megállónál számolni lehet vele, mint védelmi zónahatárral, illetve növeli a jármű késleltetését és megfelel a mélységi védelem elvének is. A takaráson, illetve a gépjármű többi részén szükséges elhelyezni a 2. ábrán látható ADR jelzést, amely a szállított anyag tulajdonságáról ad információt. A jelzések használatával az elrettentés funkciót lehet erősíteni.



2. ábra: ADR szerinti radioaktivitás jelzése. [12]

A rakteret megfelelő felület- és térvédelemmel kell ellátni. A detektáló rendszerekről érkező riasztási jelzéseket minimálisan a vezetőfülkében, illetve a szállítást felügyelő őrségközpontban kell tudni megjeleníteni. A rakományt a gépjármű kísérőnek kamerán keresztül is látnia kell a vezetőfülkéből. Ha ezek a rendszerek nem építhetők ki, akkor az FVr. lehetőséget ad eltérésre is, de ezt az eljáró hatóságok vizsgálják. Ilyen eltérő megoldások például a szállítójármű közvetlen megfigyelése elő- és utófutó kocsikból vagy pedig olyan kialakítás, hogy a kocsikísérő a fülkéből közvetlenül rálásson a szállítókonténerre. [4]

A megfelelő késleltetés biztosításához mechanikai védelemre van szükség. A Kormányrendelet értelmében elegendő a rakteret vagy pedig a szállítókonténert megerősíteni, úgy, hogy 10 perces késleltetési időt biztosítson, illetve látszódjon az illetéktelen hozzáférés. [4] A kellő hosszúságú késleltetés elérhető aktiválódó eszközök telepítésével. Ezek lényege, hogy illetéktelen behatolás esetén lépnek működésbe és valamilyen módon akadályozzák az elkövetői cselekményt. Ez lehet füst képzése a raktérben vagy pedig a szállítókonténerek

speciális ragadó habbal való beterítése. A megfelelő gépjármű után a szállítmány kíséretének, illetve a szállítási útvonalnak a megtervezése a feladat.

2.3 Útvonalra és a szállítmány kíséretére vonatkozó előírások

A szállítás útvonalának meghatározásakor az alábbi fizikai védelmi előírásokat kell betartani: több alternatív útvonalat is ki kell jelölni, a legmagasabb rendű utakat kell használni és kerülni kell a sűrűn lakott területeket. Ha mégis lakott terület érintése szükséges, akkor a csúcsforgalmi időszakon túl kell a szállítást lebonyolítani. Az elsődleges és alternatív útvonalakat úgy kell kijelölni, hogy az áttérés rövid időn belül megoldható legyen. Figyelembe kell venni a nyilvánvaló veszélyforrásokat és indulás előtt ellenőrizni kell az útvonal járhatóságát és védhetőségét. Kerülni kell a rendszerességet. [4] Javasolt még olyan útvonalat választani, amely mentén kijelölhető megfelelő szükség megállóhely műszaki hiba, sofőrváltás vagy más gond esetére. Érdemes főként az autópályákat igénybe venni, a kiépített térfigyelő rendszernek hála az útvonal nagy része közvetlenül indulás előtt, illetve a szállítás során ellenőrizhető. Egy esetleges demonstráció vagy támadás előjelei hamarabb észlelhetőek.

A szállítmány kíséretének megtervezésekor a fizikai védelmi rendszer alapelveire és funkcióira vonatkozóan túl az alábbiakkal is számolni kell: járművet kell biztosítani a kötelezett képviselőjének és a dozimetriai csapatnak, illetve az esetleges hatósági ellenőröknek. Ha az FVr. előírásaitól eltér a szállítójármű, akkor annyi kísérő járművel kell számolni, hogy az összes szállítójárművet közvetlenül közre lehessen fogni. A konvojt felvezető és záró gépjárművet lehetőség szerint megkülönböztető jelzéssel kell ellátni a zavartalan haladás miatt. Az útvonal közvetlen felderítéséhez és ellenőrzéséhez előfutó gépkocsi használata ajánlott. Hogy a kereszteződéseknél és felhajtóknál a konvoj gyorsan és védve átjusson, zárógépkocsikra van szükség, amelyek megfelelő mechanikai védelmet is biztosítanak egy áthatolási kísérlet esetén. A zárókocsikból elegendő két darab olyan, amely megkülönböztető jelzéssel ellátott és amely megfelelő teljesítménnyel rendelkezik a konvoj utolléréséhez és a következő zárási hely időbeni eléréséhez. Ezt a számot növelni kell, ha a kijelölt útvonalon sűrűn van zárandó terület. A zárógépkocsik használatával nem szükséges minden kereszteződés és felhajtó biztosításához külön erőket biztosítani.

A fegyveres kíséret létszámát és felszerelését úgy kell meghatározni, hogy ellen tudjon állni és fel tudjon tartóztatni egy feltételezett elkövetői csoportot mindaddig, amíg a külső reagáló erők megérkeznek. A kíséretnek nem feladata a támadók feltétlen felszámolása, hanem a szállítmány biztosítása, szükség esetén menekítése. A konvojban levő gépkocsikat úgy kell kiválasztani, hogy azokban a kijelölt személyek és felszerelésük megfelelően elférjen. A teljesítményük legyen elegendő, hogy lépést tudjanak tartani a szállító járművekkel és olyan műszaki állapotban legyenek, hogy ne kelljen meghibásodás miatt kiállniuk.

A szállítmány esetében a mélységi védelem a 3. ábrán látható módon valósul meg. Az 1. számmal jelzett egységek jelképezik azokat az egységeket, amelyek nem részei a közvetlen kíséretnek, és adhatják az első detektáló és védelmi vonalat: felderítés végző civil ruhások, lakott terület esetén a közterületen levő rendőrök, a zárógépkocsik és személyzetük, az előfutó autó és személyzete stb. A 2. szám jelöli a közvetlen kíséretet, a 3. szám pedig a szállítójárművet, amennyiben rendelkezik a megfelelő mechanikai védelemmel és detektáló eszközökkel, vagy pedig a szállító konténert. Látható, hogy egy támadás esetén még ha az 1. és 2. védelmi vonalon át is jutnának a támadók, akkor is adhat még elegendő késleltetést a 3. vonal a külső reagáló erők megérkezéséig.

3. ábra: A mélységi védelem megvalósulása szállítmány kísérésekor [14]

2.3.1 Megállóhelyek biztosítása és intézkedések az emelt szintű fizikai védelemre

A szállítás megtervezése során törekedni kell arra, hogy a szállítmány a lehető legkevesebbszer álljon meg és egy-egy megállás ideje ne haladja meg az 1 órát. A Kormányrendelet előírása, hogy az 1 órát meghaladó megállás esetén a szállítmánynak jelen esetben B szintű, az alkalmazás és tárolásra vonatkozó fizikai védelmet kell biztosítani jogtalan eltulajdonítás ellen. [4] Ez a feltétel is erősíti azt a javaslatot, hogy a rendőrség és vagy a TEK már a szállítás tervezésétől vegyen részt a folyamatban, ugyanis ők rendelkeznek olyan mennyiségű felszerelt egységgel, amelyek képesek egy nem tervezett megállásra reagálni és a megfelelő védelmet biztosítani.

A B szintű tárolási fizikai védelem esetében a védett anyag körül három védelmi vonalat kell kialakítani, amelyek sorrendben kívülről kezdve a D, C és B szintűek lesznek. Ezek a zónahatároknak előírt detektáló és késleltetési képességgel kell rendelkezniük. [4] Egy nem tervezett megállás esetén a probléma, hogy hogyan lehet ezt biztosítani. A cél, hogy a három védelmi zóna kialakításra kerüljön a 4. ábrán látható módon. Az 1. számmal jelölt egységek azok, amelyek a közvetlen kíséretben nincsenek benne, de a megállóhely külső, D szintű biztosítását adják. Ezek lehetnek egyenruhás, illetve civil ruhás rendőrök. A 2. számmal jelölt egységek alkotják a C zónahatárt. Ezek a közvetlen kíséret és gépjárműveik. A 3. számú egység alkotja a B szintű védelmi vonalat. Ez lehet a szállító gépjármű karosszériája vagy a szállító konténer és a sofőr, valamint a kocsikísérő. Ennél a megoldási módnál a detektálásról elsősorban az élőerő gondoskodik, de lehet alkalmazni mobil detektáló és késleltető eszközöket vagy pedig a megfelelő technikával felszerelt drónokat is. [15] Ilyenkor biztosítani kell egy lokális őrségközpontot a riasztások fogadásához, illetve továbbra is el kell látni információval a szállítás biztonsági központot. A késleltetésről az élőerő, a védelmi zónákba beállított gépjárművek és a szállítókonténer, valamint az üzemanyag kazetták tömege gondoskodik.

4. ábra: A mélységi védelem megvalósulása a megállóhelyen [16]

A Kormányrendelet 3.§ (1) da) pontja kimondja, hogy amennyiben a nemzeti fenyegetettség hirtelen megemelkedik, abban az esetben az OAH, a kijelölt rendvédelmi és nemzetbiztonsági szervekkel egyeztetve, elrendelheti lokálisan vagy országos szinten az emelt szintű fizikai védelem bevezetését. [17] Bár az FVr. hatályba lépése óta ilyenre még nem volt példa, az eshetőségre mindenképpen fel kell készülni. Ez a tény egy újabb megerősítése a jogszabályi változtatásnak, hogy a rendvédelmi szervek vegyenek szervesen részt a folyamatban.

Az emelt szintű fizikai védelem bevezetéséről haladéktalanul tájékoztatnia kell a szállítás felügyelő őrségközpontot és a kíséret parancsnokát. A beérkező információk feldolgozását követően az alábbi lehetőségeik vannak: a szállítmány megerősített kíséretet kap az út hátralevő részére, a szállítmány visszafordul a kiinduló állomásra és a helyzet változásáig ott marad vagy pedig egy kijelölt köztes megállóhelyre megy és ott várakozik. Mindegyik esetben szükség van plusz állami erők bevonására. Ez akkor tehető meg a leggyorsabban, ha ezek a szervezetek már kezdettől fogva tudnak a szállítmány helyzetéről, illetve az egységeik készenléti állapotban vannak. A kiválasztáskor figyelembe kell venni, hogy előfordulhat, hogy az emelt szintű állapot hosszabb ideig fennmarad. Erre az esetre is készíteni kell tervet (egy új, megerősített szállítás más útvonalon vagy módon például).

A kiindulási állomásra való visszafordulás akkor lehetséges, ha ott adott a megfelelő védelem vagy a felállításának a lehetősége. Ezért az itt található készültséget a szállítás teljes ideje alatt fenn kell tartani.

A végállomásra való eljuttatás opció esetén a beérkezést követően a kazetták kirakodását a friss fűtőelem tárolóba, a megfelelő rendészeti biztosítás mellett, haladéktalanul meg kell kezdeni.

Köztes megállóhelyet akkor érdemes előzetesen kijelölni, ha a szállítási útvonal hossza miatt lehetnek olyan szakaszok, amelyeknél az első két opció nem lehetséges vagy nem ajánlott. Ilyen megállóhelynek olyan telephelyet célszerű választani, amely rendelkezik valamilyen védelemmel már és rendelkezésre állnak ott reagáló erők. Ilyenek lehetnek rendőrségi vagy katonai telephelyek vagy olyan más cégek, akik az üzemanyag kazettákkal azonos védelmi szintű radioaktív anyagot alkalmaznak vagy tárolnak. Ezeken a helyeken a készültséget a szállítás teljes ideje alatt fenn kell tartani.

Bármelyik megoldást is választják szükségessé válhat a kíséret megerősítése. Ezt a kísérő járművek és erők számának növelésével lehet megtenni, illetve kiegészítő védelmi lehetőségek is szóba jöhetnek, például légi kíséret biztosítása vagy az útvonalon a rendőri jelenlét és ellenőrzés fokozása.

3 Konklúzió

A Paksi Atomerőmű friss üzemanyaggal való ellátása közúton keresztül nem ütközik jogszabályi akadályba. A vonatkozó jogi előírások módosítása viszont elősegíthetik, hogy a folyamat során magasabb védelmet lehessen biztosítani a szállított nukleáris anyagnak. A szállítás lebonyolításához megfelelő szállítójárművek kialakítása vagy beszerzése szükséges, illetve olyan útvonalak kiválasztása, amelyeken probléma nélkül el lehet érni a végcélt és amelyen megfelelő megállóhelyek jelölhetők ki szükség esetére. A kíséretben résztvevő állománynak olyat kell kijelölni, amely végzett már bármilyen más közúti szállítás vagy delegáció biztosítását vagy pedig gondoskodni kell a megfelelő kiképzésükről és felkészítésükről. A köztes megállóhelyek védelme, illetve az emelt szintű fizikai védelem bevezetésekor szükséges intézkedések más területekhez hasonlóan megoldhatóak.

A közúti szállítási mód bevezetésével biztosítható, hogy a vasúti közlekedés szüneteltetésekor is ellátható legyen az atomerőmű, illetve a rövidebb időnek és útvonalnak köszönhetően kisebb állomány is elegendő a teljes védelemhez.

Irodalomjegyzék

[1] Első alkalommal érkeztek Magyarországra légi úton szállított friss erőművi fűtőelem-kazetták. Országos Atomenergia Hivatal. 2014. október 9. http://www.haea.gov.hu/web/v3/OAHPortal.nsf/web?OpenAgent&article=news&uid=5975C22F0021959BC1257D6C003D3D33

[2] 1996. évi CXVI. törvény az atomenergiáról. (Különösen 30.§ (1) a))

[3] 190/2011. (IX. 19.) Kormányrendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről.

[4] Berek, L., & Solymosi, J. (2015). Veszélyes anyagok szállításának biztonsága: Bolyai Szemle. XXIV. évfolyam, 2015/2. szám. NKE Szolgáltató Kft. Budapest

[5] 190/2011. (IX. 19.) Kormányrendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről. 5.§ (2) bekezdés.

[6] B/15684. számú jelentés az atomenergia 2015. évi hazai alkalmazásának biztonságáról. Magyarország Kormánya.

[7] [8] 47/2012. (X. 4.) BM rendelet az atomenergia alkalmazásával összefüggő rendőrségi feladatokról. 5.§ paragrafus.

[8] Kiégett Kazetták Átmeneti Tárolója. RHK Kft. online ismertetőanyag. http://www.rhk.hu/docs/KKAT_harant_web.pdf

[9] [10] Hózer, Z.(2015). Az új paksi reaktorok üzemanyag. Fizikai Szemle. LXV. évfolyam 2015/12. szám. Eötvös Loránd Fizikai Társulat.

[10] DMS s.r.o.vállalat honlapja. https://www.dms.cz/en/engineering/package-assemblies/

[11] Berek, L., & Vass, A. (2017) Transzformátor állomás szállítása közúton. Hadmérnök. XII. évfolyam 3. szám.

[12] 190/2011. (IX. 19.) Kormányrendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről. 29.§ (5) bekezdés.

[13] Kép eredetije: http://hvg.hu/itthon/20170130_putyin_latogatas_budapest_tek

[14] Kovács, T., & Viplak, A. (2017) Drónok a biztonságtechnikában. Hadmérnök. XII. évfolyam 2. szám.

[15] Kép eredetije: https://www.vezess.hu/magazin/2015/02/03/mit-tud-a-merkelt-vedo-pancelozott-audi/

[16] 190/2011. (IX. 19.) Kormányrendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről. 3.§ (1) da)

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

A Magyarországon meglévő és a férőhely hiány miatt létesítendő büntetés-végrehajtási szervezet biztonsági rendszereivel szemben támasztott általános követelmények

Exposition of requirements claimed on security systems for existing and newly to be established prisons in Hungary

Bagi Tamás Zoltán
Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Magyarország
bagit@elinor.hu

***Összefoglalás* — Magyarország Kormánya a következő években a Büntetés-végrehajtási Szervezetben férőhely bővítési programot hirdetett, amelynek keretében 2019-ig új standardizált büntetés-végrehajtási intézet építését tervezi, amelyek egyenként ötszáz illetve ezer fő befogadására alkalmasak. En-nek megfelelően a Belügyminisztérium irányítása alá tartozó Büntetés-végrehajtás Országos Parancsnoksága 2015. január 26-án pályázati felhívást tett közzé. Az alapvető cél, hogy a léte-sítendő új büntetés-végrehajtási intézetek kialakítása az Európai Börtönszabályok követelmény-rendszerének, CPT ajánlásainak, valamint az Emberi Jogok Európai Bírósága által támasztott követelmények számbavételével valósuljon meg, azoknak messzemenőkig megfeleljen.**

***Kulcsszavak*:** követelmények, biztonsági rendszer, fehér könyv, biztonsági intézkedések

***Abstract* — The Government of Hungary has announced a capacity expansion program for the Hungarian Prison Service Organisation for the next few years planning to establish new standardized prisons by 2019 each of them accommodating either five hundred or a thousand convicts. Ac-cordingly, the Hungarian Prison Service under the guidance of the Ministry of Home Affairs published an invitation to tender on 26 January 2015. Basic objective is to design new prisons in compliance with the requirements of the European Prison Rules, the CPT's recommenda-tions, as well as the Human Rights imposed by the European Court, all of which the new insti-tutes should largely meet.**

***Keywords*:** requirements, security system, white book, safety measures

1 BEVEZETÉS

*A biztonság fogalmának értel*mezése: az emberekben a kezdetektől fogva egészen a mai modern társadalmakig megvolt és meglesz az igény, hogy megvédjék saját magukat, és a hozzájuk közel álló vagy tartozó személyek életét, és megszerzett javaikat. Összefoglalva „A biztonság személyek és szervezetek azon állapota, melyet, a létüket, illetve rendeltetésszerű működésüket veszélyeztető tényezők és az azokkal szemben alkalmazott védelmi erőforrások együtthatása határoz meg.”. Természetesen, ahogy fejlődött a tudás és a technika, ez a feladat az emberiség számára úgy vált egyre nehezebbé és összetettebb feladattá. A Magyar Értelmező Kéziszótár meghatározása szerint: „A dolgoknak, életviszonyoknak olyan rendje, olyan állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek nincs, vagy alig van lehetősége, amelyben ilyentől nem kell félni”. [1], [2], [3]

A biztonság alapvetően két területre bontható: személy és vagyonbiztonság. A személybiztonsági részbe tartozik az emberi élet védelme, a testi épség védelme és a személyi szabadság.

A vagyonbiztonság körébe sorolható az objektumok biztonsága, amelybe beletartoznak a speciális objektumok is. Ide tartozik a rendezvények biztosítása, a pénz-, és értékszállítás, valamint a szállítmánybiztosítás is. Az objektum latin eredetű szó, és olyan épületet, műtárgyat vagy létesítményt jelent, amelyeket veszélyeztetettségüknél fogva, vagy egyéb ok miatt őrizni és védeni szükséges. Az objektumokat több tényező szerint is lehet csoportokba sorolni. (pl. funkció, elhelyezkedés, védettség foka, veszélyesség foka stb.). Az így kialakított csoportokat eltérő objektumbiztonsági és védelmi szintek jellemzik, különösen igaz ez a speciális funkciókat ellátó objektumok esetében. [4]

2 BÜNTETÉS-VÉGREHAJTÁSI SZERVEZET BIZTONSÁGI RENDSZERÉNEK FELÉPÍTÉSE

A büntetés-végrehajtási szervezet (büntetés-végrehajtási intézetek, intézmények, és a hozzájuk tartozó gazdasági társaságok) az állam biztonsági rendszerén belül helyezkedik el, a köz-rend és közbiztonság alrendszerében. Ahogy a legtöbb állami felügyelet alatt álló intézmény rendszer, úgy a büntetés-végrehajtás is hierarchikus rendszerben működik, amelynek csúcsán a Büntetés-végrehajtás Országos Parancsnoksága áll, mint középirányító szervezet. A büntetés-végrehajtási szerv eltérő feladatai alapján, mint ahogy az objektumok közötti eltérő csoportok esetében is a biztonsági rendszerüket a saját feladatuknak és felépítésüknek megfelelően kell, hogy kialakítsák, figyelembe véve a törvényi és anyagai lehetőségeiket.

Összefoglalva „A büntetés-végrehajtási szervezet biztonsági rendszere azon szabályok, valamint tárgyi, személyi és szervezeti elemek összessége, amely biztosítja a büntetés-végrehajtási szervezetek jogszabályban

meghatározott feladatainak biztonságos körülmények közötti ellátását." [5]

A büntetés-végrehajtási szerveknek olyan költséghatékony biztonsági rendszert kell kialakítania és üzemeltetnie, amely megfelel az Európai Börtönszabályok követelményrendszerének, CPT ajánlásainak, valamint az Emberi Jogok Európai Bírósága által támasztott követelményeknek, és folyamatosan biztosítja a fogvatartottak őrzését, felügyeletét, ellenőrzését. A biztonsági rendszernek biztosítani kell továbbá a büntetés-végrehajtási szervek őrzését és védelmét, valamint a személyi állomány testi épségének megóvását, ezzel a jogszabályban meghatározott feladatainak biztonságos ellátását. [9]

A büntetés-végrehajtási szervek biztonsági rendszerének főbb elemei: a büntetés-végrehajtási szervezet tevékenységére vonatkozó hatályos jogszabályok, rendeletek, utasítások, szervezeti egységek, személyi állomány, biztonsági létesítmények, biztonsági berendezések, technikai- és kényszerítő eszközök, okmányok.

Jelenleg Magyarországon működő büntetés-végrehajtási intézeteket a büntetés-végrehajtási fokozatok szerint sorolhatjuk fegyház (legszigorúbb), börtön, fogház (legenyhébb) szintűnek. Ezek alapján az egyes intézetek felépítése, kialakítása, a fogvatartás módja, valamint a biztonsági rendszerei jelentősen eltérnek.

1. ábra – Veszprém Megyei Büntetés-végrehajtási Intézet
http://bv.gov.hu/bv-intezetek

2. ábra – Tiszalöki Országos Büntetés-végrehajtási Intézet
http://bv.gov.hu/bv-intezetek

3. ábra – Balassagyarmati Fegyház és Börtön
https://upload.wikimedia.org/wikipedia/commons/8/86/Balassagyarmat_-_Megyeh%C3%A1za.jpg

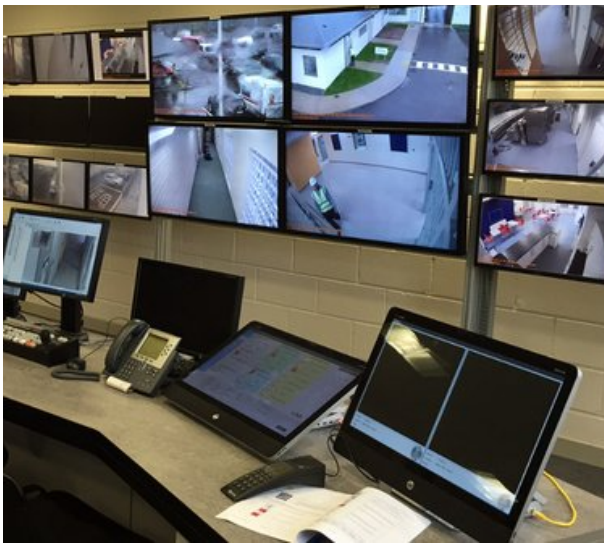
Ezeket az eltéréseket nem csak a korábban említett büntetés-végrehajtási fokozat szerinti különbségek okozzák. Ezek az eltérések adódhatnak az intézetek építésének időbeli eltéréséből földrajzi, illetve építészeti adottságaikból, és a rendelkezésre álló anyagi forrástól. Néhány büntetés-végrehajtási intézet/intézmény egy már korábban meglévő, azonban nem börtönként funkcionáló objektum felhasználásból, átalakításából került kialakításra.

Például a Tökölön található börtön 1959-ig internáló táborként működött. Az ugyanezen a területen elhelyezkedő rabkórház a múlt század 20-as éveiben huszárlaktanya működött, amely 1958-ig a honvédség birtokában volt, különféle funkciókat betöltve. A volt lovassági kaszárnya jelenleg a kórház épülete. [6]

4. ábra – Tököli Országos Büntetés-végrehajtási. Intézet, Fiatalkorúak Büntetés-végrehajtási Intézete, Büntetés-végrehajtás Központi Kórház
http://hirado.cms.mtv.hu/wp-content/uploads/sites/7/2015/10/CEGER19990914211.jpg

Az évtizedekkel ezelőtt épült intézetek esetében folyamatos az igény azok fejlesztésére és modernizálásra. A cél, hogy a kornak megfelelő, modern biztonsági rendszereket alakítsanak ki, hogy azok megfeleljenek a jelenkori elvárásoknak.

5. ábra – Szegedi Fegyház és Börtön
http://m.cdn.blog.hu/ko/konyves/borton-2070.jpg



6. ábra – Szegedi Fegyház és Börtön
https://img.rasset.ie/000baa40-614.jpg

A Büntetés-végrehajtás Országos Parancsnoksága 2015. januárban pályázati felhívást tett közzé, amely kapcsán Önkormányzati területeken 5 új börtön építését szeretné megvalósítani 2019-ig. Az új börtönök kapacitása 500, illetve 1000 fő. A kialakításuk hasonlóan a meglévő büntetés-végrehajtási intézetekéhez- meg kell, hogy feleljen a hatályos jogszabályi előírásoknak és az európai ajánlásoknak, ezen túlmenően költséghatékonynak és modernek is kell lenni-ük.

3 Létesítendő intézetek funkcionális felépítése

A büntetés-végrehajtási intézetben a személyi állomány, a kiszolgáló egységek, és a fogvatartottak elhelyezését és foglalkoztatását úgy kell kialakítani, hogy lehetőleg egymáshoz csatlakozó, blokk-rendszerűen, egymással rövid úton, megfelelő ellenőrzés mellett átjárható egységekből álljon. [7]

Egy intézethez 10 db elkülöníthető egységet lehet meghatározni:

a) külső biztonsági egység,
b) beléptető egység,
c) látogató egység,
d) befogadó egység,
e) parancsnoki egység,
f) fogvatartotti elhelyezéssel, befogadással, foglalkoztatással, vallásgyakorlással és sportolással kapcsolatos egység,
g) egészségügyi egység,
h) élelmezéssel, karbantartással és raktározással kapcsolatos egység,
i) munkáltatással kapcsolatos egység,
j) kutyatelep egysége

A biztonság tekintetében alapvető elvárás a fogvatartás biztonságának fenntartása. Ez azt jelenti, hogy olyan állapotot szükséges kialakítani és folyamatosan fenntartani, amelynél a büntetés-végrehajtási intézetben, illetve a büntetés-végrehajtási feladat teljesítése miatt a büntetés-végrehajtási intézet területén kívül tartózkodó személyek élete, testi épsége, szabadsága, a büntetés-végrehajtás anyagi javainak sértetlensége, valamint a büntetés-végrehajtási feladatok zavartalan ellátása biztosított legyen. Ehhez az intézetek területén belül egy több pillérre épülő összetett biztonsági rendszert szükséges kialakítani, amely statikus elemeken túl a kor elvárásainak megfelelő modern, – a személyi állomány automatikus kiértesítésére is alkalmas – számítógép vezérlésű biztonságtechnikai rendszert foglal magába.

A külső védelmi rendszer a „Fehér Könyv”-ben foglalt követelményeknek megfelelően az újonnan létesítendő objektumokat legalább 4 méter magas, mászásra alkalmatlan műszaki megoldásokkal rendelkező bástyafallal kell körülvenni. A bástyafal és közvetlen környezetének láthatóságára körvilágítási rendszert kell telepíteni, amely a szükségáramforrásról is (aggregátor) üzemeltethető. Erre praktikusan az alacsony energia felvételű, hosszabb élettartamú és lehetőleg a jelenleg alkalmazott hagyományos nátriumgőz lámpáknál nagyobb fényáramú LED világítást célszerű alkalmazni. A bástyafal megfelelő szilárdságú és a biztonsági célokat kielégítő építőanyagból kell, hogy készüljön, amely megfelelő betonalappal rendelkezik. A felülete sík, perem, illetőleg rés nélküli, a színe világos. A bástyafalat úgy kell kialakítani, hogy azon kapaszkodásra, elrejtőzésre, mászásra alkalmas kiszögellés ne legyen, ha ez nem valósítható meg, akkor azokat a helyeket az áthaladást nehezítő műszaki akadállyal kell ellátni. Műszaki akadályként elsődlegesen pengeéles dróthengert kell telepíteni.

Az objektum külső őrzésére az objektum sarkain, illetve a gépjárműbejáratnál, a fal síkjában őrtornyokat kell építeni. Az őrtorony kialakításánál elsődleges szempont, hogy a 360°-os megfigyelés mellett biztosítani kell az ott szolgálatot teljesítő személyi állomány külső támadás elleni védelmét is (pl. biztonsági, lövedékálló üveg)

7. ábra – Illusztráció
http://metmark.hu/media/otlethaz/images/1377601380/metmark_p182vndsh615qk1j23kltg5819qq7.jpg

8. ábra – Illusztráció
http://www.metmark.hu/old/000_fotoalbum/07_biztonsagtechnika/album1/img_06.jpg

A bástyafaltól a belső terület felé, 5 méter távolságra pengeéles dróthengerrel megerősített biztonsági kerítést kell építeni. A biztonsági kerítés földfelszíntől mért magassága 4 méter legyen. Készülhet fémhálóból, lemezből vagy pengeéles drótból. A tartóoszlop lehet fémből vagy vasbetonból, a közöttük lévő távolság legfeljebb 3 méter.

A kerítésnek 20 cm széles, 20 cm magas (talajszinttől) egybefüggő betonlábazatot kell építeni. A fémhálót, illetve a dróthengert legalább 20 cm-enként a lábazathoz kell erősíteni.

9. ábra – Illusztráció
http://expandaltlemez.hu/images/gallery//1332519107_1.jpg

A bástyafal belső oldala mellett legalább 2 méter szélességben nyomsávot kell kialakítani úgy, hogy a talaj nyomképzésre alkalmas legyen. A nyomsávba való belépés tilalmát figyelmeztető táblával, a nyomsáv határát pedig egyéb eszközzel egyértelműen jelezni kell.

A bástyafalt és a biztonsági kerítés között, illetve a kerítés belső vonalától számított 5 méter távolságon belül építmény (beléptető épületet kivéve), fa vagy a terület áttekinthetőségét akadályozó, illetve az akadály leküzdését elősegítő egyéb tárgy nem helyezkedhet el.

A bástyafaltól a belső terület felé, attól néhány méter távolságra pengeéles dróthengerrel megerősített biztonsági kerítést kell építeni. A biztonsági kerítés és a bástyafal közé, illetve a fogvatartottak elhelyezési épülete körül mikrohullámú áthatolás jelzőrendszert vagy infrasorompót kell telepíteni, amellyel a szökési kísérletek és az objektumba történő behatolási kísérlet észlelhető. Ezt a rendszert további elektronikus megfigyelési eszközökkel szükséges kiegészíteni a kívánt biztonsági szint eléréséhez.

Az épületeken kívül és belül egyaránt további biztonságtechnikai eszközöket (kamerák, mozgásérzékelők stb.) kell telepíteni a belső mozgások kontrollálására, dokumentálására.

A külső és belső területek megfigyelésére alkalmazott kameráknak a korlátozott fényviszonyok között is értékelhető képet kell tudniuk rögzíteni holttér mentesen. Alapvető követelmény, hogy az intézet területén történő bármely eseményt a zárt láncú fix és forgó kamerák képein keresztül egy központi ügyeleti helységben telepített munkaállomáson több monitoron, illetve monitorfalon történő megjelenítéssel lehessen nyomon követni. A forgó kamerák riasztáskor automatikusan ráfordításra kerülnek a riasztási területre.

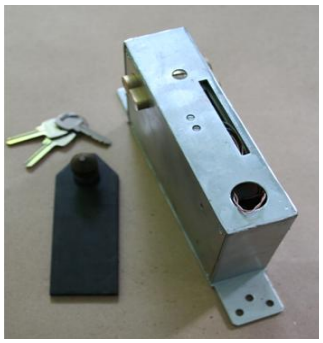
10. ábra – Illusztráció- többmonitoros rendszer
http://bloximages.newyork1.vip.townnews.com/godanriver.com/content/tncms/assets/v3/editorial/8/47/8478a32e-a42e-11e4-a78c-67263f532a8a/54c441ca95edc.image.jpg

11. ábra – Illusztráció - monitorfal
http://www.nyugatijelen.com/pictures/xbigs/72957.jpg

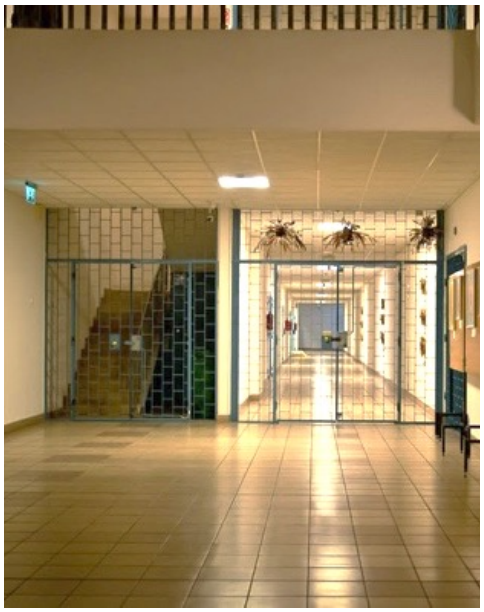
A közterületekre nyíló bejáratokat olyan biztonsági kapukkal kell ellátni, amely igazodik az épület funkciójához, jellegéhez. Ezen túlmenően az építészeti és területi sajátosságokat figyelembe véve minden olyan helyiségre, amelyet a fogvatartottak használnak, vagy ideiglenesen igénybe vehetnek, biztonsági ajtót kell telepíteni. A zárkaajtókat mindkét oldalon legalább 1,5 mm vastagságú acéllemezzel borított, acélszerkezetű kivitelben kell elkészíteni. Az ajtókat a büntetés-végrehajtásnál rendszeresített, legalább három ponton záródó, kizárólag a folyosó felől működtethető zárószerkezettel (kilinccsel és zárbetéttel) kell ellátni. Az ajtókon betekintő, ételbeadó és szellőző nyílást kell kialakítani, amelyek, a folyosóra kifelé nyithatók legyenek. Emellett ezekre a biztonsági ajtókra állapotjelzőket is kell telepíteni.

A távműködtetésű ajtókra kizárólag olyan elektromechanikus zárakat lehet felszerelni, amelyek feszültség nélkül zárt állapotban maradnak. Az elektromechanikus zárnak kulccsal is nyithatónak, zárhatónak kell lennie.

12. ábra – Illusztráció – Dunamix Kft.
http://forum.dunamix.hu/kepek/zajto.JPG



13. ábra – Zárkazár
http://forum.dunamix.hu/kepek/zajto.JPG



14. ábra – Illusztráció –
http://galeria.hir24.hu/files/376/055/000/55376/55376_434999_784x523.jpg

15. ábra – Elektromechanikus zár
http://zaruzlet.hu/elektromos_zar.html

A bejárati ajtókat (beleértve a személy- és gépjármű bejárati kapukat, illetve az elhelyezési épület bejáratait) zsiliprendszerű, távműködtetésű ajtókkal kell kiépíteni.

16. ábra – Zsiliprendszer (kívül és belül)

Az intézetben a meghatározott ajtókat olyan mechanikus és elektromos működtetésű zárral kell ellátni, amelyek egységes, ún. mester kulcsos rendszerben üzemeltethetők.

A zsiliptéren belül kapukeretes fémkereső, valamint röntgensugaras csomagvizsgáló berendezéseket kell telepíteni. A technikai eszközök az őrhelyről működtethetők, illetve ellenőrizhetők legyenek. Az épületben a zsiliptéren kívül várakozó helyiséget kell kialakítani azon személyek számára, akik kizárólag kísérettel mozoghatnak a büntetés-végrehajtási intézet területén. Az ellenőrzési területről nyíló, technikai eszközökkel ellátott külön helyiség kialakítása szükséges a személymotozás végrehajtására. A beléptető épületben, a zsiliptér mellett biztosítani kell egy olyan helyiséget, amelyben a büntetés-végrehajtási intézet területére be nem vihető tárgyak (szúró-, vágó eszköz, fegyver, mobiltelefon), biztonságos elhelyezése (lemezkazettákban, csomagmegőrző szekrényekben) megoldható. Az optimálisan zsilipelt ellenőrzési térből a személyi állomány, a szolgálati vagy hivatali ügyben eljárók, valamint a hozzátartozói látogatók útvonalát külön lehet választani. Ebben az épületben, de különálló blokkban kell kialakítani a látogatók (hozzátartozó, ügyvéd, rendőrségi meghallgató, stb.) fogadására szolgáló helyiségeket.

17. ábra – Illusztráció – csomagátvizsgáló rendszer
http://www.electromax.com/images/Rapiscan/rapiscan%20527.gif

18. ábra – Kapukeretes fémkereső
http://zandz.hu/wp-content/uploads/2015/12/HI-PE_Plus_femkereso_kapu1.jpg

19. ábra –Kézi fémkereső
http://www.metector.hu/wp content/uploads/2013/05/garrett-super-scanner-v-kezi-femkereso-3.jpg

A teljes objektumban vezeték nélküli személyriasztó rendszert kell kiépíteni, amely segítségével vészjelzés adható az intézet bármely pontjáról, valamint a szolgálati helyek között biztosítani kell a kettős kommunikációs összeköttetést (EDR rádió, őri jelző telefon… stb.).

4 Összegzés

Az új büntetés-végrehajtási intézetek tervezése során célszerű a standardizált megoldások használata és előnyben kell részesítenie a rohamosan fejlődő biztonságtechnikai eszközöket. A korszerű technikai berendezések alkalmazása a büntetés-végrehajtási intézetekben, mint veszélyes objektumokban lehetővé teszik a fogvatartás jogszerű végrehajtását, valamint megkönnyítik a személyi állomány munkáját és csökkentik a rendkívüli események bekövetkezésének kockázatát.

Irodalomjegyzék

[1] Farkas Ferenc, Sztodola Tibor, Hanzi Attila: Büntetés-végrehajtási Biztonsági Jegyzet, Büntetés-végrehajtási Szervezet Oktatási Központja, Budapest 2007, 6.oldal

[2] Berek Lajos, Berek Tamás, Berek László: Személy- és Vagyonbiztonság, ÓE-BGK 3071, Budapest 2016, 7. oldal

[3] Magyar Értelmező Kéziszótár http://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara/kereses.php?kereses=biztonság; (2016.12.30)

[4] Berek Lajos – Objektumok biztonsága+SP.pptx; (2016.12.30)

[5] A Büntetés-végrehajtás országos parancsnokának 26/2015. OP Szakutasítása a büntetés-végrehajtási szervezet Biztonsági Szabályzatának kiadásáról, I. fejezet 2. pont

[6] A Tököli Országos Büntetés-végrehajtási Intézet története http://bv.gov.hu/tokol-az-intezet-tortenete (2016.12.31.)

[7] A „Fehér Könyv" – 500 fő (és 1000 fő) fogvatartott elhelyezésére alkalmas bv. intézet tervezési követelményeinek meghatározására; 2.0 változat; (2016.08.05)

[8] Berek Tamás – Elek Imre: Zárszerkezet, mint a mechanikai védelem sebezhető pontja Mű-szaki Katonai Közlöny XXV. évfolyam, 2015. 3. szám 47-58 p. ISSN 2063-4986 http://www.hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2015_3_sz/2015_3sz.pdf

[9] Kínzást és az Embertelen vagy Megalázó Bánásmódot vagy Büntetést Megelőzni Hivatott Európai Bizottság (CPT) http://www.cpt.coe.int/lang/hun/hun-standards.pdf (2016.12.30)

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Elektronikus vagyonvédelmi rendszerek lehetséges kiegészítő funkciói

Possible additional features of electronic property protection systems

Beszédes Bertalan
Óbudai Egyetem, Alba Regia Műszaki Kar, Székesfehérvár, Magyarország
beszedes.bertalan@amk.uni-obuda.hu

***Összefoglalás* — A cikk a komplex vagyonvédelmi rendszereknek, azok elektronikai védelmet megvalósító komponenseivel foglalkozik. Ezen belül kiemelten az elektronikus kültéri védelem, a behatolást jelző rendszer és a beléptető rendszer lehetséges kiegészítő funkcióinak ismertetésével. A bemutatott megoldások hardverigény tekintetében törekszenek a rendszer költségeinek alacsonyan tartására, valamint a szoftveres lehetőségek kihasználására.**

***Kulcsszavak*:** elektronikus vagyonvédelmi rendszer, kültéri védelem, behatolás-jelző rendszer, radar szenzor, ultrahangos távolságmérő, jelenlét érzékelés, rezgésérzékelő, piezoelektromos szenzor, gyorsulás érzékelő, beléptetőrendszer, személyazonosítás.

***Abstract* — The article deals with the electronic protection component, within the complex property protection systems. In particular, it describes the possible complementary functions of electronic outdoor protection, the intrusion detection system and the access control system. The solutions presented here is aimed to keeping the system's hardware costs low, and to use software opportunities.**

***Keywords*:** electronic property protection system, outdoor protection, intrusion detection system, radar sensor, ultrasonic distance meter, presence detection, vibration sensor, piezoelectric sensor, acceleration sensor, access control system, personal identification.

1 BEVEZETÉS

Az elektronikai védelem feladata a behatolás, behatolási szándék érzékelése és értesítés küldése az élőerős védelem számára. Az élőerős védelem helyszínre vonulásának és megfelelő reagálásának következtében a vagyon elleni támadás elhárítható. [1]

A rendszerben kritikus tényező az idő. Ha az élőerős védelemnek nincs lehetősége a jogellenes behatolás és távozás időtartalma alatt a helyszínre érni és intézkedni, a behatoló elmenekülhet az esetleges-en megszerzett javakkal. Az elektronikai védelem képes a behatolást jelezni, mielőtt a behatoló a védett épületen, épületrészen belül kerülne – így megnövelve a reagálásra fordítható időt. Ebben az esetben a rendszernek elengedhetetlen összetevője – a védendő értéktől függően – a megfelelő szintű mechanikai védelem, amelynek célja a behatolás akadályozása, behatolásra fordítandó idő kitolása.

2 ELEKTRONIKUS VAGYONVÉDELMI RENDSZER FELÉPÍTÉSE

Az elektronikus kültéri védelmi és behatolás-jelző rendszerek egy központi egységből, legalább egy érzékelőből és kiépítéstől függően egy vagy több beavatkozó és/vagy értesítő egységből épülnek fel.

A központi egység fő feladata a riasztórendszer vezérlése, a különböző egységei közötti kommunikáció biztosítása, a beérkező adatok értelmezése, és a beavatkozásra képes egységek vezérlése. Kültéri védelemi és behatolást jelző rendszerek feladata a védett területre történő behatolás érzékelése. A beavatkozó egység célja a behatolóval szembeni fellépés, az értesítő egységé pedig értesítés küldése az élőerős védelemnek.

2.1 Eszközök közötti kommunikáció

A részegységek közötti kommunikáció történhet vezetékes vagy vezeték nélküli összeköttetésen. Az egységek a megfelelő eszközökkel zavarhatók, tönkretehetők, ezért célszerű megfelelő árnyékolással ellátni ezeket. A vezetékezés is alkalmas a zavar felvételére és az egységekbe történő bejuttatására. Célszerű árnyékolt vezetékezést használni (akár kétszeresen árnyékolt kábelt), valamint a vezetékeket zárt csőhálózatba telepíteni. Az ilyen kialakításnál, a csőcsatlakozásokkal szemben elvárás a csőszakaszok közötti jó galvanikus kontaktus biztosítása, illetve az elektromágneses hullámokkal szembeni jó csillapítóképesség. A kiterjedt fémhálózatot mind zavarvédelmi, mind életvédelmi szempontból csatlakoztatni kell az egyenpotenciálra hozó hálózattal. A fenti kiépítés nagyban megnöveli a telepítés anyag- valamint munkadíj-költségét is, csak indokolt esetben célszerű alkalmazni.

A vezeték nélküli összeköttetés mentesíti a felhasználót a vezetékezés költségeitől – különösen utólagos telepítés esetében. A vezetéknélküli érzékelő anyagköltsége viszont magasabb a vezetékes, hasonló paraméterű érzékelőénél. Az optimális megoldás sok esetben egy hibrid rendszer kiépítése. Lehetőségként kínálkozik a behatolók számára a vezetéknélküli egységek jeleinek elnyomása, helyettesítése, így az említett megoldás kisebb biztonsági szintet eredményez. Megoldásként kínálkozik a vezetékhálózaton érkező, valamint elektromágneses sugárzás formájában megjelenő zavaró jelek érzékelése, kiegészítő érzékelő segítségével. Amennyiben a zavarjel vagy zavarsugárzás meghalad egy előre meghatározott

szintet, az alrendszer jelzést küld a központnak, amit az szabotázsként érzékel [2].

Célszerű egy külső szerverrel is lekérdezni (a szerver felé jelenteni) a központ működőképességét. Amennyiben a központ nem ad életjelet vagy hibakódot küld, a szerver értesíti az élőerős védelmet. A behatolónak lehetősége nyílhat beépülni a kommunikációs csatornába, így elfedni, meghamisítani az üzenetváltást. Amennyiben alkalmazott ez a megoldás, lehetőség van egy, a központnál elhelyezett, fizikailag védett, galvanikusan leválasztott, csak egyirányú adatforgalmat megengedő, írható adattároló telepítésére. A központ az említett másodlagos háttértárolóra archiválhatja a kiküldött és vett üzeneteket. Amennyiben a külső szerveren tárolt adatok és a másodlagos háttértárolón tárolt adatok nem egyeznek meg, szabotázs történt [2]. Az élőerős védelem feladata az adatok összehasonlítása.

Az élőerős védelem értesítése hagyományosan történhet számítógéphálózati eszközökön keresztül vagy GSM hálózaton keresztül. Kínálkozik egy eddig még nem alkalmazott alternatív csatorna is a kis adatmennyiség átvitelére. A Narrow Band-IoT egy szabványosított, LTE infrastruktúrán használható mobil technológia, alkalmas kis adatmennyiségek átvitelére. A meglévő mobilhálózatot használja, ezzel biztosítva van a jó lefedettség, licens-elt (1-2€ / év eszközönként), azaz a szolgáltató garantálja a minimális sávszélességet és a hálózathoz való hozzáférést. Célszerű több csatorna egyidejű használata az élőerős védelemmel történő kommunikáció során.

A központi egység is tartalmaz akkumulátoros tartalék-áramforrást. Lehetőség van a szigetüzemű tápellátásoknál is alkalmazott megoldások telepítésére is [3]. Fontos, hogy a rendszer fel legyen készítve az ilyen irányú támadások elhárítására is, például a napelemek vezetékein keresztüli zavarás, túlfeszültség érzékelésére, levezetésére. Indokolt esetben kiépíthető redundáns tápellátási rendszer is [4]. Az említett megoldás szintén jelentősen növeli a telepítés költségeit.

2.2 Kültéri védelem és behatolást jelző rendszerek

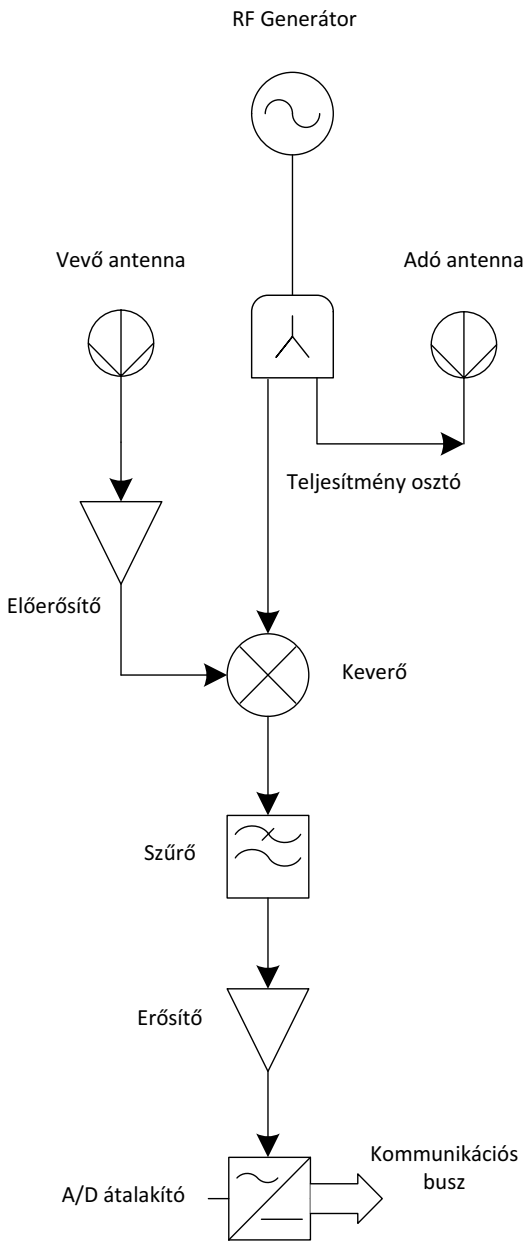
A behatolás érzékelésére és a behatoló tevékenységének nyomon követése érdekében védelmi köröket kell létrehozni. A fentieket a kültéri védelem, a felületvédelem vagy héjvédelem, az épületen belüli térvédelem, és a tárgyvédelem eszközeivel biztosíthatjuk. [1]

Mozgás- és/vagy jelenlétérzékelésre a gyakran alkalmazott lépésjelzők, a mágneses térérzékelők, infrasugaras eszközök, mikrohullámú eszközök, passzív infraérzékelők, rezgésérzékelők mellet lehetőség van videó megfigyelő rendszerek telepítésére is.

Cél a költséghatékony kiegészítő lehetőségek bemutatása, ezért a továbbiakban elsősorban az alacsony költségű radar szenzorok, ultrahangos távolságmérők, és rezgésérzékelők ismertetése és alkalmazási lehetőségei következnek.

2.2.1 Radar szenzorok

A radar szenzorok egy adó és egy vevő egységből állnak, felépítésük blokkdiagramja az 1. ábrán látható. Felhasználásukkal, egy objektumról visszaverődött jel feldolgozásával nyerhető információ. A Doppler effektus kihasználásával [5] nem csak a szenzortól való távolság mérésére, hanem az objektum sebessége is megállapítható, a visszavert hullám frekvenciájának változásából – jellemzően nx10Hz (2. ábra). (A sebességadat a szenzor szempontjából vizsgálva igaz.) Az üveget leszámítva minden általános építőanyagon keresztülhatolva képesek érzékelni a jelenlétet, így fa, műanyag vagy gipszkarton burkolat mögé, vakolattal vagy tapétával fedett kötődobozba is elhelyezhetők.

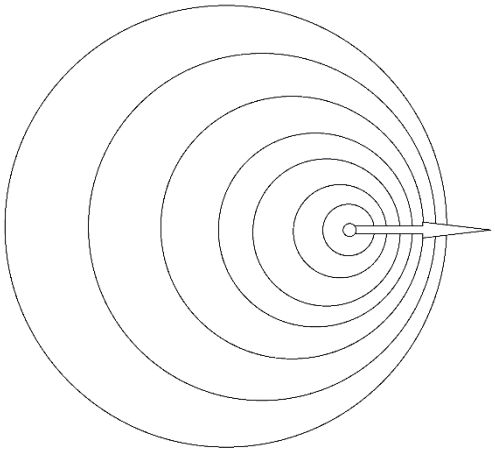


1. ábra: Radar szenzor általános blokkdiagramja

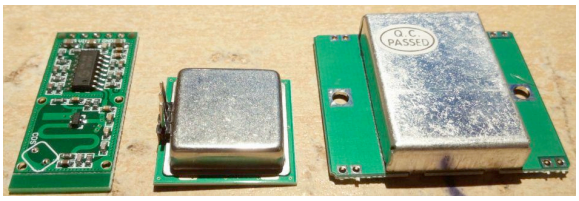
A különböző típusú, polgári célokra kiépített riasztórendszerek kiegészítésére használható, költséghatékonyan beszerezhető modulok a 3. ábrán láthatók, a hozzájuk tartozó főbb tulajdonságok az 1. táblázatban vannak összegezve. A baloldali típus, az elvégzett kísérletek alapján inkább csak jelenlét érzékelésre, távolság mérésére alkalmas, a másik két típus az említetteken felül alkalmas sebesség mérésére is.

A bemutatott radar szenzorok felhasználhatók a kültéri védelem területén, például: épület megközelítése, épület vagy oszlop melletti elhaladás, ajtó megközelítésének

érzékelésére. Valamint jól használhatók térvédelem eszközeiként, például: folyosón történő haladás, ajtó megközelítésének érzékelésére.



2. ábra: Doppler-effektus



3. ábra: Radarszenzorok: RCWL-0516, PD-V11, HB100

1. táblázat: Radar szenzorok jellemzőinek összehasonlítása

	RCWL-0516	PD-V11	HB100
Árfekvése	500 HUF	1300 HUF	1500 HUF
Érzékelési szögtartomány	360°	180°	180°
Működési frekvencia	3.181 GHz	24.125 GHz	10.525 GHz

2.2.2 Ultrahangos távolságérzékelők

Az ultrahangos távolságérzékelők működési elve a mikrohullámú radar szenzorokhoz hasonló. Ebben az esetben is egy adó és egy vevő modul szükséges az érzékeléshez. Az adóból induló jelsorozat egy – méréshatáron belüli – objektumról történő visszaverődés segítségével jut el a vevőbe, a jelkibocsátás és a jelfogadás közötti időkülönbségből becsülhető az objektum és a szenzor távolsága.

A hang levegőben történő terjedési sebessége függ a hőmérséklettől és a páratartalomtól. Ezen paraméterek mérése nélkül is jól alkalmazható a szenzor jelenlét érzékelésére és távolság becslésére, de pontos távolságméréshez szükség van a légtér tulajdonságainak vizsgálatára. A hőmérséklet és páratartalom mérése elvégezhető kisértékű szenzorok segítségével, a korrigált távolság az alábbi kifejezés segítségével adható meg:

$$d = (v_0 + 0{,}606*T + 0{,}0124*H)*t / 2 \qquad (1)$$

ahol v0=331,39m/s, az ultrahang sebessége száraz közegben, 0°C-on, T a hőmérséklet Celsius fokban, H pedig a páratartalom.

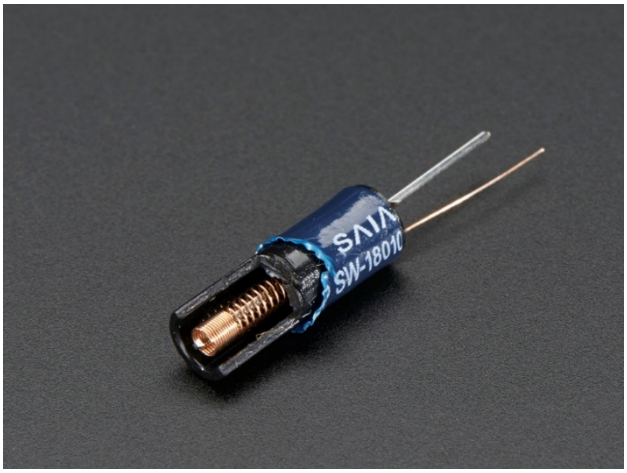
Fontos megjegyezni, hogy az ultrahangos távolságérzékelők beltérben alkalmazhatóak. A légmozgás könnyen eltérítheti az ultrahang-hullámokat, ezzel elkerülve a vevő modult, így hibás mérést eredményezve.

Térvédelemre viszont jól használhatók az egy modulban elhelyezkedő adó és vevő egységek, valamint a fizikailag különválasztott adó- valamint vevő egység pár is. Utóbbi esetben lehetőség van egy üzemidőben változó tér mozgásra történő biztosítására. A riasztórendszer élesítésekor – egy statikus helyzetben – a hanghullámok az adóból kiindulva, csillapítva és visszaverődésekkel együtt érkeznek meg a vevőbe. A beérkező mintát az alrendszer tárolja, ehhez hasonlítja a később érkező mintákat. Ha a biztosított térben van olyan objektum, ami helyet vagy alakot változtat, akkor a hanghullámok csillapítása, visszaverődései megváltoznak. A megváltozott jel el fog térni az élesítéskor mintavételezett referencia jeltől, ami központba küldött riasztást kiváltó jel indítását fogja eredményezni. Az aktuális referenciamintától való megengedett eltéréssel befolyásolható az alrendszer érzékenysége.

Lehetőség van az ultrahangos szenzor radarszenzorral és PIR szenzorral való kombinált használatra a megbízhatóbb térvédelem kialakításának érdekében.

2.2.3 Rezgésérzékelők

Az alábbi alacsony anyagköltségű rezgésérzékelők jól használhatók a héjvédelem eszközeiként (4. ábra). A záródó kontaktus vagy a rezgés mintázata is információtartalommal bír az őt felügyelő alrendszer számára. A rugós rezgésérzékelők geometriai és anyagtulajdonságoktól függően változó karakterisztikákkal szerezhetők be. Kialakítástól függően választható alacsonyabb, illetve magasabb frekvenciákra érzékenyebb szenzormodulok, valamint a – például: ajtóra történő – rögzítés módjával is befolyásolható az érzékenység.



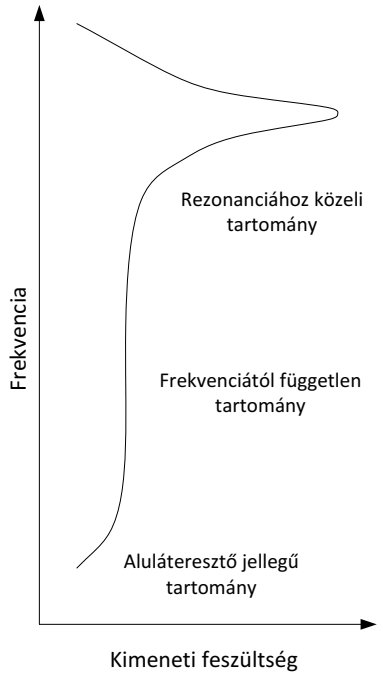
4. ábra: Rezgésérzékelő szenzor [8]

<u>Piezoelektromos szenzorok</u>

A piezoelektromosság olyan fizikai jelenség, melynél erőhatás következtében elektromos polarizáció (töltésszétválasztás) lép fel, így egyszerűen megvalósítható a mechanikai erőhatás – feszültség konverzió.

A magasabb frekvenciájú rezgésekre reagál [9] nagyobb kimeneti feszültséggel a szenzortípus (5. ábra). A széles

felhasználási lehetőségekből a héjvédelem és tárgyvédelem eszközeit kiemelve, jól és költséghatékonyan használhatóak, rezgések és vibrációk detektálására (6. ábra).

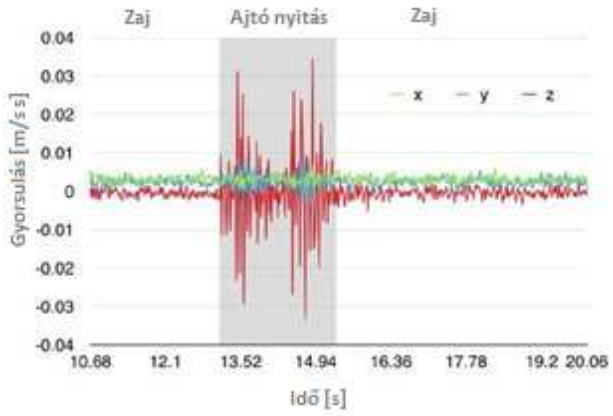


5. ábra: A piezoelektromos szenzor konstans amplitúdójú erőhatás hatására leadott a kimenetén megjelenő feszültség a frekvencia függvényében

6. ábra: Piezoelektromos érzékelő

MEMS modulok

Két és három tengelyes gyorsulásmérő szenzorok alacsony költségráfordítással beszerezhetők. Sok szenzor a tengelyek körüli elfordulás mérésére is képes. A szenzorokban elhelyezett, erőhatás bekövetkezésekor elmozdulni képes tömeg – a kondenzátor egyik fegyverzete – segítségével, a kapacitás-mérés elvére visszavezetve megállapíthatók a szenzort érő gyorsulás és elfordulás-értékek. Jól használhatók a tárgyvédelem és a héjvédelem területein, például: mozgatás, üvegtörés, ajtónyitás, fúrás, feszítés rezgéseinek érzékelésére. A szenzor jeleit feldolgozó alrendszer a mért értékek alapján képes megkülönböztetni a behatolásra jellemző jelalakot [10], például a szomszéd lakásban becsapott ajtó jelalakjától (7. ábra).



7. ábra: Mért gyorsulási értékek egy ajtónyitási próbánál

2.2.4 Fizikai jellemzők megváltozása

Héjvédelem esetében jól használhatók kiegészítő szenzorként behatolás detektálására a belső teret vizsgáló eszközök. A léghőmérséklet, páratartalom, légnyomás [11], széndioxid-szint, fényerő mért értékeinek lokális, nagy meredekségű megváltozása jelenthet egy ajtó- vagy ablak nyitást. Biztosabb a kiértékelés az épületen kívüli tér fizikai tulajdonságainak ismeretében.

Fontos a kiértékelést megzavaró tényezők figyelembe vétele a szenzorok elhelyezésekor, például: az ablakon bejutó napsugárzás fény és hőhatása, valamint a téves riasztásra okot adó események szinkronizálása az alrendszerrel, például: automatikus szellőztető vagy fűtő/hűtő berendezések használata. A jól felkészített belső tér monitorozó alrendszer jelzést kap a riasztórendszer részét nem képező belső tér tulajdonságait befolyásoló egységek működéséről, ez alapján módosítani tudja a megváltozott fizikai paraméterek által kiváltott szabotázs-jelzések súlyozását. A fenti alrendszer alacsony anyagi ráfordítást igényel, de jelentősen növelheti az elektronikus vagyonvédelmi rendszer megbízhatóságát.

2.3 Beléptető rendszerek

A beléptető rendszer feladata a védelmi körök határain – valamint az egy védelmi körön belül kialakított szakaszok határain –, átlépésére használható pontokon való átjutás szabályozása, a felhasználók jogosultságainak ellenőrzése, a felhasználók azonosítása, és a felhasználók áthaladásának szabályozása. A beléptetőrendszer kapcsolatot tart az elektronikus vagyonvédelmi rendszer központi egységével, illetve vezérli a szakaszhatárra telepített áthaladást engedélyező vagy tiltó beavatkozó egységet. [1]

2.3.1 Személyazonosítás

A dolgozat a személyazonosítás lehetséges módjaira tér ki részletesebben, továbbra is célul kitűzve a költséghatékony megvalósítási lehetőségek ismertetését. A személyek azonosítására szolgálóinformáció három csoportba sorolható be. Ezek a tudás alapú, a birtok alapú, és a biometrikus azonosítás.

Tudás alapú azonosítás

Tudás alapú azonosítás esetében a felhasználó a saját, titkos jelszavát adja meg a kezelőn. Jelszóegyezés esetében a kezelő engedélyezi az elektronikus vagy elektromechanikus beléptető egység működését. A leggyakrabban alkalmazott felhasználói felület a nyomógombokkal vagy érintő felületen kialakított billentyűzet. Egy újszerű koncepció a forgó jeladó(k), végállással rendelkező elfordulás mérő(k), toló kapcsolók felhasználói jelszóbeviteli lehetőségkét történő alkalmazása. A megszokottól eltérő kivitel nehezítheti a behatolást.

Kulcs vagy birtok alapú azonosítás

Célszerű a belépő személyének azonosítását is elvégezni a jelszó validálása mellett, így biztosítva a különböző felhasználókhoz tartozó jogosultsági szinteket, valamint a módszer felhasználásával naplózható a felhasználók tevékenysége is. Ezt nevezik kulcs vagy birtok alapú azonosításnak. Kiküszöbölhető az illetéktelen behatolás abban az esetben, ha a behatoló ismeri a felhasználói azonosító-jelszó párost és a belépésre jogosult felhasználó a rendszer által felügyelt területen belül helyezkedik el. Kiküszöbölhető, egy felhasználó kétszeri belépése ugyanarra a területre, illetve az egy felhasználó több különböző területen történő egyidejű jelenléte.

További megszorítások alkalmazásával a biztonsági szint növelhető, például: az egymástól beléptető rendszerrel elválasztott területek között csak a megengedett átjárókon keresztüli közlekedéssel, vagy riasztást generálva egy vagy több terület kihagyásakor, az utolsó kilépési ponttól fizikailag távoli belépést megkísérlő érvényes felhasználói azonosító-jelszó páros használatakor, vagy a felhasználó a területről történő kilépését követő és egy másik szomszédos területre történő belépési kísérlet között eltelt, az engedélyezettnél rövidebb vagy hosszabb időtartam esetében. Az említett lehetőségek feltétele a különböző beléptető rendszerek rendszerbe kötése, a központtal való kommunikáció biztosítása. A belépések darabszámának korlátozása is lehetséges egy adott területen -, egy adott időtartományon belül. Az időnként előforduló kivétel engedélyezése egy magasabb prioritási szinttel rendelkező személy számára elérhetővé tehető.

A fizikai kulcs lehet passzív, aktív vagy intelligens eszköz, az utóbbi a legmegbízhatóbb, beépített műveletvégző képességének köszönhetően. A megvalósított modell jelenlegi állapotában egy aktív RFID olvasóval képes a felhasználók megkülönböztetésére.

A beléptető rendszert fizikai valójukban, kezelő telepítési helyén jelen lévő személyek használják. Érdemes a kezelőnél elhelyezett szenzorral elvégezni a jelenlét érzékelését, az illetéktelen távoli engedélyezés kiküszöbölésének érdekében.

Radar szenzorok felhasználásával és további szoftveres kiegészítéssel, különbség tehető lassú, átlagos tartományon belüli és gyors mozgás között, például: előszobában elhelyezett beléptető kezelőfelület esetén, előírhatunk a megközelítésre vonatkozó mozgási szabályokat időtartamokhoz kötve.

Biometrikus azonosítás

A megszerezhető kulcs vagy jelszó nélküli, megbízható azonosítás nyújtja a legmagasabb biztonsági szintet de egyben ez a legköltségesebb megoldás is a megvalósításhoz igényelt hardver- és szoftvereszközök felhasználása miatt.

Továbbra is cél a költséghatékony megoldások, megoldási lehetőségek bemutatása. A biztonsági szint – ennek fényében – tovább növelhető, ha a fizikai kulcson kívül a belépésre jogosult személy biológiai egyedi tulajdonságai is validálásra kerülnek. Ez megvalósítható szoftveres modulok segítségével is.

A leggyakoribb billentyűzetes felhasználói felületen – mind nyomógombos, mind érintőképernyős kivitelben – alkalmazható az adatbeviteli eseményeket kísérő információ feldolgozása. A belépőre jellemző a billentyűk nyomva tartásának hossza és a gombnyomások vagy érintések között eltelt idő. Jellemző még a beviteli felület pontos helyének megnyomásától és a nyomás erősségétől függő rezgések egyénre jellemző vizsgálata is. A mérés elvégezhető egy gyorsulásérzékelő MEMS szenzor segítségével.

A jelszó beviteléhez köthető adatok felvételekor több minta vétele szükséges, ezekből meghatározhatók az egyes generált változókra elfogadható szélső értékek. Fontos figyelembe venni a felhasználó időbeli beviteli technikájának változását. Minden egyes belépéskor fontos lenne csúszóablakos elven tárolni a belépésre jellemző mért adatokat, és ezek alapján újra kalkulálni a megengedett szélsőértékeket. Az egyénre jellemző mért adatok szélsőértékből való kitérésekor, valamint a mért jellemző változásának dinamikájából fontos figyelmeztető, akár riasztást kiváltó esemény generálható.

Célszerű a három eltérő személyazonosítási elven alapuló módszer együttes, de egymástól független alkalmazása, a megbízható védelmi szint elérése érdekében.

3 MEGVALÓSÍTÁS

Egy, a bemutatott megoldások tesztelésére szolgáló riasztórendszer modelljének rendszerterve a 8. ábrán látható. A központi mikrokontroller vezérli a köré épített modulokat, egységeket. [12]

Az érzékelők – jelen kiépítésben – egy zóna-duplázott vezeték szakadásérzékelésre és egy jelenlét érzékelésére alkalmas ultrahangos távolságmérő modult foglalnak magukba.

A felhasználói felület a kezelőn helyezkedik el, tartalmazza a felhasználó azonosítására alkalmazott RFID modult (jelen kiépítésben a rendszer élesítése és inaktiválása is ezen a felületen keresztül történik), egy LCD kijelzőt és a gyors állapot kijelzésére alkalmas státusz LED-eket. [13]

Az adatok küldése és fogadása a külvilág felé két csatornán lehetséges: vezetékes etherneten keresztül és/vagy GSM hálózaton keresztül.

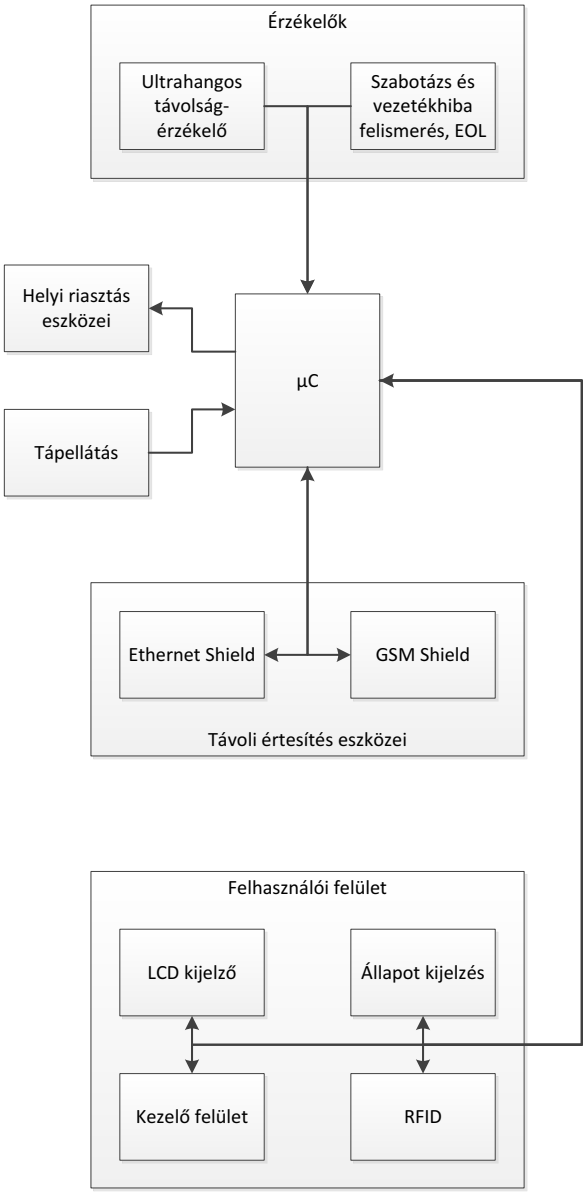
A riasztórendszer egyszerűsített, megépített modellje a 9. ábrán látható, az aktuális megvalósításban alkalmazott kiegészítő modulok az ábrán vannak jelölve.

A modellben alkalmazott ultrahang szenzor a HC-SR04. A szenzorba épített mikrokontroller a mért távolság függvényében változtatja a mintavételezés frekvenciáját a küldött és a fogadott jelek ütközésének elkerülése érdekében. (A kisebb távolsághoz nagyobb frekvencia társul.)

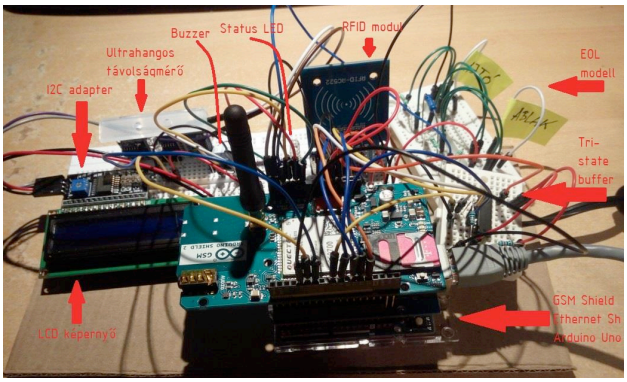
Az alkalmazott Ethernet shield és RFID író/olvasó modul is SPI buszon keresztül kommunikál a mikrokontrollerrel. Nehézséget jelentett az említett buszra kötött eszközök együttműködését hosszútávon, stabilan

biztosítani, ezért tri-state-es buffer fokozattal leválaszthatóvá tettem az eszközöket. Az Ethernet shield a buszról történő leválás után nem minden alkalommal tudott újra csatlakozni a rendszerhez.

A mikrokontroller bemeneti lábainak alacsony száma is korlátot jelentett a fejlesztés folyamán. Ez és az SPI busz megosztásának problémája vezetett el a továbbfejlesztett modell kialakításához, amiben két kontroller dolgozik külön feladatokon, de egymással kommunikálva. Az eddig is használt kontroller felel a külvilággal és a felhasználóval való kapcsolattartásért, az újonnan illesztett nagyobb lábszámú kontroller pedig az érzékelők lekérdezéséért valamint a riasztás és szabotázs érzékeléséért.



8. ábra: Rendszer architektúra



9. ábra: Megvalósított modell

4 Továbbfejlesztési lehetőségek

A hardver további bővítése mellett tervezem az említett szoftveres kiegészítő funkciók rendszerbe integrálását is. Miután a tervezett fejlesztések megtörténtek, szeretném vizsgálni a rendszer zavarállóságát is [14].

Véleményem szerint az egyedileg fejlesztett rendszerek megbízhatósága jelentősen nagyobb, mivel a behatoló nem képes a telepítés helyszínétől elkülönülve próbálkozni a rendszer megkerülésével, feltörésével – amennyiben a műszaki dokumentáció nem áll a behatolást tervező rendelkezésére.

Továbbá, szükséges még egy általános telepítői felület fejlesztése – amely csak telepítői jelszóval módosítható – a riasztórendszer könnyebb telepíthetőségének és testreszabhatóságának elősegítésére. A rendszer moduláris hardver és szoftver felépítése is támogatja az előirányzott fejlesztéseket.

5 Összefoglalás

A gyakran alkalmazott elektronikus vagyonvédelem által nyújtott hardverelemek és szoftveres megoldások mellet lehetőség van eddig még ritkán alkalmazott funkciók beépítésére is. Ezesetben cél a költségek alacsonyan tartása mellett egy komplexebb rendszer kialakítása, a biztonsági szint növelése. A bemutatott példák az előbbi feltételeket teljesítik az elektronikus kültéri védelem, a behatolást jelző rendszer és a beléptető rendszer esetében is. Az ajánlott megoldások relevanciája – a szerző reményei szerint – polgári és ipari területeken is jelentősek.

Irodalomjegyzék

[1] Berek Lajos. Biztonságtechnika. Budapest: Nemzeti Közszolgálati Egyetem. 2014. 48 p.

[2] György Györök, Bertalan Beszédes. Highly reliable data logging in embedded systems. In: Anikó Szakál, Iveta Zamecnikova. SAMI 2018: IEEE 16th World Symposium on Applied Machine Intelligence and Informatics : Dedicated to the Memory of Pioneer of Robotics Antal (Tony) K. Bejczy : proceedings. 237 p. Košice; Herlány, Szlovákia. 2018.02.07-2018.02.10. Seattle (WA): IEEE, 2018. pp. 49-54. ISBN:978-1-5386-4771-4

[3] Vass Attila, Berek Lajos. Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei. HADMÉRNÖK 24:(2) pp. 41-57. (2015)

[4] Györök György, Bertalan Beszedes. Fault tolerant power supply systems. In: Orosz Gábor Tamás. 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország. 2016.11.17. Budapest: Óbudai Egyetem. 2016. pp. 68-73.

[5] Doppler-effect. https://soundwavesreillymckennaaly.weebly.com/doppler-effect.html. (2018. május 13.)

[6] Continuous-wave radar. http://www.wikiwand.com/en/Continuous-wave_radar. (2018. május 13.)

[7] Fast Vibration Sensor Switch. https://andicelabs.com/shop/sensors/fast-vibration-sensor-switch. (2018. május 13.)

[8] http://www.nubbeo.com.ar/modulo-sensor-de-vibracion-sw420-tilt-arduino-nubbeo-549560390xJM (2018. május 13.)

[9] Piesoelectric sensor. https://en.wikipedia.org/wiki/Piezoelectric_sensor. (2018. május 13.)

[10] Michael A. Mahler, Qinghua Li, Ang Li. SecureHouse: A Home Security System Based on Smartphone Sensors. Department of Computer Science and Computer Engineering, University of Arkansas. IEEE International Conference on Pervasive Computing and Communications (PerCom). March 2017. https://www.researchgate.net/publication/313508127_Secure-House_A_Home_Security_System_Based_on_Smartphone_Sensors. (2018. május 13.)

[11] Muchen Wu, Parth H. Pathak, Prasant Mohapatra. Monitoring building door events using barometer sensor in smartphones. 2015 ACM International Joint Conference. September 2015. https://www.researchgate.net/publication/311490862_Monitoring_building_door_events_using_barometer_sensor_in_smartphones. (2018. május 14.)

[12] Dr. Györök György. Mikrokontrollerek hardver-hatékony alkalmazása. In: Nagy Rezső, Hajnal Éva. Garai Géza Szabadegyetem II. Székesfehérvár: Óbudai Egyetem, 2015. pp. 5-15. ISBN:978-615-5460-62-3

[13] Györök György. Programozható analóg áramkörök mikrovezérlő környezetben. Óbudai Egyetem, ISBN 978 615 5018 97 8, Budapest, 2013.

[14] Gy. Györök. A-class amplifier with FPAA as a predictive supply voltage control. In: 9th International Symposium of Hungarian Researcherson Computational Intelligence and Informatics (CINTI2008). 2008. 361–368. p.

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

A digitális állam információbiztonsága: kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban

Information security and the digital state: the role of the risk management principles in the strategic documents

Beláz Annamária
Óbudai Egyetem Biztonságtudományi Doktori Iskola, Budapest, Magyarország
belaz.annamaria@phd.uni-obuda.hu

***Összefoglalás* — Napjaink szolgáltató állam modelljének elsőszámú célja az ügyfél-elégedettség növelése, ennek megfelelően a hatékony közigazgatási rendszer kiépítése. Hazánkban az elmúlt évek digitális-állam kiépítésével összefüggő fejlesztési programjai is ezt a célt szolgálták. Nem szabad ugyanakkor elfelejteni, hogy a digitális állam kiépítésekor prioritást kell élveznie az információbiztonsági szempontoknak.**

A tanulmány célja, annak elemzése, hogy milyen szerepe van az információbiztonsági kockázatfelmérési és kezelési elvek megjelenésének a nemzeti stratégiai dokumentumokban, valamint annak bemutatása, hogy jelenleg milyen formában tartalmazzák a stratégiai dokumentumok meg ezen elveket.

***Kulcsszavak*:** információbiztonság, kockázatmenedzsment, stratégiai irányítás, közigazgatás, digitális állam

***Abstract* — The aim of our modern days` on demand government is to build effective efficient and economic public administration system and to increase client satisfaction. This is why electronic governmental services, identification and authentication processes developed continuously during the past few years in Hungary. The improvement programs on digital state building supported this goal as well. We cannot lose sight of the fact that during digitalisation programs in order to build an open, safe and secure digital state, cybersecurity aspect must be a priority.**

The purpose of the study is to present and analyse the role of the risk management principles in the current Hungarian national strategies. Moreover the research will examine their coherence with international standards.

***Keywords*:** information security, risk management, strategic governance, digital state, public administration

1 BEVEZETÉS

A hálózat alapú információs rendszerek létfontosságú szerepet játszanak a társadalmak mindennapi életében. A közigazgatás modernizációja és a digitalizálódás folyamata hozzájárul ahhoz, hogy a hatósági ügyintézési feladatok bekerüljenek a hivatali épületekből az állampolgárok lakásaiba, személyes okos eszközeibe, ebből kifolyólag ezeknek a rendszereknek megbízható működése és biztonsága létfontosságú. Ugyanakkor az információs rendszerek biztonságos működését veszélyeztető támadások nagyságrendje, gyakorisága és a hatása folyamatosan erősödik.

A statisztikai adatok alapján a 2017-es év első felében globálisan közel kétmilliárd adatrekord került illetéktelen eltulajdonításra, milliós károkat okozva ezzel a köz és magánszektornak egyaránt. Az eltulajdonított adatok huszonegy százaléka (404.244.346 adatrekord) a közszektorból származik. [1] Az illegális adatszerzés mellett számos egyéb információbiztonsági támadásnak vannak kitéve a közszféra szervezetei, többek között: szolgáltatásmegtagadással járó támadás, weblaprongálás, káros szoftverek, adathalászat, kéretlen levelek, jogosulatlan hozzáférés.

A szolgáltató állam közigazgatásának információs rendszere, az abban előállított, tárolt és továbbított adatok, valamint a rendszert használó személyek és szervezetek biztonsága érdekében szükséges, hogy a magyar közigazgatás rendelkezzen azokkal a minimumképességekkel, amelyekkel a megfelelő szintű védelem biztosítható. Ennek érdekében szükséges, hogy a fejlesztési programok szerves részét alkossák az információbiztonsági szabályok, valamint a területhez kapcsolódó kockázatfelmérési és kezelési elvek, megoldások. A következőkben röviden bemutatásra kerülnek a kockázatmenedzsmenttel kapcsolatos alapvető fogalmak és elvek.

2 KOCKÁZATFELMÉRÉS ÉS KEZELÉS: ELVEK, FOGALMAK

Miért fontos a kockázatmenedzsment a közigazgatási folyamatok tervezésekor és a modernizáció során? Akkor lehet sikeres egy modernizációs folyamat, ha minél teljesebb mértékben eléri a stratégiában megfogalmazott célokat. A célok eléréséhez egyrészt nélkülözhetetlen, hogy a célok világosan legyenek megfogalmazva, mérhető, követhető legyen az akciók végrehajtása. Másrészről azonban elengedhetetlen, hogy a stratégia végrehajtói, a vezetők jó döntéseket hozzanak, minimalizálva a kudarc lehetőségét. A kockázatok egyértelmű felmérése és kezelése segít a bizonytalanság csökkentésében támogatva a döntés-előkészítést és végrehajtást.

A tudományos gondolkodás és kutatás kiindulópontját mindig a vizsgált terület fogalomrendszerének áttekintése adja, így érdemes megvizsgálni legalább a kockázat fogalmát anélkül, hogy a fogalmi keretek tisztázása kapcsán túl mélyre merülnénk a kérdésben. A kockázat, kockázatmenedzsment, kockázatkezelés, kockázatértékelés fogalmak egyaránt használatosak a köz- és magánszférában, azonban a kifejezések értelmezése nem egységes. A kockázat definíciója eltérő az egyes tudományterületek és elméletek, mint például a pszichológia, orvostudomány, közigazgatás, pénzügy, szociológia megközelítésében. [2]

„A kockázat annak lehetősége, hogy egy olyan esemény történik meg, amely negatívan hat a célok elérésére.” [3]

„A kockázat általánosságban valamilyen esemény, tevékenység vagy tevékenység elmulasztása, amely a jövőben valószínűleg bekövetkezik, és ha bekövetkezik, akkor ennek általában negatív hatása van az adott szervezet céljainak elérésre.” [4]

„A kockázat valamely cselekvéssel, vállalkozással járó veszély, kár, baj, kellemetlenség lehetősége.” [5]

„A kockázat a bizonytalanság hatása a célokra.” [6]

Ezekből a meghatározásokból is világosan látható a kockázat fogalmaknak tartalmilag közös elemei: egy lehetségesen bekövetkező esemény és az esemény hatása(i), melyek veszélyeztetik a szervezet működését, az adott feladat, projekt végrehajtását. Az információbiztonság területén, a fogalmi keretek tisztázásához, az információbiztonsági rendszer kiépítéséhez és a kapcsolódó kockázatmenedzsment feladatok végrehajtásához érdemes követni a Nemzetközi Szabványügyi Testület (International Organisation for Standardisation, ISO) egységes iránymutatásait. [7] Az ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek című szabvány tartalmazza a kockázatmenedzsment [8] alapelveit, valamint a kockázatfelmérés és –értékelés lépéseit. A következőben ezek kerülnek bemutatásra.

2.1 A kockázatmenedzsment alapelvei

A kockázatmenedzsment lényegének megértéséhez és a kockázatmenedzsment stratégiai-szervezeti szintű megjelenítéséhez elsőként tisztában kell lenni a mögöttes alapelvekkel. A kutatás során így a stratégiai dokumentumok elemzésekor nagy hangsúlyt fektettem az alapelvek vizsgálatára, keserve a kockázatmenedzsment látásmód megjelenését ezen dokumentumokban.

A kockázatmenedzsment főbb alapelvei a következők:

A kockázatmenedzsment feladata az *értékek létrehozása és védelme*. A kockázatkezelés hozzájárul a célok kimutatható eléréséhez és a teljesítmény javításához a szervezet számos területén.

A kockázatmenedzsment *minden szervezeti folyamatnak részét alkotja*. A kockázatkezelés soha sem különül el a szervezet lényego folyamataitól és feladataitól, ellenkezőleg, a stratégiai tervezéstől a projektmenedzsmenten keresztül a változások kezeléséig minden területen áthatja a szervezeti működést.

A kockázatmenedzsment *a döntéshozatal szerves része*. A kockázatértékelés hozzájárul ahhoz, hogy a szervezet vezetői megalapozott döntéseket hozzanak, hiszen támogatja a valid információn alapuló releváns döntési alternatívák kidolgozását.

A kockázatmenedzsment központi feladata a *bizonytalanság fogalmának értelmezése*, természetének explicit módon történő megfogalmazása.

A kockázatmenedzsment *rendszerszerű, strukturált és időszerű*. A strukturált kockázatfelmérési és értékelési rendszer hozzájárul a hatékonysághoz, konzisztens, összehasonlítható és megbízható adatokat eredményez.

A kockázatmenedzsment *az elérhető legpontosabb tényeken, információkon alapu*l, többek között: korábbi adatok, tapasztalat, érdekelt felek visszajelzései, megfigyelései, előrejelzései és szakértői vélemények.

A kockázatmenedzsment *szervezetre szabott*, igazodik az egyéni igényekhez. A szervezet külső és belső környezetével, valamit a kockázati profiljával összhangban kell megalkotni.

A kockázatkezelési terv *megalkotásakor figyelembe kell venni a humán és kulturális tényezőket*, képességeket, látásmódokat, valamint a szervezetben dolgozó és azzal kapcsolatba kerülő külső személyek szándékait.

A kockázatmenedzsment *transzparens és inkluzív* folyamat, a megfelelő időben és mértékben szükséges az érdekel felek, kiváltképp a döntéshozók bevonása. Így a kockázatkezelés mindig releváns, időszerű lesz, a kockázati kritériumrendszer pedig figyelembe veszi a döntéshozók nézőpontjait.

A kockázatmenedzsment *dinamikus, ismétlődő és rugalmasan alkalmazkodik a változásokhoz*. A kockázatmenedzsmentnek olyan állandó folyamatnak kell lennie, amely érzékeli a szervezetben történő változásokat és folyamatosan alkalmazkodik hozzájuk. Számításba veszi, hogy a kockázatot jelentő tényezők, események változhatnak, eltűnhetnek és jöhetnek újak.

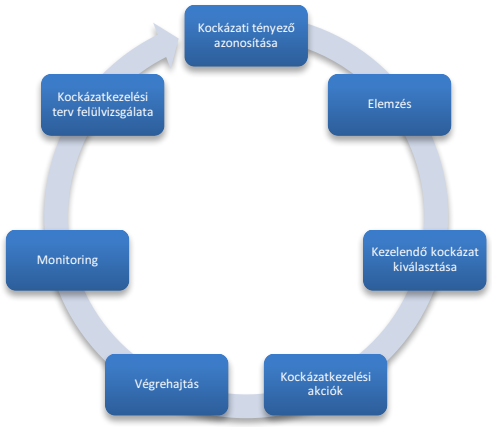
A kockázatmenedzsment *hozzájárul a szervezet folyamatos fejlődéséhez*.

2.2 A kockázatkezelési ciklus

Akárcsak a stratégiai tervezés, a kockázatkezelés ciklikus folyamat. Egyetlen szervezet sem állandó, még a kiszámíthatóságon alapuló bürokratikus közigazgatási szervezetrendszer is folyamatosan fejlődik, a belső és a külső környezete megújul. Ennek okán különböző időpontokban más és más tényezők jelentenek kockázatot egy adott szervezet számára, így a szervezeti működés fenntartása érdekében nem elegendő egyetlen alkalommal létrehozni egy kockázatkezelési tervet, majd a teendők listájáról „kihúzni”.

A kockázatkezelési ciklus a következő elemekből épül fel:

1. kockázati tényezők feltárása,
2. a feltárt kockázati tényezők elemzése,
3. a kezelendő kockázatok kiválasztása,
4. a kiválasztott kockázatokra kockázatkezelési akciók megfogalmazása
5. a kockázatkezelési feladatok végrehajtása,
6. nyomon követési és monitoring feladatok
7. a monitoring tevékenység során feltárt hiányosságok kezelése



1. ábra Kockázatkezelési ciklus elemei (saját szerkesztés)

A fogalmi alapvetés, valamint az alapelvek megismerése után a tanulmány további része a szolgáltató állam modell szerepét vizsgálja a digitális állam kiépítésével kapcsolatban.

3 A SZOLGÁLTATÓ ÁLLAMMODELL SZEREPE

Az állam és végrehajtó szervezetrendszerének szerepéről az állam- és közigazgatáselmélet területén végeláthatatlan viták folytak, s folynak napjainkig. A tudományos diskurzus során kiemelkedők azonban olyan szakaszok, ahol a közigazgatás lényegi tevékenysége sajátos karakterisztikát mutat. Napjainkban ezt a kiemelkedő szerepet a szolgáltató állam modell tölti be.

A szolgáltató állam koncepciója Max Weber szerint a kapitalizmus közigazgatásra gyakorolt hatásaként jött létre. Véleménye szerint a kapitalizmus támasztotta fel az állandó, megbízható, szilárd, hatékony, intenzív és racionálisan kiszámítható közigazgatás iránti igényt. [9]

WEBER elméletéből levezetve GAJDUSCHEK György megállapította, hogy a bürokratikus szervezetekben a kiszámíthatóság és a hatékonyság mindig egymással fordítottan arányosan van jelen, es a közigazgatás számára a kiszámíthatóság minden esetben prioritást élvez a hatékonysággal szemben. [10] Tehát a szolgáltató állam közigazgatásában, bár nagy mértékben mennek végbe modernizációs folyamatok, ezek végrehajtásakor mindig a kiszámíthatóságnak kell jellemeznie az átmenetet. A kockázatfelmérési és kezelési elvek

Todd RAMSEY A szolgáltató állam [11] című művében kifejti, hogy a szolgáltató állam, szemben a korábbi modellekkel (pl. éjjeliőr állam, jóléti állam), alapvetően proaktív, az ügyfél elvárásainak megfelelő, igény szerinti szolgáltatásokat nyújt, miközben gyakran támaszkodik a partnerekre, beszállítókra. Ramsey idézett művében a szerint határozza meg a szolgáltató államot, hogy a közigazgatási modernizáció mely ismérvek mentén zajlik. Hat egymással összefüggő ismérvet állapított meg, melyek a következők:

- a koncepció,
- a szervezeti kultúra,
- a működési modell,
- a technológiai infrastruktúra,
- az átalakítási menetrend és
- a távlatos gondolkodás.

Az információbiztonsági kockázatfelméréssel és kezeléssel kapcsolatban a legfontosabb ismérvek a szolgáltató állam működési modellje és a technológiai infrastruktúra. Egy szervezet által létrehozott értékeket a működési folyamatok adják. A szolgáltató típusú szervezetben a tevékenységek és a folyamatok a maximális ügyfélelégedettség elérésére optimalizáltak. Napjaink fejlesztési csapdája lehet azonban, hogy gyakran nem a lényegi (core) folyamatok és alaptevékenységek modernizációja, hanem a kiegészítő folyamatok és tevékenységek (non-core) fejlesztése történik meg, a kockázatmenedzsment teljes nélkülözésével. Ezért fordulhat elő az az állapot, hogy egy látszólag fejlett hivatal valójában közel áll az összeomláshoz, feladatait képtelen ellátni. [12] Fontos, hogy a technológiai infrastruktúra fejlesztése mindig a szervezet működési elveinek, folyamatainak kidolgozását kövesse.

Minél nagyobb egy állam, és minél szélesebb a feladatköre, annál jobban ki van téve a támadásoknak. Ez a megállapítás többszörösen igaz a szolgáltató állam modell tekintetében, hiszen a közigazgatás feladatköre egyre szélesebbé válik, továbbá a működés és az ügyintézés fókusza átkerül az offline térből az online térbe. A szolgáltató állam ügyfélorientáltsága tévesen elhamarkodott lépésekre ösztönözheti a jogalkotókat, azt eredményezve, hogy a digitális állam kiépítésének mihamarabbi elérése, mint cél mellett eltörpülnek az információbiztonsági, valamint az időigényes kockázatfelmérési és elemzési kérdések.

A továbbiakban vizsgálat tágyát képzik azon stratégiai dokumentumok, amelyek a digitális állami kiépítésével foglalkoznak, valamint a nemzeti biztonság kérdéseiről rendelkező szabályozások, tervek.

4 KOCKÁZATFELMÉRÉSI ÉS ÉRTÉKELÉSI ELVEK A STRATÉGIAI DOKUMENTUMOKBAN

Közpolitikai szempontból a stratégia egy meghatározott cél, állapot elérése érdekében végrehajtandó cselekvések, akciók hosszú távú terve. [13] A stratégiai dokumentum a cselekvések végrehajtása érdekében felelősöket jelöl ki, az akciókhoz erőforrásokat rendel. A stratégiai tervezés során a cél eléréséhez szükséges cselekmények részletes és módszertani szempontból következetes kidolgozása történik meg, beleértve a stratégia értékeléséhez és finomhangolásához szükséges folyamatokat is.

A Magyary-program keretében kialakításra került új stratégiai irányítási rendszer [14] azt a célt szolgálja, hogy a stratégiai szemlélet a kormányzati tervezés részévé váljon, a stratégiai dokumentumok pedig egy egységes hierarchikus rendet alkossanak. A döntéshozók és a végrehajtásban résztvevő személyek egyre inkább igénylik a stratégiai döntéstámogatás kialakítását, működtetését.

Miért fontos a kockázatkezelési elvek megjelenése a nemzeti szintű és ágazati stratégiai dokumentumokban?

Egy állam a hosszú távú céljait nemzeti stratégiai dokumentumokban fekteti le. Ezen dokumentumoknak tartalmazniuk kell a célok eléréséhez szükséges terveket, valamint az ezt megakadályozni képes kockázatokat. A közigazgatás egyes szerveinek célrendszerei csak akkor lehetnek egységesek, ha egy felsőbb szintű nemzeti dokumentum tartalmazza a fő irányvonalakat, keretrendszerként szolgál az alsóbb szintű dokumentumok elkészítéséhez. Hasonlóképpen az egyes szervezetek csupán önmagukra nézve állapíthatnak meg kockázati tényezőket, azonban egy országos szintű dokumentum átfogó képet tud nyújtani a fenyegetésekről, országos kockázati tényezőkről és mintaként szolgál az egyes közigazgatási szervek, hatóságok számára.

4.1 A digitális állam kiépítéséhez és az információbiztonsághoz kapcsolódó stratégiák

Digitális Nemzet Fejlesztési Program (NIS és Zöld Könyv)

„A jelenleg zajló Digitális Nemzet Fejlesztési Program elsősszámú dokumentuma a Nemzeti Infokommunikációs Stratégia 2014-2020 (NIS) [15] kijelölte a hazai informatikai és távközlési szektor fejlesztésének súlypontjait, és a digitális ökoszisztéma elemeinek (digitális gazdaság, elektronikus szolgáltatások, szükséges infokommunikációs infrastruktúra, az elektronikus szolgáltatásokat igénybe vevők bővítendő köre) összehangolt fejlesztését irányozta elő.

A Digitális Magyarország főbb céljai:

szupergyors internet elérhetővé tétele;

- a helyi közösségek, valamint a teljes magyar közösség összetartozásának erősítése a digitális technológia révén;
- az állam által nyújtott szolgáltatások fejlődése;
- az ország versenyképességének növelése a digitális szolgáltatások, valamint a digitális készségek terjedésének elősegítése által; valamint
- a digitális infokommunikációs alkalmazások, szolgáltatások elterjesztésének támogatásán keresztül az életminőség javítása minden élethelyzetben (magában foglalva a biztosságtudatosságra való oktatást).

A Digitális Nemzet Fejlesztési Program második kapcsolódó dokumentuma a Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól. [16] A Zöld Könyv akciótervi dokumentum, célja egyrészt a Nemzeti Infokommunikációs Stratégiában meghatározott intézkedések részletesebb kifejtése, az egyes intézkedések céljának, operatív teendőinek, becsült forrásigényének, az intézkedéstől várt eredmények és megvalósításért felelős intézmények megjelölése, másrészt a 2014-2020-as uniós tervezési ciklusban az érintett Operatív Programok keretein belül megvalósításra kerülő intézkedések koncepcionális megalapozása.

Nemzeti Biztonsági Stratégia

A magyar Kormány 2012. február 15-én fogadta el a hazai stratégiai rendszer legmagasabb szintjén álló dokumentumát, Magyarország Nemzeti Biztonsági Stratégiáját (NBS). [17] A Nemzeti Biztonsági Stratégia célja, az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése. Az elemzés alapján a stratégia meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.

Nemzeti Kiberbiztonsági Stratégia

A Nemzeti Kiberbiztonsági Stratégia [18] hivatott Magyarország kiberbiztonsági keretrendszerét felállítani és kijelölni az országos szintű kockázati tényezőket.

Logikai szempontból szoros összefüggésben áll több felső szintű dokumentummal, közvetlenül hivatkozik az Alaptörvényre és a Nemzeti Biztonsági Stratégiára, azonban nincsenek letisztázva a közvetlen kapcsolódási pontok a digitális állam kiépítésével kapcsolatban, mivel a Digitális Nemzeti Fejlesztési Program később jelent meg és a stratégiák összhangjának biztosítása nem történt meg.

Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014-2020

A dokumentum az egész közigazgatás fejlesztésére vonatkozóan határoz meg feladatokat, azzal a céllal, hogy a szolgáltató állam minél teljesebb kiépítése megvalósuljon hazánkban. A stratégia hatásterületei: a szolgáltató közigazgatás szervezési feltételeinek fejlesztése, a közigazgatás emberi-erőforrás gazdálkodásának fejlesztése, a közszolgáltatások színvonalának javítása, valamint a digitális állam felépítése.

4.2 Kockázatkezelési elvek megjelenése a digitális állam kiépítéséhez és az információbiztonsághoz kapcsolódó stratégiákban

Az alábbi táblázat összefoglalja, hogy milyen kockázatkezelési, -felmérési elvek jelennek meg az információbiztonság területén a nemzeti stratégiai dokumentumokban.

1. táblázat: Kockázatmenedzsment elvek megjelenése a stratégiai dokumentumokban (saját szerkesztés)

Kockázatkezelési elvek megjelenése a stratégiai dokumentumokban	
Nemzeti Infokommunikációs Stratégia	A dokumentum SWOT elemzés alapján megállapítja, hogy kockázati tényező az állampolgárok internetes szolgáltatásokkal szembeni bizalmatlansága. A kockázati tényezővel kapcsolatban a tudatosító programokat jelöli meg kezelési módszerként.
Zöld könyv az infokommunikációs szektor 2014-2020 közötti fejlesztési irányairól	A Zöld Könyv a NIS biztonság horizontális tényező tekintetében kiemeli, hogy a tervezett akciók hozzájárulnak a magyar közigazgatás elektronikus információbiztonsági szintjének emelkedéséhez, egyúttal a kockázatok csökkennek.
Nemzeti Biztonsági Stratégia	A stratégia 31. pontjában elsődleges feladatként határozza meg a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérését és priorizálását.

Nemzeti Kiberbiztonsági Stratégia	A stratégia bár a 4. pontjában említi a kibertérből érkező fenyegetések és az információs hadviselés kockázatát, nem tűz ki célokat és cselekvési tervet sem állít fel a kockázatok mérséklésére. Nem említi ezen kívül a kiberbűnözés kockázatát, különböző lehetséges vállfajait, valamint Magyarország kitettségét, fenyegetettségének mértékét az egyes kiberbűncselekmények tekintetében.
Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014-2020	Bár a stratégia fő célja a digitális állam kiépítése, az akciók között nem foglalkozik a kockázati tényezők felderítésével, értékelésével. Feladatként kijelöli az internetes szolgáltatásokkal kapcsolatos biztonsági kockázatok tárgyszerű megismertetését az állampolgárokkal, azonban a tudatosító tevékenység végzésének kijelölése nem minősül kockázatkezelési elvnek.

5 Összegzés

Az irodalomkutatás, a jogszabályok és stratégiai dokumentumok vizsgálatát követően megállapítható, hogy a szolgáltató állam modell kialakulása, valamint a digitális állam kiépítésére tett erőfeszítések megkövetelnék az országos stratégiai dokumentumokban a kockázatkezelési irányelvek megjelenését, azonban sajnálatos módon a kockázatmenedzsmenttel kapcsolatos rendelkezések nem csak az információbiztonság területén, hanem teljes mértékben hiányoznak ezekből a dokumentumokból.

A kockázatkezelési szempontok mellőzése a nemzeti szintű stratégiai dokumentumokból azt eredményezi, hogy az információbiztonság területén a közigazgatásban nem alakul ki egységes nézőpont, feladat és célrendszer, így az egyes közigazgatási szervezetek kockázatkezelési tervei struktúrájukban és szemléletmódjukban heterogének, horizontális nézőpontok nem jelennek meg bennük.

A fenyegetettségek és a célkitűzések megalapozottságának érdekében országos információbiztonsági kockázatelemzés és értékelés elvégzése szükséges. Az Európai Parlament és Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS Irányelv) című dokumentum meghatározza a nemzeti kiberbiztonsági stratégiák legfontosabb témáit. A rendelkezés külön pontként jelöli a kockázatok feltárására szolgáló kockázatértékelési terv elkészítését, a kockázatkezelési elvek megjelenítését. Úgy vélem a jogszabály alapján elkészítendő nemzeti szintű kockázatértékelés és kockázatkezelési terv megoldást jelenthet a tanulmányban feszegetett problémára.

Irodalomjegyzék

[1] Gemalto Breach level index: Findings from the first half of 2017 http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[2] VASVÁRI Tamás: Kockázat, kockázatészlelés, kockázatkezelés. Pénzügyi Szemle. 2015. 1. sz.

[3] Committee of sponsoring Organizations of the Treadway Commission (COSO): Enterprise Risk Management — Integrated framework, 2004 http:// www.coso.org/-ERM.htm

[4] Pénzügyminisztérium, Belső kontroll kézikönyv (útmutató), 2010 http://allamhaztartas.kormany.hu/belso-kontroll-szakmai-anyagok

[5] A magyar nyelv értelmező szótára I–VII. Kötet, Akadémiai Kiadó, Budapest 1962

[6] MSZ 13073:2014 Kockázatkezelés és –felmérés. Szakszótár.

[7] ISO 31000-es szabványcsoport, magyar nyelvű címekkel:
MSZ 13073:2014 Kockázatfelmérés és -kezelés. Szakszótár
MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek
MSZ EN 31010:2010 Kockázatkezelés. Kockázat-felmérési eljárások

[8] A kockázatmenedzsment/kockázatkezelés (Risk Management) nem más, mint „egy szervezet kockázattokkal kapcsolatos összehangolt irányítási és felügyeleti tevékenységei.”

[9] WEBER, Max: Gazdaság és Társadalom, KJK, Budapest, 1987

[10] GAJDUSCHEK György: A bürokrácia jelentései; In Közigazgatás szorítóban (szerk. Horváth M. Tamás) Unió, Budapest, 1998

[11] RAMSEY, Todd: On demand government – continuing the e-governmental journey, IBM Press, Lewisville, 2004

[12] BUDAI Balázs Benjámin: Az E-közigazgatás elmélete, Akadémiai Kiadó, Budapest, 2009.

[13] STEINER, George A.: Strategic Planning, Simon&Schuster, New York, 1979, o. 12-34.

[14] A Magyary Program Stratégiai Irányítási Rendszerrel kapcsolatos intézkedési tervéről bővebb információ: http://magyaryprogram.kormany.hu/strategiai-iranyitasi-rendszer, [online], 2017, Magyaryprogram.kormany.hu

[15] Digitális Nemzet Fejlesztési Program (1631/2014. (XI. 6.) Korm. határozat)

[16] Zöld Könyv http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Zöld%20Könyv.pdf [2018-06-04]

[17] 1035/2012. (II. 21.) Kormány határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[18] 1139/2013. (III. 21.) Kormány határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Identification of assets in the process of privacy protection

Ing. Matúš Ivančo, prof. Ing. Tomáš Loveček, PhD.
Faculty of Security Engineering, University of Zilina, Zilina

***Abstract* — Currently, the issue of personal data protection is a topical issue, because of the expected approval of the Personal Protection Act in the Slovak Republic, which will be the transposition of GDPR. The paper provides a guidance on identifying of assets and interrelated or interacting activities in connection with the process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework. In the context of a privacy risk management process, personally identifiable information will be considered as an asset. For the purposes of this article, the terms and definitions given in ISO / IEC 29100, ISO / IEC 29134, ISO / IEC 27000, ISO / IEC 27005, ISO Guide 73 will be used.**

***Keywords*:** privacy, identification, assets, processing of personal data, threats, risk

1 INTRODUCTION

The issue of the personal data protection is increasingly discussed subject at various national or international conferences. The obligation to deal with this issue no longer has arisen from law or technical standards, but rather from the need to provide sensitive (personal) information (e.g. IoT) to internal and external threats. The information and technological development of the company, in addition to the boom of classical information criminality (disruption of the basic attributes of information - accessibility, confidentiality, integrity), also has resulted in the development of methods of deep analysis and processing (e.g. Deep Learning) of Big Data, which represents a new, unresolved danger for the company. Information, from the point of view of the assets of the organization, becomes more valuable than other tangible or intangible assets. For this reason, it is necessary to pay attention to the protection of information, and in particular to information relating to a natural person (so-called personal data).

To ensure a sustainable security of information, it is necessary to introduce a systematic management mechanism that ensures correct treatment of the information used in the individual processes of the organization. Such guidance on the optimal mechanism for the handling of personal information (personal data) is provided in ISO / IEC 29 100: 2011 Privacy Policy. Regarding to the protection of personal data, the identification of the asset process transforms one of the initial steps in the information security management process.

2 ASSETS OF ORGANIZATION

In the process of risk management for information security, there are included identifying assets in the risk identification part, where the input for the Asset Identification process represents the range and limits of the risk assessment, the list of core components pertaining to owners, functions, locations, etc.

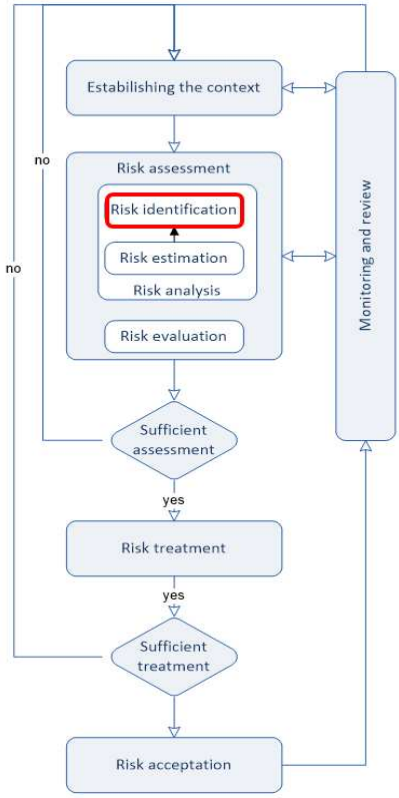


Figure 1: Information security risk management process [1]

Organization assets, whether business assets, employees or information, as well as company outputs, represent the value for the organization, next needed to be protected. Information and processing equipment assets should firstling be identified and the list of these assets should be updated on a regular basis. Each item in the asset list should be classified and assigned by the asset owner.

3 CLASSIFICATION OF ASSETS

The input of the asset identification process is defined by the scope and limits of risk management for information security. In order to determine the values of individual assets, they have to be identified. According to ISO / IEC 27005, the assets are divided as follows:

Primary assets include:

- Business activities and processes,
- Information.

Supporting assets, whose role is to ensure the integrity and connectivity of the primary assets:

- Hardware,
- Software,
- Networks,
- Locations,
- Organizations,
- Employees.

To assets into two groups (primary and supportive) enables us to understand the interrelationship between them and subsequently to create asset modules of the organization [2].

4 PRIMARY ASSETS

According to ISO / IEC 27005, business processes and information are further distributed as follows:

Business activities and processes, including processes:

- whose loss or limitation would not allow the organization to meet its main goals,
- which, if modified, can significantly affect the achievement of the main objectives,
- which are required to meet contractual legal or regulatory requirements,
- which contain secret processes (patented technologies).

Primary information is including:

- personal data are defined in the Privacy Act,
- information important to meet the organization's main goals,
- strategic information,
- Information requiring high financial costs, accumulation of storage, processing and transmission or requiring a considerable amount of time [1].

The fundamental difference between process and activity is primarily in the rate of generalization. In the term of the process, we understand any activity using resources and is managed to transform inputs to outputs. As follows from previous statement, the process is basically an activity or a sequence of activities that fulfill a predetermined goal.

The main input of each process or activity is information. On the basis of its character and content, the individual activities resulting in the desired output are subsequently performed.

From the point of view of the information security of the organization, they represent personal data, one of the most important components of the system that needs to be protected. Based on this knowledge, the regulation of European Parliament 2016/679 was issued in 2016. The regulation remarkably affects the whole process of information security management.

4.1 Classification of personal data

According to the regulation of the European Parliament 2016/679, the term personal information means *„any information concerning an identified or identifiable physical person. Identifiable physical person is a person who can be identified directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier, or a reference to one or more elements specific to physical, physiological, genetic, mental, economic, cultural or social identity of that person. "*

Among these specific identifying elements, we include in particular:

- **genetic data** - personal data concerning inherited or acquired genetic characteristics of a person and providing unique information on the physiology or health of that person
- **biometric data** - personal data resulting from specific technical processing related to the physical, physiological or behavioral characteristics of the natural person allowing to clearly identify the person
- **health data** - personal data relating to the physical or mental state of a person, including data on the provision of healthcare services [3]

5 SUPPORTIVE ASSETS

In order to ensure the processing of primary assets, it is necessary to identify support assets which threat directly affects the integrity of business activities and information. Different kinds of supporting assets can have occurred:

1. **Hardware** representing all processes supporting physical elements:
   - Data processing equipment:
     - fixed devices (PC, server),
     - portable devices (notebook, tablet, PDA),
     - peripheral devices (printer, removable disk drive).
   - Data carriers:
     - electronic media (CD, DVD, USB, HDD, SSD),
     - other media (paper, fax, slides).
2. **Software** representing all programs supporting the operation of hardware for data processing:
   - Operating system (Windows, Linux, OS X),
   - Service, management, or maintenance software (AMI, RiZone, Evis),
   - Software packages (Office 365, MySQL, Oracle),
   - Enterprise applications (Enterprise, Microsoft, Kros).
3. **Networks** representing a group of all telecommunication devices used to interconnect individual elements of the information system:
   - Communication interface (GPRS, Ethernet adapter),
   - Media and support (ADSL, FireWire, Bluetooth),
   - Active or passive transmission (router, switch, hub, bridge).

4. **Locations** shall include all places and physical means necessary for their operation:
   - Zones (access zones, security zones),
   - Compound (premises, building),
   - External environment (premises of other organizations, workers' homes),
   - Services (water supply, waste disposal, electricity supply),
   - Communications (telephone line, internal telephone networks),
   - Equipment (electricity, converter, air conditioning).
5. **Organizations** representing the entire organizational framework, consisting of all staff structures and procedures controlling the following structures:
   - Managing Authorities (Managing Authority, Organization Headquarters),
   - Organizational structure (security service, fire service, IT),
   - Project / System Organization (Information System Migration Project, New Application Development Project),
   - Suppliers / subcontractors / producers (purchasing services company, company management company).
6. **Employees** representing a group of persons involved in the information systems of the organization:
   - Managers (senior management, project managers),
   - Developers (enterprise application developers),
   - Operators and maintenance (system administrators, application operators),
   - Users (human resources management, finance, risk management) [1].

For the purposes of regulation No. 2016 / 679, processing means *"operation or set of operations with personal data or sets of personal data, such as retrieval, recording, arrangement, structuring, storage, reprocessing or alteration, searching, browsing, exploitation, transmission, or otherwise provided, regrouped or combined, limited, erased or destroyed, whether performed by automated or non-automated means."*

These processing operations are carried out by individual support assets.

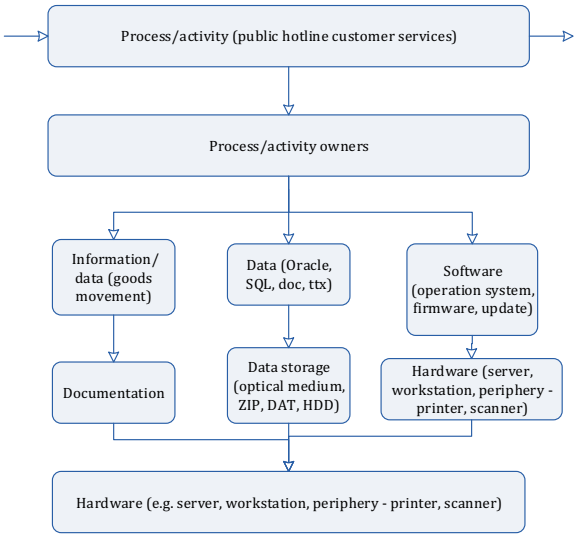


Figure 2: Dependence of organization's activities on assets [4]

6 LINKS BETWEEN PRIMARY AND SUPPORTIVE ASSETS

Defining links between asset types is an important part of the process of identifying primary and supporting assets. If we can't understand and describe their interrelationships and mutual links, we will not be able to evaluate the impact of individual identified threats using vulnerabilities in supporting assets.

One possible solution to the problem is to create asset modules. In the phase of its compiling, it is advisable to proceed from the process map of the organization. The asset module shows the linkage between specific primary and supporting assets with the purpose to realize a particular process, expressed as a primary asset. This approach is based on the knowledge that the information represents inputs or outputs of individual processes, and this information is accessible through specific software applications which data is stored on specific hardware devices located in specific areas and attended by specific owners. In this way, a certain dependency chain of specific assets is created. On its basis we know to accurately identify the likely vulnerable attack site and the amount of damage occurring after an attack [4].

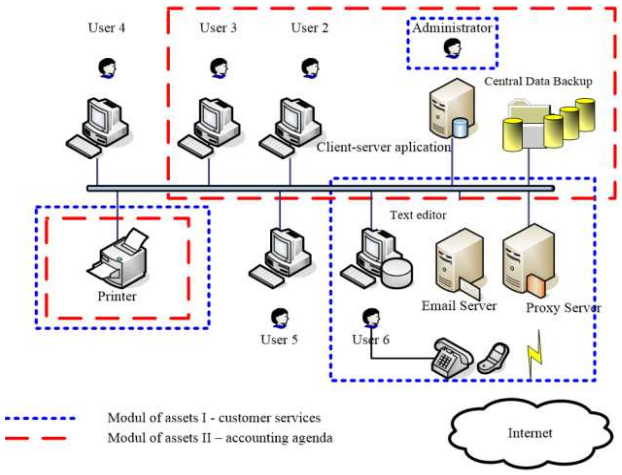


Figure 3: Example of creating modules of assets [4]

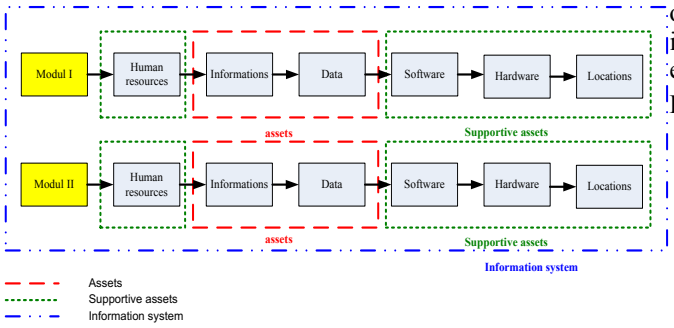


Figure 4: Example of information system in block diagram [4]

7 THREATS TO ASSETS

There is a high number of threats with effects on organization's assets, while they may differ in their source (hacker and water course), their form of expression (infringement of integrity, availability, confidentiality, or their combination), periodicity of occurrence (damaging code and an earthquake) or the extent of potential consequences. In general, we may divide threats into intentional and accidental, and further into external and internal ones.

Intentional threats are such threats, which source is a purposefully-acting natural person – attacker (organization's own employee, service-organization employee, strange person) with the aim to manipulate with organization's assets without authorization (e.g.: steal, misuse, damage, destroy, change). A motive or cause of such action may be profit, revenge, damage to interests/property, frequent staff migration, challenge, ego, rebellion, prestige, destruction of evidence, exploitation, political advantage, drawing attention of media, competitive advantage, economic espionage, curiosity or blackmailing.

Accidental threats are such threats which may arise independently from person's will. Their sources may be found inside or outside the organization. External accidental threats are such threats, which sources are found outside the organization and they operate from this space. They include environmental threats, technical threats and the so-called 'force majeure' threats. Force-majeure threats are to be understood as threats independent from person's awareness or acting (meteorite fall, deflection of the planet from Earth's axis). Environmental external threats are mainly disasters (sun eruptions, inundations, floods, fires, windstorms, landslides) where cumulated energies or masses are released excessively, possibly accompanied by destructive factors with negative impacts on assets. Technical external threats are mainly emergencies (explosion, fire) bringing about effects of destructive factors with a negative impact on assets. Internal accidental threats are threats; which sources are located inside the organization. Such threats may include social and technical threats. Internal accidental technical threats may be mainly crashes of technical devices forming a part of the organization, or technical failures of physical assets (Single Points of Failure). Internal accidental social threats are mainly represented by authorized persons who may, as a result of a lack of their knowledge (security awareness), forgetfulness or negligence, threaten the value of assets (blocking the access to a system after unsuccessful logins of an authorized person; unauthorized entry into an information system as a result of damaging security elements) [4].

Basic types of threats may be divided into:

- physical damage (fire, corrosion, freeze-up),
- natural disasters (climatic, seismic, floods),
- loss of basic services (air-conditioning breakdown or water supply malfunction, electric energy supply interruption),
- technical failure (device failure, overloaded network, maintenance error),
- threats to information (remote espionage, divulgement, forgery, wiretapping),
- threat to functionality (shortage of staff),
- unauthorized activities (unauthorized use of equipment, authorities, data processing, forgery),
- disruptions caused by radiation (electro-magnetic radiation, thermal radiation) [1].

8 CONCLUSION

The result of asset identification is a list of assets of the organization that provides the basis for the subsequent risk analysis impacting the assets. Without a thorough examination and knowledge of all information assets would be impossible to effectively protect the goals and mission of organization. For this reason, is necessary to introduce a systematic management mechanism for each organization to ensuring the correct handling of the information used in its individual processes. The importance of creating of given mechanism results from the growing threats of attacks on companies' personal data and their exploitation for commercial or criminal purposes. Each primary goal of organization is to ensure that its clients and employees are protected against threats that could harm their privacy. Therefore, the solution of this issue is currently considered to be one of the most important tasks of each organization.

REFERENCES

[1] ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.

[2] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council - Article 94 - Repeal of Directive 95/46/EC

[4] Kampová, K., Loveček, T.: Security systems - Managing security in organization. EDIS publishers, University of Žilina, 2007. ISBN 978-80-554-0615-2.

[5] ISO/IEC 29 100:2011 Information technology - Security techniques - Privacy framework

[6] ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment

The electronic component for the aim of protecting laboratories

A komplex védelem elektronikai komponense a laborbiztonság érdekében

Tamás Berek
* National University of Public Service / Institute of Military Leadership Training, Faculty of Military Sciences and Officer Training, Budapest, Hungary
berek.tamas@uni-nke.hu

Abstract

The state of our future security can be destroyed, besides many definite factors, by the usage of chemical, biological, radiological and nuclear (CBRN) weapons, devices used for peaceful industrial aims, or the chemical, biological or nuclear components of research that are not 'guarded' properly and can be used for criminal aims. Unofficial access to the radioactive and infectious and poisonous materials and the prevention of their expropriation, their defense is of extreme importance. On the other hand, the special staff of the above-mentioned establishments, in certain occupations, has to face risks posed by chemical, biological, radiological sources. However, these risks can be significantly diminished by a properly worked out defense program. For the reason that the workers at dangerous workplaces and the users of dangerous devices and materials would not be harmed by the everyday working conditions and also that by unlawful appropriation of costly devices or dangerous materials or devices containing dangerous materials and this way, the danger posed by these would not get beyond of the controlled working areas or from the territory of the establishment, so the creation of the physical protection of the mentioned areas and equipment is extremely important. After the accomplishment of the concept of property protection, with the planning of the complex security system, the work on the proper rate establishment of security subsystems needs serious analyzing and evaluation. The author shows that with the inducement of the electronic component of the property protection, what characteristics have to be taken into consideration because of the security risks dangerous materials pose.

***Keywords*:** laboratories, complex security system, integrated physical protection

Összefoglalás

Jövőnk biztonsági környezetének állapotát több más meghatározó tényező mellett a CBRN fegyverek, eszközökön kívül békés célú ipari, vagy kutatási kapacitások nem kellően „őrzött" vegyi, biológiai, vagy nukleáris összetevőinek bűnös szándékú felhasználása is ronthatja. A laboratóriumokban és egyéb létesítményekben található radioaktív, fertőző és méreganyagokhoz való illetéktelen hozzáférésnek és azok eltulajdonításának megakadályozása érdekében azok védelmének biztosítása kiemelt jelentőséggel bír. A fenti intézmények szakállománya bizonyos munkakörökben ugyanakkor ki van téve fizikai-, kémiai-, biológiai- és sugárveszélynek, mely kockázatok jelentősen csökkenthetők megfelelően kidolgozott védelmi program kialakításával. Annak érdekében, hogy a veszélyes munkaterületet, eszközöket, anyagokat használók számára ne jelentsen közvetlen veszélyt a mindennapi munkavégzés, illetve a nagy értékű eszközök és veszélyes anyagok vagy veszélyes anyagokat tartalmazó eszközök eltulajdonításával az általuk hordozott veszély ne kerüljön ki az ellenőrzött munkaterületekről és az intézmény területéről, az érintett területek és berendezések fizikai védelmének körültekintő kiépítése létfontosságú. A vagyonvédelmi koncepció kialakítását követően a komplex biztonsági rendszer tervezésekor komoly elemző és értékelő munkát követel meg a védelmi alrendszerek helyes arányainak kialakítása. A szerző bemutatja, hogy a vagyonvédelmi komplexum elektronikus komponensének kialakításakor milyen sajátosságokat kell figyelembe venni a veszélyes anyagok biztonsági kockázata okán.A szerzők pár mondatban foglalják össze a cikk célját.

***Kulcsszavak*:** laboratóriumok, komplex biztonsági rendszer, fizikai védelem

1 INTRODUCTION

In February, 2008, a common EU CBRN work team was organized as a result of the common EU CBRN special policy, whose aim is to diminish the endangerment of the EU citizens from an unexpected CBRN attack.

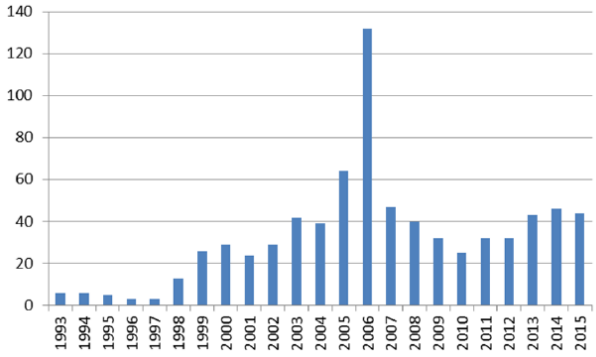
This CBRN work group, taking into consideration the general level of the CBRN endangerment, with the assessment of particular problems, together with other factors, established, with regards to the CBRN prevention that "it is easy to get access to several CBRN materials and turn them into weapons". [1] From the point of view of the risk factors of the CBRN materials that can be mentioned the order mentioned by the work group was ranging primarily from chemical materials, in smaller scale, of biological organisms and radioactive radiation sources.

According to the impact examination, the decision about the development of the EU capacities was made in connection with the fight against CBRN. In prevention, the basic task is to impede any access to legitimately produced or used CBRN materials by any unauthorized persons, including terrorists or other criminals. The first element of

this requirement is to establish authorization and continuous control. The other important element is the control and supervision of CBRN materials. In the publication of 2009 of the European Commonwealth Committee that deals with the strengthening of the chemical, biological, radiological and nuclear security and guaranteeing the proper defense of the CBRN materials and the limitation of the possibilities of their access for inappropriate use. [1]

According to the 2016 report of the International Atomic Energy Agency (IAEA)there were 2889 events reported in connection with radioactive materials between 1993 and 2015, of which 454 events were unauthorized possession and connected crimes, 762 events were proven stealth and 1622 incidents were other illegal activities, in 51 cases the incidents could not be characterized. [2]

The reported thefts and losses included, among others, such radioactive sources as 137-Cs, 241-Am, 90-Sr, 60-Co, 192-Ir which show that the sources are usually portable industrial devices and due to their mobility, they can be easily stolen or lost. It means that it is necessary to improve the efficiency of security regulations and procedures in the future. Thieves are not interested in the possible usage of the radiation source but in the black-market value or the metal mass of the device.



1. figure: Incidents reported to the ITDB involving theft or loss, 1993–2015. [2]
Source: IEAE Incident and Trafficking Database (ITDB)Figure title

There is another worry appearing among specialists in connection with CBRN threats. The significant development of the molecular biology and genetics and the consequent appearance of new laboratories with elevated security levels can be noticed. On the one hand, it makes possible for researchers to research in their own countries such dangerous disease spreaders as SARS crown viruses hemorrhagic fever, the access to which was limited and difficult and on the other hand it carries a risk in other countries where, due to financial problems, it is difficult to take care of the physical protection of dangerous establishments in the long run. Those that show lack of keeping regulations in biological security and biological protection are of potential risk sources. There can be serious abuse by those who are authorized or have access against those who, with the development of certain elements of biological security and defense, the protection elements against of personal abuse should also be developed. Accidents in laboratories or the escape of a dangerous biological materials is not necessarily the result of illegal activities or a sabotage, improper activities in the labs or wrong packaging of dangerous materials and their transportation can also cause the escape of these materials. [3]

2 THE PLANNING CONSIDERATIONS OF THE ESTABLISHMENT OF THE SECURITY SYSTEM

The especially important element of the above-mentioned precautionary measures aimed at the lessening of the security threats is the physical protection of the dangerous materials that can be used for criminal purposes, too. For the formation of the protection of the lab that accordingly to its function needs to operate with different dangerous materials (radioactive, chemical, biological) or needs to detect these materials, certain characteristics need to be taken into consideration.

During the induction and detailing of the endangerment originating from the lab activities and its surroundings, it is important to establish the aim of the protection, the sources of the danger and accordingly, to plan and build the system of protection so that each protectable value and activity is indicated.

For the protection to be continuous and comprehensive, with the buildup of the security system, the separate, independent from each other, autonomous subsystem effectiveness and harmonization as well as the provision of the condition of controlling is necessary. The effectiveness of the physical guarding is provided by mechanical and electric devices together with vitally strong combination of procedures, not to forget about the role of the preventive measures.

A basic document that establishes the order of security provision, it needs to be studied carefully during the defense planning. There is a need for building up a security system where an algorithm that provides supervising conditions for the autonomous operability of the integrated subsystems harmonizes their communication, and at the same time, it provides the possibility for intervention for the supervising personnel within the authority area of the staff of the establishment.

In the interest of the protection system build up, as part of the defense philosophy, risk assessment is necessary. It needs to tackle the question of escaping of the dangerous poisonous radioactive materials into the outer surroundings, as a result of carelessness, criminal aims or even a technical mistake. [4]

The aim of the risk assessment in the given establishment, its operation is the detection, grouping and evaluation of the possible risks in the connection with the activities. During the evaluation the possibility of the risk appearance, their effect as well as avoidance, measures taken to lessen the impact are examined. During the evaluation, the following factors are needed to be considered:

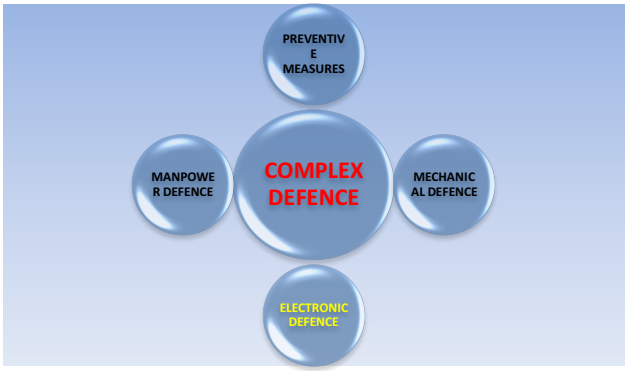
- The surrounding characteristics of the establishment, the criminal statistics of the area
- The architectural, energetic, electronic, IT subsystems
- The operational systems of the establishment, regulations, rules of the authorities
- Basic functions of the establishment, temporary, supplementary functions
- Composition of the personnel and visitors [5]

The size and placement of the lab in its surrounding is of utmost importance and it also needs to be evaluated

previously. During this evaluation, it is necessary to establish the especially important elements of the building that can be an easy target in case of an attack. The examination of the size and placement of the building is important from the point of view of the dangerous areas, places for storing dangerous materials within the building since they are significant for the organization of defense.

It is also important to examine the activities taking place in the establishment. The controlled work areas and work processes brought about within the lab complex, including personnel and the dangerous materials, the protection of the waste collection points is of extreme importance. The same protection applies to areas not considered to be work places and the outer surroundings of the lab.

Materials built into the establishment (technical devices, the use of special building materials, instalment of special technology, etc.), their quality and quantity also defines the establishment of the defense, the security plan of the security service and the acceptance of the future operational regulations. It is not enough to protect the place from the potential criminals, the staff who does the examination of the dangerous materials and the continuous work process also needs to be protected with no less effort. [6]



2. figure: Components of complex property protection
Source: edited by Berek

3 ELABORATION OF THE PROTECTION CONCEPT

The protection concept describes the components, functioning, relationship, methods of operation of the individual elements of the property protection system. It defines the parameters of the necessary mechanical, electronic IT defense subsystems, devices, their interdependency, their functional characteristics, operation, the methods of maintenance. [5]

During planning, it is necessary to indicate those areas where heightened protection is needed due to the presence of sources of danger. Special entrance authorization is necessary. When dangerous areas in labs are protected there is little opportunity to fulfil viral tasks, so it is necessary to increase the rate of the electrical protection equipment and at the same time the strengthening of the inner control is also in the forefront. It is the task of the Lab staff to control the regulations and procedures, to operate and maintain the security systems. It is well-known that the efficiency of the property defense system is determined by the efficiency of the weakest element. In improperly built systems quite often the living component is the weakest link. For the security maintenance of the building, besides the establishing of the responsibility areas, the provision of controllability and as one of its conditions, the formation of the regulation system is very important to prevent breaking the rules or in case of inner sabotage, for the establishment of responsibility and the assurance of its connection to the proper person.

For the lab complex it is necessary to create a building control system when during its operation the need for human intervention comes up in case of mistake correction or in unforeseen exceptional security danger.

According to the above-mentioned the following electronic systems are necessary in the involved establishments:

- Intrusion and attack detention system
- Video surveillance and taping system
- Entrance allowing system
- Electronic fire warning system
- Systems monitoring the presence of dangerous materials

The first three of the above-mentioned elements are mainly components of direct property defense but they also provide protection for activities and people who work in dangerous zones.

3.1 Intrusion detection system

The main aim of the intrusion detection system is the information for the staff about an unauthorized intrusion or its attempt. The properly planned and settled system, with its sensors built directly on the devices of the mechanic protection, informs the staff at the very beginning of the damage of the mechanic protection on the spot by sound and light signs or with distance signs, through the telephone center directly or indirectly. [5]

The planning guidelines pertaining to intrusion systems are introduced in the MSZ EN 50131-1 specification dealing with the “Detection systems, intrusion and attack detection systems. System requirements” The specification ranks the intrusion and attack systems and parts of their elements into the desired level of security. The levels of security are based on the levels of risk which are based on the type of the given establishment, the values found inside and the level of the typically expectable threat. According to the above-mentioned the specification ranks the electronic property protection devices into four security categories. From the low risk 1st stage which deals with the intruder with limited knowledge and having easily accessible manual instruments, to the 4th level security where the intruder is supposedly has high level of special knowledge and special instruments.

For the property protection of labs working with dangerous materials, the intrusion system must be security level 3 or 4.

Level 3. Medium or high-level risk. The intruder or the robber is supposedly well-skilled with intrusion and attack systems. He possesses a large number of instruments, portable electronic devices.

Level 4. High risk. It must be applied when security is the number one priority. The intruder or robber is supposed to be able to plan in detail an intrusion or a robbery. He must have resources and the whole scale of devices including devices capable to substitute the basically important parts of elements of the intrusion and attack system. [7]

The sensors and the special nuclear, biological and chemical detectors, signals coming from meteorological

sensors must be processed by a system that is capable to maintain all of them together and can control the warning and indication units together with the necessary building supervision equipment.

The information provided by the property protection systems inside the buildings, with special attention to the video surveillance and intrusion systems (video images, list of events, address distribution, etc.) and their inappropriate handling can significantly raise the chance of possible theft and can diminish the efficiency of the protection system. Accordingly, the event list of certain centers as well as the stored videos can hide sensitive information from the point of the security of the lab complex, that's why their access must be strictly regulated.

3.2 General requirements concerning access systems

During the planning of the access system of an analytical lab it is necessary to examine, among others, the specifics of the zones of the building, persons with authorization for entrance, the danger sources of the controlled areas in connection with the dangerous materials. It is necessary to define functions expected of the entrance system.

The main function of the entrance system is the inside and outside access to the building as well as regulation of the different levels of movement within the object. Nowadays, besides the determination of the access authorization there is an expected need for the limitation and changeability of the authorization both in time and place. The person following function of the access system is also important since the movements and the presence of the person present in the lab is recorded by the system and it can indicate the number of people and their time spent in the controlled areas. The maintenance function of the "guest card" issued for temporary access is also important from the point of view of the lab.

From the point of view of the lab operator there is an expectation from the access system to have the function of building supervision that makes it possible to switch on and off the ventilation of the airing system as well as the system of cooling automatically depending on the amount of people inside. Nowadays modern software makes it possible that with certain defined outputs connected to the programmed input events the center could be able to perform conditional operations. It can switch on cameras, e.g. at the doors of poison storing, in the case of PLC (Programmable Logic Controller) the air technical equipment can be switched on or off at different times or with event control.

The ability to archive and store events is certainly the highlighted function of the system as well as logging. In the case of a lab, besides the above-mentioned, an important requirement is to monitor the dangerous materials in the lab by a subsystem whose detectors are situated in controlled areas and they can be integrated into the electronic component of a complex property protection system.

Taking into consideration the danger sources of an analytical lab, the access system must be able to operate online. This method of operation provides the installation of several functions important for the security of industrial units and workplaces.

The basic elements of the access system, points installed at the entrance to objects, sites and zones are connected to computer centers through the online systems of the local communication network [5]

This center must be able, even with the operation of several entrance points, to make complicated decisions that need the simultaneous assessment of the number of people present in the controlled zone, their authorization of presence, rights for performing tasks in the lab (the classification of particular persons according to the above-mentioned points), the signals from the detectors of the property monitoring web and other equipment that provides the safe maintenance of the establishment (e.g. airing engines).It is crucial if we need the performance of security decision mechanisms that considers the entire state of the security system of the lab. For example, if in the radiological lab the allowed number of persons, according to the safety regulations is maximum 6, then the entrance for the 7^{th} is not allowed. In this case, of course, it is necessary to support the system with additional elements so as to avoid cheating the system.

The program of the center that provides the online operation of the access system and that also directs the controllers according to the defined authorization, needs to provide the following possibilities:

- In case of being empty, certain zones should be entered only by two persons
- In certain cases, the push bolt of the electronic safety lock needs to be loosened
- In case of zone emptying automatic closure
- Listing of persons inside

Areas where dangerous materials are and there is work with those must be protected by an access system that needs the possession and use of a physical device, such as a proximity smart card. The application of only one identification principle often cannot be considered as a risk rate solution. In the case of especially protected zones the biometric identification or a committee type, including at least two persons, needs to be measured.

It seems that certain biometric based access with personal identification directly to a certain lab zone needs a separate examination since certain specifics of the lab work can exclude certain procedures, for example rubber gloves wearing makes finger printing is impossible. Emergency opening, at the same time, is a basic requirement for each system. The system should make it possible to open the entrance points in case of an extreme event for the sake of escape of the staff inside.

The entrance controls have to have an input that having sensed the warning of the fire system or the disaster warning opens the entrance points automatically. For each entrance point it is necessary to plan a door opening device (panic button) in case of emergency situation. Emergency openers are usually push buttons. In case of danger (or in case of sensing it) by pushing the button the controller, having disrupted the electricity circuit of the electric lock, makes the door possible to open. The emergency buttons should be fitted to the entrance points of the zones protected by entrance terminals, to the labs, next to readers [4]

The access system is an efficient device of protection during work time. With its usage, it is possible to register the identity of those wanting to enter and the time of the entrance.

3.3 CCTV and the electronic article surveillance

During worktime, the protection of the intrusion detection center being in partially sharpened status is supplemented by the CCTV with the help of information

gathering and its storing. The CCTV can provide the lab with significant help in case of possible events. When cameras are set several requirements need to be satisfied. On the one hand, cameras are needed to be placed at points where they can provide assessable recordings according to the aim of application in such way that the recording would show an event important only from the security point of view, or in case of identification, a certain person. When the place of the cameras is created, since the main aim is not deterrence, the site needs to be discreet and at the same time efficiency should not be limited. Offices of the lab, including changing rooms, rooms for cleaning do not need to be monitored by cameras. On the one hand it is not necessary, on the other hand, it disturbs the staff but at the routes of movement, at certain workplaces of the lab (e.g. at the chemical suction booth) a recording of a work procedure can be an important document in case of an accident. The similar surveillance of the poison and isotope storage can be of crucial importance at the identification of the culprit of a robbery or smuggling.

It is natural that The CCTV system cannot hurt the basic rights of the staff, cannot provide information about the research and analytical work. When this efficient element of zone observation is created it is important that the recorded image is fixed according to the data protection rules and the expected image quality and the time synchronization is provided. In case of password access, it is important to place the cameras at an angle where the passwords of the staff cannot be observed or recorded.

From the point of view of security technics, it is important that in the observed dangerous work zones, following an undesirable event, the source of danger is identified and the responsibility is established. The choice of cameras proper for the given aim is influenced by several factors. It is necessary to examine the working environment of the cameras and the resolution of the image coverage. Naturally this specifies the choice of the optics.

When examining the resolution, it can be generally said that high resolution cameras are expensive, so they need to be optimized according to the task. Quite often it is necessary to analyze the information of the image recorded in the lab when procedure detection or identity establishment takes place, so high-resolution cameras are very important in such places. Because of sensitiveness the cameras have to be operated in changeable light circumstances inside, some of them work for 24 hours; consequently, the application of highly sensitive cameras is advisable.

From the point of view of the basic requirements concerning work with radioactive materials the regulation of radiology protection states that “The recording of radioactive materials and their compounds has to be established in a way that accordingly that the types of materials, their quantity, placement, designation and their use can be established and controlled.” To reach this aim RF devices are needed that can be controlled from distance, be resistant to outer impacts (chemical, radiological), can be operated with high level of security, able to perform tasks similar to the functions of the EAS systems. If the need for the above-mentioned security is realized, following the necessary tests, having defined isotopes or samples, the system can immediately warn who and when worked with an isotope as long as the staff the pattern storage, the isotope cupboard and the samples/isotopes are provided with identification devices.

A warning issued by sensors, properly placed in the lab and which monitor the presence of dangerous materials, should also appear in the offices of dispatchers but the neutralization of the intrusion detection system and subsystem monitoring the presence of dangerous materials whose detectors are connected to the warning subsystem, the authorization of measures have to stay within the area of the professional and personal supervision of the lab.

4 CONCLUSION

When a project is created and maintained, where there are materials stored temporarily or operationally, their presence, by itself, is a source of danger. During the planning and inducement of protection in the controlled area, the provision of the highest level of the technical, mechanical, electronic and personal security, is one of the main aspects of the creation of the planned security technology subsystems in accordance with the function of the lab.

To know the type of dangerous materials and storage is vital in order to take appropriate safety measures for prevent an accidental incident. [8]

In an emergency event the controlling system is able to perform several measures simultaneously; its basic task is the prevention of emergency situations, so in case if they happen a vital support of the operation of the system is needed. Monitoring the controlled areas it has to signal immediately so that the operator can intervene immediately. A sensitive part of the complex protection is the information about the technological system and the controlled zones, so the control system needs to ensure that only authorized personnel has access to it. The task of people who work in the establishment is the handling and acknowledgement of warnings, which is a serious responsibility. That is why in the system of control the levels and areas of responsibility have to be precisely defined.

The fact and method of misappropriate unauthorized possession of the dangerous materials and isotopes that are wanted to be used with criminal intentions by those who have authorized access to them cannot be detected and indicated by the intrusion detection system. The proxy card and the access code can be stolen or blackmailed. In such cases the CCTV integrated into the access control system can provide the real identity of the person entering the establishment.

When the protection of the establishments testing dangerous materials is induced, thanks to the proper buildup of the concept of the property protection, the complex security technical system must be able to handle the building supervision and the devices monitoring Dangerous materials together with the elements of property protection system to provide the possibility of operative intervention in a way that together with the expected level of protection, the conditions of work are taken care of without the staff feeling to be threatened.

REFERENCES

[1] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a vegyi, biológiai, radiológiai és nukleáris biztonság Európai Unión belüli megerősítéséről – az EU CBRN cselekvési terve {SEC(2009) 790}

[2] IEAE Incident and Trafficking Database (ITDB) a Nemzetközi Atomenergia Ügynökség honlapján http://www-ns.iaea.org/security/itdb.asp (letöltés: 2017. 09.26.)

[3] Berek Tamás - Pellérdi Rezső: ABV (CBRN) kihívásokra adott válaszlépések az EU-ban 2011. Bolyai Szemle XX. évf. 2. szám, ISSN: 1416-1443 http://archiv.uni-nke.hu/downloads/bsz/bszemle2011/2/Berek_Pellerdi.pdf

[4] Berek Tamás: ABV (CBRN) analitikai laboratórium beléptetőrendszere a biztonságos üzemeltetés szolgálatában 2011. Hadmérnök http://www.hadmernok.hu/2011_2_berek.pdf

[5] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009.

[6] Berek Tamás - Bodrácska Gyula: Az élőerős őrzés az objektumvédelem építőipari ágazatában , 2010. Hadmérnök, http://www.hadmernok.hu/2010_4_berek_bodracska.php

[7] Móré Attila : MSZ EN 50131-1:2007/A1:2009. Riasztórendszerek. Behatolás- és támadásjelző rendszerek 1. rész: Rendszerkövetelmények in Detektor Plusz, 2010/ 1-2. sz.

[8] Berek Lajos-Solymosi János: Veszélyes anyagok szállításának biztonsága 2015. Bolyai Szemle XXIV évf. 2. szám, ISSN: 1416-1443 https://folyoiratok.uni-nke.hu/document/uni-nke-hu/bolyai-szemle-2015-02.original.pdf

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Kiberbiztonság az autóiparban

Automotive Cybersecurity

Tokody Dániel*, Albini Attila*, Ady László**, Temesvári Zsolt Marcell*, Rajnai Zoltán*
* Óbudai Egyetem, Biztonságtudományi Doktori Iskola, Budapest, Hungary
** Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, Budapest, Hungary
daniel_tokody@ieee.org attila.albini@gmail.com adylaszlo@gmail.com zsolt.temesvari@gmail.com
rajnai.zoltan@bgk.uni-obuda.hu

***Összefoglalás* — Tanulmányunkban megvizsgáltuk a járművek kiber-fizikai rendszerré válásának és hálózatba kötésének motivációit. A legfőbb motivációk közé tartozik a biztonságos közlekedés és az energiahatékony mobilitás megvalósítása. A járművek hálózatba kapcsolásának több módját is sorba szedve, valamint a járműrendszerek funkcionális- és kiberbiztonságával kapcsolatos észrevételeink alapján egy új biztonság szemléletű tervezési módszert ajánlunk a nemzetközi szabványosításhoz illesztetten az autonóm intelligens járművek és az okos mobilitási rendszer létrehozásához.**

***Kulcsszavak*:** funkcionális biztonság, kiberbiztonság, járműrendszerek, járműfedélzeti rendszerek védelme

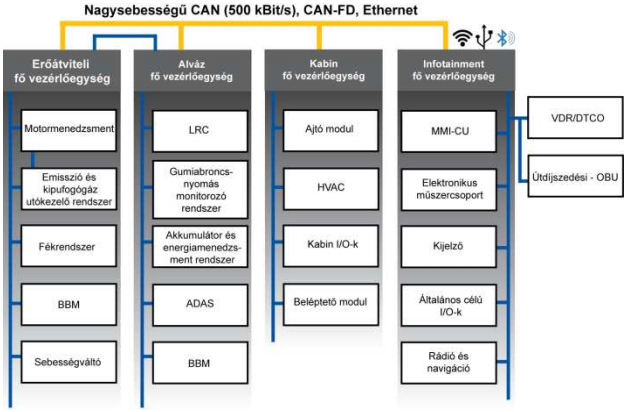
***Abstract* — In our study, we examined the motivation of vehicles becoming cyber-physical systems and their connection. The mentioned main motivations include safe transportation and energy-efficient mobility. We are also suggesting a new safety and security method by our observations about functional and cyber-safety of vehicles to develop new autonomous intelligent vehicles and a smart mobility system based on the international standards.**

***Keywords*:** functional safety, cyber security, vehicle systems, in-vehicle network security

1 BEVEZETÉS - ÚT A HÁLÓZATBA KAPCSOLT JÁRMŰVEK FELÉ

Az elmúlt években világszinten évente kb. 1,25 millió ember halt meg az utakon a közúti járművekkel kapcsolatos balesetek során a WHO statisztikái szerint. [1] A kooperatív intelligens közlekedési rendszerek létrehozásának célja a folyamatos és közvetlen információcsere a közlekedés valamennyi résztvevője között. Az ez irányú járműkommunikáció legfontosabb motivációit a közúti közlekedés biztonságának növelése, a forgalmi dugók és torlódások számának, időtartalmának (idő- és üzemanyag takarékosság magas szintű megvalósítása) és a közlekedés CO_2, illetve károsanyag-kibocsátásának csökkentése jelenti.

Az átlagos gépjárműhasználó ma már azzal szembesül, hogy a korszerű járművek keréken guruló komputerként egy közlekedési célú kiber-fizikai rendszerként definiálhatók. A mai modern gépjárművek kb. 70 darab elektronikus vezérlő egységet (ECU-t azaz Electronic Control Unit) tartalmaznak. [2] Egy felsőkategóriás járműben ez a szám már elérheti a 150-et is. Az autonóm intelligens járművek esetében pedig jelentősen több és még összetettebb intelligens vezérlőegységek és érzékelők sora határozza meg az adott jármű autonóm működését. A legismertebb ECU-k között említhető a motorvezérlő modul vagy éppen a fékvezérlőegység. [3] Az első ábrán egy általános haszongépjármű elektromos/elektronikus elosztott szabályozási rendszerének architektúrája látható az említett és néhány további főbb vezérlőegységek feltüntetésével. Ez szemlélteti a járművek belsőhálózatát, azaz a járműrendszerek hálózatba kapcsolását.



1. ábra: Haszongépjárművek elektromos/elektronikus elosztott szabályozási rendszerének architektúrája (saját szerkesztés) [3][4]

Az autó- és járműgépészet ma már inkább olyan interdiszciplináris járműmérnöki tudományt jelent, amely kapcsán a gépészeti, villamosmérnöki, informatikai, adattudományi és anyagtudományi stb. területek együttes felhasználására is szükség van.

A járművek és a közlekedés biztonságának növelése érdekében az európai szintű kooperatív közlekedési rendszer létrehozása és az ezzel kapcsolatos kommunikációs hálózatba való kapcsolás megvalósítása folyamatban van. A hálózatosodás új kihívások elé állítja a teljes iparágat. Így a járművek kiberbiztonságának növelése az elmúlt pár évben egyre nagyobb hangsúlyt kap.

1.1 Az intelligens autonóm járművekkel kapcsolatos legfontosabb fogalmak

Az **intelligens közlekedési rendszerek** általános definíciója szerint a biztonság elérése érdekében és a mobilitás környezeti hatásainak csökkentésére az infokommunikációs rendszerek alkalmazásával törekszünk az intelligens közlekedési rendszerben. [5][6]

Néhány fontos fogalom az intelligens közlekedési rendszerekben:

Automatizált jármű, olyan jármű melynek járműrendszerei lehetővé teszik a vezető számára, hogy bizonyos vezetési funkciókat a járműre bízzon. [7]

Autonóm jármű (teljesen automatizált jármű), olyan jármű, amely járműrendszerei lehetővé teszik az autonóm közúti jármű számára, hogy biztonságosan közlekedhessen az adott közlekedési rendszerben megfelelő keretek között. [7]

Az **intelligens autonóm közúti jármű,** azaz interaktív kooperációra képes közúti jármű, amely emberi beavatkozás nélkül önmaga irányításával és navigációjával a közlekedési helyzet figyelembevételével képes működni.

Az **intelligens autonóm közúti járműrendszerek** azon technológiai rendszerek, fődarabok összessége, amelyek segítségével az autonóm intelligens jármű, autonóm működésre képes, pl.: intelligens szenzorok és beavatkozók.

Összekapcsolt vagy hálózatba kötött jármű, olyan közúti jármű, amely rendelkezik olyan járműrendszerrel, ami biztosítja a vezeték nélküli kommunikációt a közlekedési rendszer egyéb külső elemei, más járművek, hálózatok és szolgáltatások között a minél magasabb szintű vezetés automatizáltsághoz. [7] [5] [6] A járművek automatizálásával, kommunikációs összekapcsolásával, hálózatba kötésével csökkenthető az emberi járművezető közlekedésben betöltött szerepe.

Az autóipari kiberbiztonság az autóipari kibertérben az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását jelenti, a járművek, a járműveket használók, a járművel kapcsolatos szoftverek és szolgáltatások, eszközök, illetve hálózatok komplex környezetében. [8]

1.2 A közúti járművek biztonsági rendszereinek fejlődése

Az 1950-es évektől a 2000-es évekig a közúti járművek tekintetében a biztonságos közlekedés és a kényelmes fáradságmentes vezetési élményt pl.: a biztonságiöv, a blokkolásgátló rendszerek vagy éppen a tempomat (sebességtartó rendszer) jelentette. 2000 – 2010 között az elektronikus stabilitás szabályozás (menetstabilizáló), a holttér figyelő rendszer, a ráfutásos ütközést megelőző figyelmeztető rendszer, illetve például a forgalmi sáv tartásának gépi úton történő megvalósítása volt a biztonság növelésének eszköze. 2010 – 2016 között a intelligens tolatókamera, az automatikus vészfékezés, a gyalogos-felismeréssel egybeépített automatikus járműmegállító rendszer, az automatikus tolatást segítő rendszer, a sávelhagyásra figyelmeztető rendszer vált általánossá a magasabb kategóriás járművekben. 2016 – 2025 közötti években a már közkeletűvé vált iparági vízió szerint az adaptív sebességtartó rendszer, a forgalmi torlódásban segédkező rendszer vagy éppen az automata parkolási rendszer fogja segíteni a járművezetők tevékenységét. 2025-at követően pedig várható a teljesen automata biztonsági rendszerek elterjedése, valamint az autópályák esetében már valószínűleg alkalmazható lesz a járművekbe épített autópilóta is. [9]

1.3 Európai törekvések, a biztonság növelésének új eszköze az összekapcsoltság megvalósítása

Első lépésként a kommunikáció útján való összekapcsoltság irányába 2015. április 29-én „az Európai Parlament és a Tanács 2015/758 rendeletével a 112-es egységes európai segélyhívó szolgáltatáson alapuló fedélzeti e-segélyhívó rendszer kiépítésével összefüggő típus-jóváhagyási követelményekről és a 2007/46/EK irányelv módosításáról” szóló rendeletében megalapozta és általánossá tette a gépjárművek közös rendszerbe való kötését. [10] Amely folyományaképpen az Európai Unióban 2018. március 31-től minden újonnan forgalomba helyezett közúti járműbe kötelező beszerelni az eCall segélyhívó rendszert, amelyet a nemzeti hatóságoknak ellenőrizni kell. [10]

„Az eCall-funkcióhoz szükséges hardvert az autóban a beépített telematikai egység jelenti, ami elsősorban egy modemből – a közös hálózati kapcsolódást biztosító készülékből – egy műholdas helymeghatározó antennából (pl.: Galileo műholdas navigációs és helyzetmeghatározó rendszer), és a járművel való kapcsolódást biztosító elektronikából áll.” A rendszerhez illesztetten van lehetőség tartalék a jármű elsődleges villamos rendszerétől független tápellátás biztosítani a segélyhívást megvalósító eszköz számára. [11] Mindez annyit jelent, hogy a jövőben az új gépjárművek már legalább egy hálózatához alapvetően csatlakozni fognak.

A közlekedési telematikai rendszerek fejlődésével például a járművek távoli diagnosztikai lehetőségei is bővültek. Ezt a kapcsolatot általában a járművek vezeték nélküli helyi hálózathoz csatlakoztatásával egy mobil eszközön keresztül az internet elérése érdekében alakítják ki. Amely lehetőséget ad például egy online járműszervizzel való kapcsolatfelvételre vagyis az interneten keresztül egy újabb hálózathoz csatlakozik már az adott jármű.

A harmadik típusú példa a járművek hálózatba kapcsolásának olyan folyamata, amelynek már az ember nem szükségképpen szereplője. Vagyis a járművek kommunikációs lehetőségeinek bővülésével létrejöhetett egy új féle minden eddiginél hatékonyabb formája a hálózatba kapcsolt járműveknek. A kommunikáció kialakítására már többféle biztonságkritikus formát is létrehoztak. A többszereplős rövid hatótávú vezeték nélküli megoldások között a célorientált rövid távolságú kommunikáció megvalósítása a cél (pl.: Dedicated Short Range Communications - DSRC). [12]

Az említett technológiai fejlesztése kihatással vannak az utasbiztonságra, üzembiztonságra vagy akár a közlekedésbiztonságra.

1.4 A hálózatba kapcsolás modern vezetéknélküli kommunikáció alapú módszerei

Az információtovábbítás egyik módja az intelligens közlekedési rendszerekben a célorientált rövid távolságú kommunikáció (DSRC) megvalósítása. [12] Amely a következő kommunikációs lehetőségeket jelenthetik:

V2I – jármű-infrastruktúra közötti együttműködés, kommunikáció, amelynek során a jármű által - közlekedés közben - gyűjtött adatok kerülnek továbbításra a közlekedési infrastruktúra felé, beleértve a közlekedés biztonságára, a közlekedési környezetére vonatkozó információkat, valamint a mobilitás további részleteit. [12] [13] [14]

V2V – jármű-jármű közötti együttműködés, kommunikáció a járművek bizonyos csoportjára vonatkozó sebességek, pozíció információk vezeték nélküli kommunikáció útján történő megosztása azzal a céllal, hogy a balestek és forgalmi torlódások elkerülhetőek legyenek. A cél megvalósítása pozitív hatással van az élőkörnyezetre. [12] [13]

V2C – jármű-felhő közötti együttműködés, kommunikáció olyan információcserét megvalósító technológia, amely során a jármű számára lehetővé válik, hogy más, a felhőhöz kapcsolódó rendszereket, például az energiaellátó rendszert, töltő infrastruktúrát, okos otthonokat, okos parkolókat stb. használjon, információt osszon meg és szerezzen a kapcsolódó rendszerektől működésének tökéletesítéséhez és szolgáltatásainak bővítéséhez. [15] [16] [17]

V2P – jármű-gyalogos közötti együttműködés, kommunikáció lehetővé teszi, hogy a közlekedési környezettel kapcsolatos információkat a járművekkel, infrastruktúrával és a járókelők mobileszközeivel megosztva a jármű képes legyen jelezni a gyalogos számára az adott közlekedési helyzetet, ezáltal növelve a biztonságos közlekedés esélyét. [18]

V2X – jármű- és minden lehetséges dolog közötti együttműködés, kommunikáció lehetővé teszi, hogy összekapcsolja az összes járműtípust és a különféle infrastrukturális rendszereket. Ez a kapcsolat magában foglalja az autókat, az autópályákat, a hajókat, a vonatokat, a repülőgépeket, valamint a gyalogosokat stb. is, ezáltal megvalósítva a teljes körű kooperativitást a közlekedésben. [13][18][19]

A kooperativitáson alapuló hatékonyság és közlekedés biztonsága a célorientált rövid távolságú kommunikáción (DSRC) és a fejlett vezetőtámogató rendszerek és szolgáltatások (Advanced Driver-Assistance Systems - ADAS) együttműködésén keresztül valósítható meg.

A közös rendszerhez, hálózathoz kapcsolódik a rendszerben lévő számos jármű érzékelőhálózata, az infrastruktúra kommunikációra képes elemi (pl.: vezetéknélküli érzékelő hálózatok [20]) és a közlekedési rendszer összes résztvevőjének alhálózatai. A közös hálózatban rejlő információk alapján azonnali automatikus reakciókat (megfigyelés, riasztás, fékezés és kormányzás stb.) válthatnak ki a közlekedés folyamán előálló megfelelő információ konstellációk. Ezeknek a funkcióknak a hatékony megvalósítása csak is márkafüggetlen módon és a nemzeti határokon átívelő [21] infrastrukturális megoldásokkal való létrehozása adhat megfelelő funkcionális biztonsági szintet a közös integrált európai kooperatív közlekedési rendszerben.

2 A BIZTONSÁG ÉRTELMEZÉSE AZ AUTONÓM INTELLIGENS JÁRMŰVEK KIBER-FIZIKAI JÁRMŰRENDSZEREINEK ESETÉBEN

A UNECE 29-es munkacsoportja 2017-ben elfogadta és közreadta az automatizált, összekapcsolt és hálózatba kötött közúti járművek üzemeltetésére vonatkozó szempontokat, követelményeket, elősegítve ezzelaz automatizált vezetési funkciókkal rendelkező közúti járművek biztonságos használatát. A szabályozás az autonóm járművek részletes funkcióira még nem kidolgozott, így például az autonóm járművek kiberbiztonságának terén még szükség van a szabályozást is érintő további fejlesztésekre. [8] [22]

Az automatizált és együttműködő intelligens közlekedési rendszerek fontos elemei a földi járművek. Az autonóm intelligens földi járművek biztonság szempontú vizsgálata, tervezése során elsődlegesen a SAE International szerinti biztonság összetevőket vesszük figyelembe.

A SAE szerint a biztonság összetevőit: a funkcionális biztonság, az aktív biztonság (pl.: ADAS), az elektronikus és elektromos rendszerek hardver és szoftver megbízhatósága, valamint az emberi tényező rendszer biztonságra gyakorolt hatásai alkotják. Más besorolás szerint a biztonság háromféle területre bontható: funkcionális biztonság („functional safety”), műszaki biztonság („technical safety”), függő biztonság („contextual safety”) (EN 50126-2:2017). [23]

Az említett felsorolásban csak mögöttes értelmet keresve találjuk a járművek és járműrendszerek informatikai, kiber részének biztonságát. A "kiber" és a "biztonság" szavaknak autóipari területen korábban meglehetősen más értelme volt, mint például az informatikában. A "biztonság" fogalmát szinte kizárólagosan a jármű fizikai, funkcionális biztonságával összefüggésben használták.

A gépjárműveken belüli, a járművek elektromos/elektronikus alrendszerei közötti kommunikációs rendszerek fejlődésével és a belső villamos kábelezések bonyolultságának csökkentésének igényével, a belső hálózat rugalmasságának, valamint megbízhatóságának növelésével a fedélzeti buszok alkalmazása terjedt el járműipari alkalmazásokban az 1990-es évektől. Létrehozva ezzel a kommunikációs hálózatra és beágyazott irányítástechnikai rendszerekre alapozott úgynevezett Drive-by-Wire struktúrákat. [24] [25]

A járművekbe épített funkcionalitások bővülése (pl.: fedélzeti tájékoztató és szórakoztató elektronika – Infotainment stb.) a buszrendszerek számának növekedését és jellegének bővülését jelentette. A biztonsági funkciókat megvalósító buszokat elválasztották a kényelmi funkciókat biztosító hálózattoktól. A járművek funkcionális biztonsága a járművekben található hardver és szoftver elemektől vált függővé. [25]

A gyakorlati tapasztalatok szerint a forgalomba került gépjárművek jelentős része kiber támadhatóság szempontjából kitett a kiberbiztonsági szempontokat csak részlegesen figyelembe vevő tervezési folyamatból adódóan is. Tipikusan az adott kényelmi funkciót megvalósító jármű fedélzeti rendszerek (pl.: navigációs rendszer, Bluetooth kapcsolat, In-car Internet stb.) a megvalósítás során nem kielégítő védelemmel vagy akár védelem nélkül kerülnek létrehozásra. Ezeket a hibákat kihasználva és a járművek nem megfelelően védett kommunikációs hálózatokhoz való csatlakoztatásával [26] elérhetővé válhatnak olyan biztonsági funkciók, amelyek működése megzavarható, az irányítása átvehető, akár közvetlen fizikai kapcsolat nélkül. Ezért az okos mobilitási rendszer fő elemét az autonóm intelligens járművet már kiberbiztonság szempontjából is tervezni kell. Az intelligens autonóm járművek kiberbiztonság szempontú tervezése új és szabványosítás alatt álló terület. [25] [27] [28] [29] [22]

2.1 Az autonóm intelligens járművek kiber-fizikai járműrendszereinek funkcionális biztonsága

A funkcionális biztonság azt jelenti az autonóm intelligens járműrendszerek kapcsán, hogy az adott járművet olyan állapotban kell tartani, hogy az emberi élet védelme a legnagyobb mértékben biztosított legyen. Más szavakkal „a funkcionális biztonság azt a törekvést jelenti, amely során a jármű alapvető funkcióinak hibáit megakadályozzuk az utasok biztonsága érdekében. Többek között ilyen alapvető funkciók, amelyek közvetlen kapcsolatban állnak a biztonsággal a kormányzási vagy éppen a fékezési funkciók. A légzsákok, a gyűrődési zóna, az ESP vagy az ABS is a jármű funkcionális biztonságát befolyásoló tényezők.”[30]

Az autonóm intelligens járművek közlekedés biztonsággal összefüggő kiber-fizikai rendszereire a 2. ábrán láthatunk példát a jármű környezetére vonatkozó rendszerekkel egyetemben. Ez a példa jól mutatja, hogy a járművek biztonságos közlekedését aktívan vagy akár passzívan befolyásoló informáló, figyelmeztető, felügyelő, biztonsági, beavatkozó, hatásokat csökkentő vagy mentést könnyítő rendszerek mind-mind kihatással vannak az informatikai- és kiberbiztonságra.

„A biztonsági integritás (safety integrity – a biztonság sértetlensége) annak valószínűsége, hogy egy biztonsági rendszer az előírt biztonsági funkciókat egy adott időszakban meghatározott körülmények között megfelelően végrehajtja, azaz nem lépett fel veszélyeztető meghibásodás. Egy rendszerhez rendelt biztonsági integritási szint (SIL) meghatározza az alkalmazandó fejlesztési, tervezési, gyártási, üzemeltetési módszereket.” [31] Mindazonáltal a funkcionális biztonsághoz köthetően a járművek elektromos és elektronikus rendszereinek biztonságát is jellemezhetjük a biztonság integritással. A jármű ipari biztonságkritikus rendszerek esetében az ASIL (Automotive Safety Integrity Level) értékek használatosak a járművek életciklusa során.

2.2 Az autonóm intelligens járművek kiber-fizikai járműrendszereinek informatikai biztonsága

A informatikai biztonság azt jeleni, hogy ügyelünk rá, hogy más ne kaparinthassa meg a tulajdonunk. Erre jó példa a bankautomatákban tárolt pénz védelme, vagy az informatikában a jelszavak/adatok biztonsága is. Így a autonóm intelligens földi járművek informatikai biztonság szempontú vizsgálata, tervezése során elsődlegesen a kiberbiztonság megvalósítása a cél. Az intelligens közlekedési rendszerek jármű, járműrendszerek és intelligens infrastruktúra konstellációjában az informatikai biztonság értelmezése kapcsán több összetevőt azonosítottunk kutatásunk során.

„A informatikai biztonság a járművek szoftvereinek és az ezzel kapcsolatos rendszereinek biztonságát jelenti. Az esetleges szoftveres véletlenszerű vagy szisztematikus hibák és a külső kibertámadások elleni védelmet. A járműipari szoftverek különböző szerepet töltenek be a járművek működésének és funkcionális biztonságának biztosításában.” [30] A közlekedési rendszerben például a ‘0231512’ számsor lehet egy adat. Viszont, ha ez az adat az egyik jármű kommunikációs azonosítója a közlekedő járművek ad hoc hálózatában, akkor ez már egy információ az adott rendszerben.

Muha szerint az informatikai biztonság rendszertana alapján a védendő elemek között találhatóak a rendszert használó személyek, az informatikai rendszer fizikai környezete, a működéséhez szükséges infrastruktúra, a hardver, a szoftver, a kommunikációs eszközök és hálózat, az adat hordozók, valamint a rendszerrel kapcsolatos szabályozás. [32] Ez nem csak általánosan, de az autóiparban is igaz, vagyis az informatikai biztonság azt jelenti, hogy az információ bizalmasságára, sértetlenségére és rendelkezésre állására fokuszálunk. Mindemellett az autóipari kiberbiztonság alatt az iparági infokommunikációs rendszerek védelmét is értjük. Az autóipari kiberbiztonság magába foglal mindent és mindenkit, akik a kibertéren keresztül a járműipari alkalmazásokhoz hozzáférhetnek.

3 KIBERFENYEGETÉS, KIBERVÉDELEM, KIBERBIZTONSÁG KÉRDÉSE AZ AUTÓIPARBAN

A járművek fizikai védelmére, például a ballisztikai szempontból való külső támadhatóságára már hosszú ideje megfelelő figyelmet fordítanak a fejlesztők, a katonai alkalmazások jól példázzák ezt. [33] [34] A kiberfenyegetések, mint például a vírusfertőzések, célzott adatvesztés előidézése, hardver hiba előidézése szándékos törlésből adódó adatvesztés elleni felkészülés elengedhetetlen a járműipari alkalmazásokban is. A fenyegetésekből adódóan keletkezhetnek fizikai károk, kritikus szolgálatás kimaradás, kompromitálódás, funkció vesztés stb. [35]

Ugyanakkor az előzőekben leírt jármű architektúra és az intelligens közlekedési rendszerek működése is felveti a járművek kibervédelmének kérdését.

A közlekedési rendszer növekvő automatizáltságával egyenes arányban növekszik a kibervédelemre szoruló közlekedési rendszerben kulcs szerepet játszó eszköz pl: járművek, intelligens infrastruktúra, út menti egységek stb.

„A kiberbiztonság a kibertérben lévő szolgáltatás vagy adat meghatározott kiberfenyegetések ellen, előre meghatározott védelmi szintű állapotát jelenti.” [35]

Mit jelent a kiberbiztonság a járművek és járműrendszerek esetében? A 2.1 pontban általánosságban megfogalmazottakon túl az intelligens autonóm járművek belső struktúrájában, külső környezetében létrehozott, illetve alkalmazott információs és kommunikációs hálózatok, rendszerek és ebben a hálózatban, rendszerben létrejövő, áramló információ megfelelő védettségének, bizalmasságának, hitelességének stb. a biztosítása, azaz a károsodástól, illetéktelen hozzáféréstől és módosítástól stb. való védelmének megvalósítása.

3.1 *Kibervédelmi módszerek járművek esetében*

A modern járművek egyre több támadható felületének (pl.: kihasználható szoftverhibák) illetve a járműhasználók magánszférájának megsértésének komoly biztonsági kockázata van. A járművek ellen irányuló kibertámadások (pl.: malware támadások, fedélzeti diagnosztikai rendszer biztonsági rései stb.) egyre növekvő és aggasztó számban jelentek meg az utóbbi időben. [36] [37]

A járművek, járműrendszerek kibervédelmének lépéseit a következő pontokban fogalmazzuk meg:

A járműrendszerek (járművek belső rendszerei közötti) és járművek közötti kommunikáció biztonságának és az autóipari és közlekedési informatikai és információs rendszereinek fizikai infrastruktúrájának védelmének megvalósítása. [38]

A járműrendszerek és járművek működésbiztonságának megvalósítása a közlekedési folyamatok szándékos megzavarása, megváltoztatása elleni védelem létrehozása során. [38]

Az intelligens közlekedési rendszerek, a járművek és járműrendszerek informatikai és információs biztonságágának megvalósítása a rendszerben gyűjtött, tárolt és továbbított adatok lopásával, törlésével vagy megváltoztatásával szembeni védelme. [38]

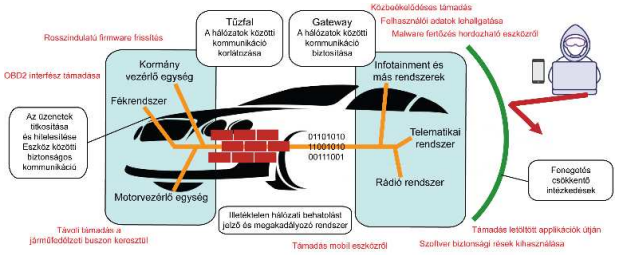
A járművek fizikai biztonsága az informatikai és információs rendszer védelme során a fizikai veszélyektől (pl.: járművezérlő egységekhez való illetéktelen hozzáférés, fertőzött, átalakított bűnös célú hardver beépítése a járműbe stb.) [38]

A közlekedési rendszer, mint kritikus infrastruktúra védelme a kibertérből érkező, akár fizikai rendszereket és az autóipari és közlekedési kritikus információs infrastruktúrákat és a ráépülő szolgáltatásokat érintő támadások elleni védelmet kell megvalósítani. [38]

Az NHTSA (National Highway Traffic Safety Administration, USA) szerint a járművek kiber támadás ellenei védelmét többszintű védelmi megközelítés alapján mind a vezetékes mind pedig a vezeték nélküli belépési pontok esetében biztosítani kell.[9]

Az autonóm intelligens járművek esetében az autonómiát biztosító többféle intelligens járműrendszer pl.: adatbiztonsági szoftver, HMI, beágyazott modem, V2X, beavatkozók, beágyazott vezérlők, ultrahangos érzékelők, odometriai érzékelők, LIDAR, radar, kamerák működésének kiberbiztonsággal kapcsolatos kérdései még nem váltak általánosan kezelt iparági kérdéssé. Számos tanulmány foglalkozik az autonóm járművek szenzorjainak a megzavarásával. [39]

Az elektromos, elektronikus és programozható elektronikus biztonsági rendszerek járműipari kiber biztonsági integritási szintjét az ACSIL (Automotive Cybersecurity Integrity Level) értékekkel határozhatjuk meg.



2. ábra: Járműfedélzeti hálózatok kiberbiztonsági kérdései hagyományos felsőkategóriás járművek esetében [40]

3.2 Biztonság szemléletű autonóm intelligens járműtervezés

Magyarország élenjár az autonóm járművek tervezésében, kivitelezésében és tesztjében. Ugyanakkor még csak nem rég nyílt jogi lehetőség a fejlesztett járművek közúti tesztjére.

A közúti járművek műszaki megvizsgálásáról rendelet így fogalmaz: a 2. § (3b) bekezdés b) pontjában a „fejlesztési célú autonóm jármű: olyan fejlesztési célú jármű, amely részben vagy teljesen automatizált működések fejlesztésére szolgál, és amelyben a jármű vezetőjének minősülő tesztvezető tartózkodik, aki az automatizáltság szintjétől függően vagy bármely, a közlekedés biztonságát veszélyeztető helyzetben, a működés közben szükséges mértékben kézi irányítást gyakorol, illetve a kézi irányítást bármikor átveheti a jármű felett”. [41]

„A fejlesztési célú autonóm járművek közúton történő tesztelését végző járműfejlesztő akkor vehető nyilvántartásba, ha valamely tevékenységét az ISO 26262 szabvány szerint végzi, illetve valamely tevékenységre vonatkozó, folyamatban levő ISO 26262 szabvány szerinti tanúsítási folyamat részese, vagy az ISO 26262 szabvány tanúsítására feljogosított valamely tanúsító szervezet szakvéleménye alátámasztja az autonómjármű-technológia funkcionális biztonságára vonatkozó, a járműfejlesztőnél alkalmazott fejlesztési gyakorlat megfelelőségét. Amennyiben a fenti feltételek nem állnak fenn, a közlekedésért felelős miniszter a 2. § (3b) bekezdés b) pontjában meghatározott járművek tekintetében a nyilvántartásba vételt megtagadja, illetve az azokra vonatkozó adatokat törli a nyilvántartásból.” [41]

Kiberbiztonságra vonatkozóan a közúti járművek forgalomba helyezésének és forgalomban tartásának műszaki feltételeiről szóló rendelet a következőket írja elő:

„9.1. A járműfejlesztőnek biztosítania kell, hogy valamennyi fejlesztési célú autonóm jármű prototípus automatizált vezérlése és egyéb járműrendszere megfelelő beépített biztonsági szinttel rendelkezzen a jogosulatlan hozzáférésből adódó kockázat kezelése érdekében.

9.2. A járműfejlesztő az elvárható legjobb minőségben alkalmazza a biztonságkritikus járműipari rendszerek fejlesztésére vonatkozó szabványokat és technológiákat.” [42]

A járművek hálózatba kapcsolása olyan fenyegetéseket jelent, mint a termékbiztonság, az adatintegritás és adatbiztonság vagy akár az interoperabilitás. Az ISO 26262 szabvány szerint a közúti járművek elektronikus rendszerének funkcionális biztonságára vonatkozóan fellelhetőek szabályok és tervezési irányelvek. A szabvány második kiadása már megköveteli az interfészekre vonatkozó kiberbiztonsági eljárások alkalmazását. Viszont átfogó formalizált járműipari specifikus kiberbiztonsági szabványokkal még nem rendelkezik ez a szakterület.

A ISO esetében a vonatkozó kiberbiztonsági szabvány javaslati szakaszban van SAE szabvány pedig kidolgozás alatt áll, de a kapcsolódó javasolt jó gyakorlat (SAE J3061™ - Cybersecurity Guidebook for Cyber-physical Vehicle Systems) első kiadása 2016 januárjában megtörtént. Természetesen további szabványok is befolyásolják az autóipari fejlesztéseket a kiberbiztonsági tervezési folyamat szempontjából, ilyen általános IT biztonsági szabványok (ISO 27001, ISO 15408) vagy a speciális biztonsági szabvány V2X kommunikációhoz (IEEE 1609.2, ETSI TR 102 638 V1.1.1).

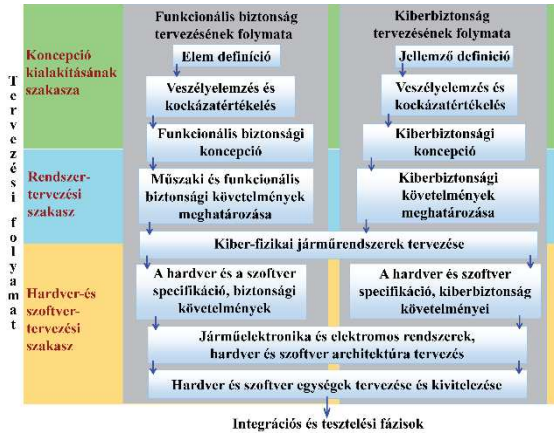
A tématerület kiforratlansága miatt szükség van az autóipari kiberbiztonsági tervezési eljárás kifejlesztésére a kapcsolódó szabványok és jó gyakorlatok alapján (SEA - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061). A kiberbiztonsági tervezési folyamatnak illeszkednie kell a funkcionális biztonság és minőségi folyamatok meglévő rendszeréhez és a megfelelő szakértelemmel rendelkezők számára végrehajthatónak kell lennie a biztonsági tevékenységnek.

A fejlesztési folyamat során nem csak a funkcionális biztonság létrehozását, hanem a kiberbiztonság megvalósítását is szem előtt kell tartani. Az IEC 62443

definiál négy biztonsági szintet, amely minőségi mutatókat, készségeket és erőfeszítés szinteket határoz meg a sikeres rendszertámadáshoz. A járművek kibertámadhatóságához szükséges erőforrások számbavételét kockázatelemzés útján el kell végezni és eredményeit implementálni kell a fejlesztési folyamatba.

A kockázatelemzés és kockázatértékelés segítségével olyan fejlesztési biztonsági koncepciót és követelmény előírást kell létrehozni, amely már rendszerterv szintjén foglalkozik a mélységi védelem kialakításával és a védelmi megoldásokat egymásra épülő rétegekként határozza meg. [43]

A 3. ábrán láthatjuk a járművek funkcionális és kiberbiztonság szempontú tervezési folyamatát. A kiberbiztonságnak a fejlesztési folyamatban nem csak egy hozzáadott elemnek kell lennie, hanem a tervezési folyamat szerves részét kell, hogy képezze egészen a koncepció fázisától, a gyártás, üzemeltetés, szervizelés és rendszer leszereléséig. Ez jelenti azt, hogy a kiberbiztonságot a járművek teljes életciklus alatt folyamatosan fent kell tartani. [22]



3. ábra: Járművek funkcionális és kiberbiztonság szempontú tervezési folyamata [43] [44] (saját szerkesztés)

4 Összegzés

Cikkünkben az elektromos, elektronikus és programozható biztonságkritikus rendszerek funkcionális biztonsági és kiberbiztonsági szempontú tervezésének elveit mutattuk be az okos mobilitási rendszer létrehozásának útján. A kiberbiztonság kapcsán fontos szempont, hogy az adott biztonsági szint csak időben korlátozott ideig tartható fent, hiszen a kibertámadások eszközrendszere folyamatosan változik. Viszont egy megvásárolt jármű esetében ma nagyon kevés esetben tudjuk elképzelni azt, hogy este a garázsban biztonsági javításokat telepítsen az autonóm intelligens járművünk. Cohen szerint az okos város egyik fő építőeleme az okos mobilitás, cikkünkben ennek az újszerű mobilitási rendszernek a tervezését tárgyaltuk. Kutatásunk szerint az okos mobilitás két pillére az autonóm intelligens járművek, járműrendszerek illetve az intelligens közlekedési infrastruktúra. Az okos mobilitás kialakításának szükségessége az kooperatív intelligens közlekedési rendszerek létrehozásának motivációban gyökerezik. Ezek a tényezők a produktivitás növelése (pl.: szállítási kapacitás növelése), a kevesebb baleset és a károsanyag-kibocsátás csökkentése akár a városi közlekedésben is. Az okos városi közlekedés kialakítása lényegében egy továbbfejlesztett ITS rendszerként kell elképzelni. Az okos város mobilitás marketingének a lényege, hogy olyan plusz szolgáltatásokat nyújtson, mint amit a hagyományos rendszerek nem. Cikkünkben számos okos mobilitási szolgáltatást predesztináltunk. Az autonóm intelligens járművek terjedése időszerű (robotok, drónok, önvezető autók) az össztársadalmi előnyösségük végett. A mai korszerű robotrendszerek, ilyenek az önvezető autók is már képesek egymás követése útján a konvojban haladásra vagy akár egy kitűzött cél önálló elérésére. A járművek közötti kommunikáción kívül a V2X (Vehicle-to-everything) kommunikáció segíti a okos város létrehozását. A járművek funkcionális, működési biztonsága már régóta kutatott terület viszont mára már a fizikai infrastruktúra a járművek fizikai rendszerei mellett egyre hangsúlyosabb szerep jut a kiber-fizikai komplex rendszereknek. Az autóipari fejlesztések kiberbiztonság szempontú megközelítése új és fejlődő terület.

A járművek és jármű rendszerek biztonságának fontos része a gyártók, szervizelők és a járművet használók, a jármű működésének résztvevőinek az adott életciklusi fázishoz tartozó biztonságmenedzsment tevékenységének megvalósítása, mivel a járművek és járműrendszerek biztonságorientált alkalmazása ma már nem csak a tervező feladata. Ahogy a hagyományos járművek vezetői felelősek járművük biztonságáért úgy az autonóm járművek üzemeltetését végzőknek a kibertér autóipart érintő veszélyeire, valamint a járművek és járműrendszerek kiberbiztonságára is figyelemmel kell lenniük a jövőben.

Összegzésképpen a járművek fejlesztésének kiberbiztonsági elvei szerint a mindennemű kommunikáció védelmére, az érzékelők, a működést befolyásoló mikrokontrollerek és mikroprocesszorok védelmére, és a lehetséges folyamatosan változó fenyegetések enyhítésére kell törekedni az autóipari fejlesztések során. [45] A mesterséges intelligencia alkalmazása - a kognitív mobilitási platform kialakítása vagy éppen a tudás alapú kritikus vezetési funkciók megvalósítása a végponttól végpontig terjedő mély tanulás segítségével - a járművek és járműrendszerek biztonságának új dimenzióját jelenti. [46]

Köszönetnyilvánítás

A cikk kutatásaihoz az Új Széchenyi Terv keretein belül az EFOP-3.6.2-16-2017-00016 számú projekt biztosított forrást. A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.

Irodalomjegyzék

[1] WHO. (2015). WHO fact sheet on road traffic injuries. http://www.who.int/violence_injury_prevention/road_safety_status/2015/magnitude_A4_web.pdf?ua=1. Letöltve: 2018.05.20.

[2] Hamada, Y., et al. (2018). Anomaly-Based Intrusion Detection Using the Density Estimation of Reception Cycle Periods for In-Vehicle Networks. SAE Int. J. Transp. Cybersecurity Priv., 1(1), 39–56.

[3] Dürrwang, J. et al. (2017). Security Hardening with Plausibility Checks for Automotive ECUs. Icwmc 2017, 38–41.

[4] Continental Co. (2018) Vehicle Control Units in commercial vehicles.

[5] HNTB. (2018). Connected and Automated Vehicles. http://www.hntb.com/Newsroom/Media-Kits/Intelligent-Transportation-Systems. Letöltve: 2018.05.05

[6] HNTB. (2018). The Road to Autonomous Vehicles - 2018.

[7] SAE. (2018). Surface Vehicle Recommended Practice J3016TM, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. 35.

[8] United Nations. (2016). Proposal for draft guidelines on cyber security and data protection. 1–5.

[9] NHTSA. (2018) Automated Vehicles for Safety. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety. Letöltve: 04-Apr-2018.04.04.

[10] Európai Parlament és a Tanács. (2015). Az Európai Parlament és a Tanács (EU) 2015/758 rendelete (2015. április 29.) a 112-es egységes európai segélyhívó szolgáltatáson alapuló fedélzeti e-segélyhívó rendszer kiépítésével összefüggő típus-jóváhagyási követelményekről és a 2007/46/EK irányelv. Az Európai Unió Hivatalos Lapja.

[11] E. S. Hunyor. (2018). Alapfelszereltség lesz az autókban a vészhívó. https://www.hirado.hu/belfold/gazdasag/cikk/2018/05/03/alapfelszereltseg-lesz-az-autokban-a-veszhivo/#. Letöltve: 2018.05.20.

[12] Outay, F. et al. (2017).ConVeh: Driving Safely into a Connected Future. Procedia Comput. Sci., 113, 460–465,

[13] Dey, K. C. et al. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation. Transp. Res. Part C Emerg. Technol., 68, 168–184.

[14] Gheorghiu, R. A. et al. (2018) Messaging capabilities of V2I networks. Procedia Manuf., 22, 476–484.

[15] Ericsson. (2018). Connected Vehicle Cloud - Under The Hood. https://archive.ericsson.net/service/internet/picov/get?DocNo=28701-FGD101192. Letöltve: 2018.04.08.

[16] Albini A. és Rajnai Z. (2018). General Architecture of Cloud. Procedia Manuf., 22, 485–490.

[17] Attila, A. et al. (2018). IT Infrastruktúra Informatikai Biztonsági Aspektusai. Bánki Közlemények, 1(1), 11-16.

[18] Delgrossi, L. and Zhang, T. (2012). Vehicle Safety Communications. Veh. Saf. Commun.

[19] Connected car. https://en.wikipedia.org/wiki/Connected_car#cite_note-1. Letöltve: 2018.04.18.

[20] Turc, T. et. al. (2017). Web-based Wireless Sensor System for SCADA Environment. Procedia Eng., 181, 546–551.

[21] Federal Ministry of Transport and Digital Infrastructure. (2017). Action plan automated and connected driving.

[22] Mester, Gy. (2018) Autonóm önvezető robot autók. (kézirat)

[23] European Committee for Electrotechnical Standardization. EN 50126-2:2017. European Committee for Electrotechnical Standardization, Brussels, p. 79, 2017.

[24] Schuster Gy. and Terpecz, G. (2011). Járműiparban gyakran alkalmazott fedélzeti buszok," Repüléstudományi közlemények, 23(2).

[25] Fodor, D. és Szalay, Zs. (2014). Autóipari kommunikációs rendszerek. Pannon Egyetem.

[26] Dobrilovic, D. et al. (2016). A method for comparing and analyzing wireless security situations in two capital cities. Acta Polytech. Hungarica, 13(6), 67–86.

[27] Tokody, D. et al. (2017). Autonóm intelligens járművek helyzete Európában. Köztes Európa Társadalomtudományi Folyóirat A VIKEK Közleményei, 1–2(19–20),199–206.

[28] Schuster, Gy. et al. (2017). Software Reliability of Complex Systems Focus for Intelligent Vehicles. Lecture Notes in Mechanical Engineering (LNME) - Vehicle and Automotive Engineering, K. Jármai and B. Bolló, Eds. Miskolc: Springer Heidelberg, 309–321.

[29] Tokody, D. et al. (2017). An overview of autonomous intelligent vehicle systems. Lecture Notes in Mechanical Engineering (LNME) - Vehicle and Automotive Engineering, K. Jármai and B. Bolló, Eds. Miskolc: Springer Heidelberg, 287–307.

[30] Deloitte GmbH. (2017). Automotive Software Quality What do OEM's have to consider for the future?, 8, 14.

[31] Abonyi J,. és Fülep, T. (2014) Chapter 3 - Safety critical systems. http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/ch03.html. Letöltve: 2018.05.18.

[32] Muha, L. (2004). Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szle., 17(4), 137–156.

[33] Pető, R. (2012). Gépjárművek ballisztikai védelme. Hadmérnök, 7(1), 32–39.

[34] Iantovics, L. B. et al. (2017). MetrIntMeas a novel metric for measuring the intelligence of a swarm of cooperating agents. Cogn. Syst. Res., 45, 17–29.

[35] Kassai, K. (2012). Kiberveszély és a magyar honvédség. Hadmérnök, 7(4), 128–141.

[36] Parkinson, S. et al. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Trans. Intell. Transp. Syst., 18(11), 2898–2915.

[37] Hashem Eiza, M. és Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Veh. Technol. Mag., 12(2),45–51.

[38] Beláz, A. és Berzsenyi, D. (2017). Kiberbiztonsági Stratégia 2.0 - A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 1-15.

[39] Petit, J. et al. (2015). Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. Black Hat Europe, 1–13.

[40] United States Government Accountability Office. (2016) Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack.

[41] 5/1990. (IV. 12.) KöHÉM rendelet, a közúti járművek műszaki megvizsgálásáról. http://njt.hu/cgi_bin/njt_doc.cgi?docid=12356.351598. Letöltve: 2018.06.06.

[42] 6/1990. (IV. 12.) KöHÉM rendelet, a közúti járművek forgalomba helyezésének és forgalomban tartásának műszaki feltételeiről." http://njt.hu/cgi_bin/njt_doc.cgi?docid=12392.351571. Letöltve: 2018.06.06.

[43] Wooderson, P. (2016). Automotive Cyber Security Testing. Presentation

[44] Schmittner, C. et al. (2016) Using SAE J3061 for automotive security requirement engineering. Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science, 9923, 157-170. Springer, Cham

[45] Fachot, M. (2017). Protecting road vehicles from cyber attacks. IEC e-tech, https://iecetech.org/issue/2017-03/Protecting-road-vehicles-from-cyber-attacks. Letöltve: 2018.05.20.

[46] Federal Ministry of Transport and Digital Infrastructure. (2017) Report-Ethics-Commission. https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile. Letöltve: 2018.05.20.

BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Az Ipar 4.0 hatása az egyetemi oktatásra - megfelelés az új ipari kihívásoknak

Impact of Industry 4.0 in university education - adequacy to the new industry challenges

Dr. Czifra György
Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, Magyarország
czifra.gyorgy@bgk.uni-obuda.hu

***Összefoglalás* — Az I4.0 a hallgatók és az oktatók részéről is megköveteli a megfelelő képzettséget, problémamegoldó-képességet, és természetesen a megfelelő tudományos felkészültséget. A felsoroltakat csak megfelelően kialakított környezetben lehetséges elérni, ezért az egyetemek kényszerítve vannak a megfelelő oktatási feltételek kialakítására. Cikkünkben arra teszünk kísérletet, hogy megtaláljuk azt az utat, amelyen járva képesek leszünk felkészíteni a hallgatókat az I4.0 kihívásaival való küzdelemre.**

***Kulcsszavak*:** Ipar 4.0, egyetemi képzés, kihívás, megfelelés

***Abstract* — I4.0 requires from students and educators to have the adequate skills, problem-solving skills and, of course, the appropriate academic skills. These skills can be achieved only in an adequately designed environment. Universities are therefore forced to develop their educational conditions according to I4.0 requirements. In our article we attempt to find the way for preparing our students for the challenges of I4.0.**

***Keywords*:** Industry 4.0, university education, challenge

1 BEVEZETÉS

A technológiai fejlődés drámai változásokat okozott a termelékenység területén. A gőzgépek megjelenése a 19. században, az elektrifikáció a huszadik század elején, valamint az automatizáció térhódítása a 80-as évek elején mind ipari forradalmat indított el. Napjainkban a technológiai fejlődés negyedik hullámát éljük, melyet digitális ipari forradalomként ismerünk és Ipar 4.0-nak nevezünk. Hálózatba kapcsolt kiber-fizikai rendszerekről beszélünk, melyek standard internetes kommunikációt biztosító protokollok segítségével kapcsolatba tudnak lépni egymással. A rendszerek adataik elemzése alapján hiba-előrejelzésre is képesek, újrakonfigurálják magukat és így képesek alkalmazkodni az ismert és ismeretlen változásokhoz is. Az I4.0 lehetővé teszi a közvetlen adatgyűjtést az egyes berendezésekről, lehetővé téve ezzel a gyorsabb, rugalmasabb, hatékonyabb gyártási eljárások alkalmazását és a magasabb minőségű, olcsóbb termékek gyártását. A felsoroltak miatt megnövekszik a termelékenység, amely a gazdaságot is előbbre mozdítja, elősegíti az ipar fejlődését és alapjaiban változtatja meg a vállalatok versenyképességét.

2 AZ IPAR 4.0 FOGALOM MEGHATÁROZÁSA

Az Ipar 4.0 kifejezés a negyedik ipari forradalom fogalmát jelenti, ami magában foglalja az információs forradalmat, a kommunikációs forradalmat, az automatizálás mesterséges intelligenciával való bővítését, valamint a nagy adattömegek mozgatását és a felhőalapú adatfeldolgozást is.

Mint az az előbbi felsorolásból is látszik, nagyon sokrétű és szerteágazó folyamatokról beszélünk, amelyek lassan behálózzák az egész ipari környezetünket. Okos gyárak, okos termelőeszközök, okos és intelligens járművek, önálló döntéshozatalra képes eszközök, amelyek az egymás közötti információcsere segítségével emberi beavatkozás nélkül képesek váratlan eseményre helyesen reagálni, vagy az ember által definiált célt saját erőforrásaikat mozgósítva, szervezve és átszervezve elérni.

A folyamat egyértelműen a humán erőforrás felhasználásának minimalizálása és a mesterséges intelligencia által irányított okos eszközök maximális használata felé irányul. Alapjában véve ez a trend kívánatos, hiszen az ember, mint jelentős hibaforrás kizárása a folyamatokból a termelés és ellátás maximális minőségét, időfüggetlenségét és egyenletességét jelenti.

Ahhoz, hogy a különböző folyamatok, az intelligens gyárak, közlekedési rendszerek el tudják látni a rájuk bízott feladatokat, több feltételnek is meg kell felelniük.

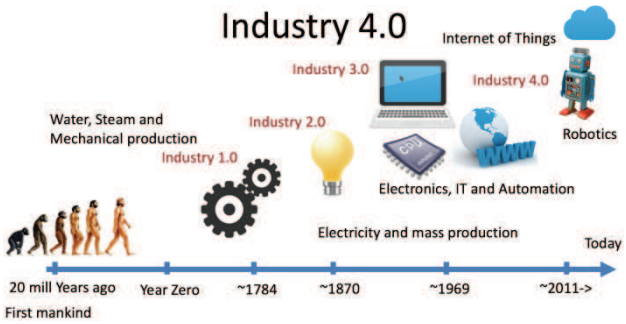
Az első feltétel, hogy a folyamatokban részt vevő rendszerelemek megfelelő adatokat, információkat legyenek képesek előállítani, amelyek leírják a pillanatnyi állapotukat, az általuk végzett tevékenység aktuális lefolyását. A következő feltétel, hogy az így keletkezett adatokat, információkat megosszák egymással, illetve továbbítsák egy biztonságos, állandóan rendelkezésre álló tárhelyre – ezt a felhőalapú számítógépes adatfeldolgozási eljárások teszik lehetővé.

Mivel minden egyes, a rendszerbe integrált eszköz adatokat állít elő, másodpercenként elképzelhetetlen mennyiségű adat forgalmát kell lebonyolítani. Egészen különleges adatforgalmazási eljárások felhasználásával ez a probléma megoldható.

Az adatok, információk óriási mennyisége kezelhetetlen tömegként semmire nem jó, ezért ki kell fejleszteni olyan intelligens adatelemző eljárásokat, amelyek segítségével egyszerű, átlátható és döntésképességet támogató információs képernyők jeleníthetők meg, illetve a mesterséges intelligencia különböző szintjein dolgozó rendszerek képesek önálló döntéseket hozni.

A döntéseket felügyelő rendszereknek tanulóképeseknek kell lenniük, hogy a már előfordult

problémák megoldásait adaptálni tudják a hasonló, de még az előzőekben nem tapasztalt meghibásodások kezelésére.



1. ábra: Az Ipar 4.0 kialakulása [11]

3 AZ IPAR 4.0 ÉPÍTŐELEMEI

Bármilyen I4.0 rendszer esetében meg tudunk különböztetni legalább négy alapvető tudományterületet, amelyek egymással összekapcsolva azt működőképessé teszik.

A mechanikai komponens képezi a rendszer gerincét, felel a mozgás, az erőátvitel, a statika, a kinematika és dinamika megvalósításáért.

Az elektrotechnikai komponens képezi a rendszer idegpályáit, felel a megfelelő impulzusok átviteléért.

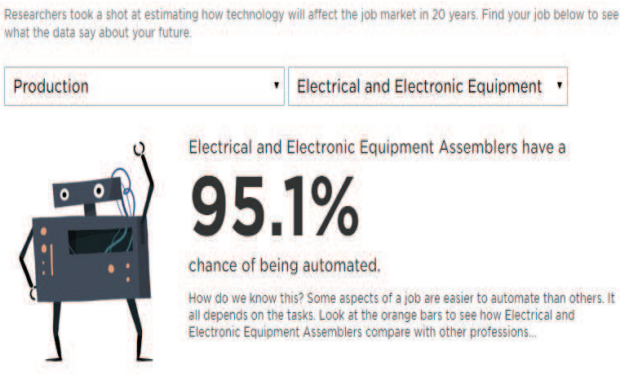
Az informatikai komponens képezi a rendszer irányító, vezérlő és kontroll impulzusainak forrását. Adatok, információk forrása és címzettje is.

A kibernetikai komponens képezi a rendszer agyát, vezérlését, intelligenciáját. Biztosítja a tanulást, a megfelelő reakciók generálását, ez tulajdonképpen a rendszer lelke.

Természetesen a fenti felosztás csak nagy vonalakban tükrözi egy I4.0 kompatibilis rendszer fő alkotóelemeit, azonban világosan látjuk, hogy a hagyományos gépész, villamossági szakember, informatikus és kibernetikus felosztást bátran elfelejthetjük. Valójában a mechatronika az, ami a legjobban megközelíti az általunk meghatározott tartalmat, ám az informatikát és a kibernetikát is integrálnunk kell, ha pontosak akarunk lenni. Így talán egy új kifejezés, a MEKI (Mechanika - Elektronika – Kibernetika – Informatika) lehet a legkifejezőbb.

Az előbbi gondolatsor valójában azt hivatott bemutatni, hogy milyen sokrétű, szerteágazó tudásra és információhalmazra van szüksége annak a szakembernek, aki helyt akar állni az Ipar 4.0 által életre hívott versenyben.

Az ipari robotok alkalmazásának üteme a 2007-es évtől kezdődően az addigi lineáris ütemről exponenciálisra változott. Erőteljes növekedés figyelhető meg a Távol-Keleten, illetve Kínában, ami annál is figyelemreméltóbb, mivel felmerül a kérdés, hogy a hagyományosan olcsó „keleti” munkaerőt helyettesítik-e a robotok, vagy egyéb területeken is átveszik az emberi munkaerő hagyományos szerepkörét? Az emberi munkaerővel szemben támasztott szakmai képzési követelmények megváltozása és a súlypontok eltolódása miatt néhány szakma erős fenyegetettségnek van kitéve – az alábbi ábra is ezt hivatott tükrözni.



2. ábra: Az emberi munkaerő robotokkal való helyettesítésének esélye [10]

A [10] forrásban elérhető adatok inkább tendenciákat mutatnak, vannak olyan területek, ahol szinte biztos és 90% feletti a helyettesítés veszélye, vannak azonban olyan szakmák, ahol a helyettesítés megoldhatatlan (minimális, inkább támogató jellegű) – bár a mesterséges intelligencia egyre nagyobb fejlettségi szintje ezen a téren is egyre emelkedő fenyegetettséget indukál.

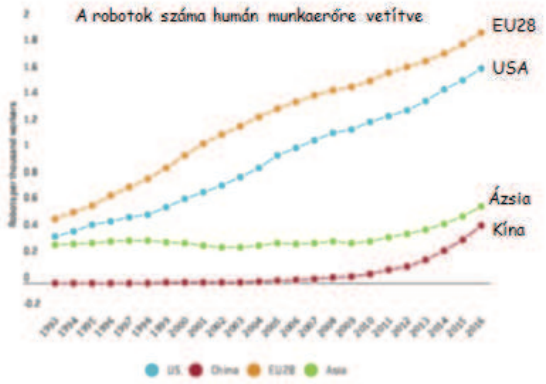
A komputerizáció hatása a munkaerő piacára meglehetősen jól fel van dolgozva különböző szempontok szerint [19]. A tendencia azt mutatja a kutatások szerint, hogy a rutin műveletekre alapozott munkát ellátó munkaerő foglalkoztatottsága csökken, ők azok, akiknek a tevékenysége jól algoritmizálható és így könnyen helyettesíthetők megfelelő intelligenciájú gépekkel. Szembetűnő a szerkezeti változás a munkaerőpiacon, a munkavállalók a közepes jövedelmű foglalkozásoktól átcsoportosulnak az alacsonyabb jövedelmet biztosító szakmák, tevékenységek felé. Ezek alapjában véve olyan foglalkozások – szolgáltatások, amelyek nagyrészt manuális szakmunkát jelentenek, amelyek kevésbé érzékenyek a számítógépesítésre, hiszen magasabb szintű követelményeket igényelnek a rugalmasság, a kreativitás, esetleg a fizikai alkalmazkodóképesség szempontjából is.

Megfigyelhető ugyanakkor, hogy kreatív, nagyobb problémamegoldó készségeket igénylő tevékenységet végző munkaerő iránti kereslet erőteljes növekedésnek indult. A kereslet növekedése, a munkaerőpiaci tendenciák megváltozása megjelenik az oktatásban is, tartósan növekszik az igény a kognitív feladatokat megoldani képes szakembereket magas szakmai színvonalon képző intézmények iránt.

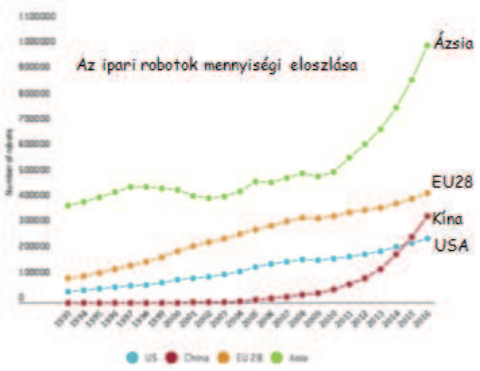
Két jól elkülöníthető csoport alakul ki, a magas jövedelmű kreatív, kognitív munkahelyeken dolgozók, illetve az alacsony jövedelmű, mondhatni kézműves foglalkozásokban való foglalkoztatás. A közepes jövedelmű, rutinmunkát végző munkahelyek kiürülnek.

Kimondhatjuk tehát, hogy valóban megjelennek új szakmák, új munkaerőprofilok, illetve eltűnnek jól bevált, biztos megélhetést nyújtó foglalkozások, szakmák, amelyek jól helyettesíthetők robotokkal, illetve mesterséges intelligenciával.

Riasztó a munkaerőhiány Magyarországon is, a vendéglátó szektort pedig fokozottan sújtja a jelenség. Győrben egy kínai étterem robotot vet be a vendégek kiszolgálása érdekében. [20]



3. ábra: Az ipari robotok száma humán munkaerőre vetítve [9]



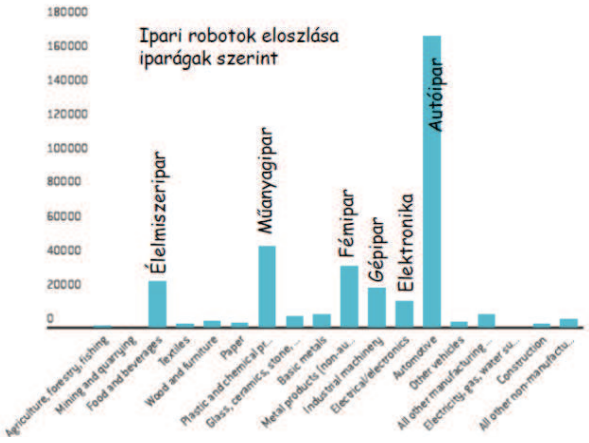
4. ábra: Az ipari robotok mennyiségi eloszlása [9]

További statisztikai adatokat elemezve világosan elkülöníthetők az iparnak azon területei, ahol a robotizáció – és a vele együtt alkalmazott egyéb I4.0 fejlesztések és megoldások – egyre nagyobb részben épülnek be a napi gyakorlatba. Az egyik valóban dinamikusan fejlődő iparág a járműgyártás, kiemelkedően az autógyártásra jellemző a rendkívül gyors emelkedés. Az elektromos vagy hibrid hajtásra való világméretű, egyre dinamikusabb átállás nyilván komoly változást fog hozni a gyártórendszerek tekintetében – elsősorban a hajtásláncot illetően. A motorgyártás, a váltóművek, futóművek gyártása teljesen átalakul a kerékagyba épített villamos hajtásoknak köszönhetően. Az önvezető járművek – és nem csak a személygépkocsik tekintetében – tömeges elterjedése forradalmasítja a mindenhol elérhető, gyors és biztonságos adatátviteli technológiákat. Természetesen a karosszériagyártás, a járművek belső terének kialakítása is szinte beláthatatlan változásokat generál a tervezés és a gyártás területén is. Már most is látható, hogy a robotizáció elterjedése milyen mértékű és léptékű.

Csak egy példát szeretnék bemutatni, a Honda után a BMW-nek is van önvezető motorkerékpárja, amely emberi irányítás nélkül is képes közlekedni. Egy csoport Stefan Hans mérnök irányításával dolgozott az R 1200 GS átalakításán. A cél nem az ember kiváltása volt, hanem olyan műszaki megoldás létrehozása, amelynek segítségével a biztonsági rendszerek a jelenleginél nagyobb mértékben tudnak beavatkozni és megvédeni a jármű vezetőjét és utasát az esetleges balesetektől.

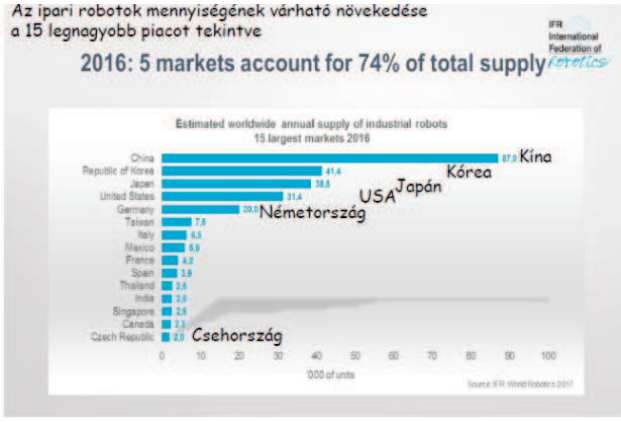
A fejlesztők véleménye szerint a kifejlesztett önvezető rendszer képes lesz megtanulni a motorkerékpáros vezetési stílusát, és a tanulást követően pedig már képes lesz felismerni a veszélyes helyzeteket, közbe tud avatkozni. Nemcsak reagálni – jelezni tud, hanem be is avatkozik aktívan. Természetesen a teljesen önvezető motorkerékpár sorozatgyártása nincs tervben, viszont néhány sikeresen tesztelt megoldás – sávtartó automatika, adaptív sebességtartó automatika már sorozatgyártásban is megjelenhet a közeli jövőben.

5. ábra Az önvezető BMW motorkerépár [21]



6. ábra: Ipari robotok eloszlása iparágak szerint [9]

A következő ábrából világosan látható, hogy az ipari robotok piacán a legnagyobb öt felvevő az egyéb területeken is hatalmas fejlődést produkáló ország:

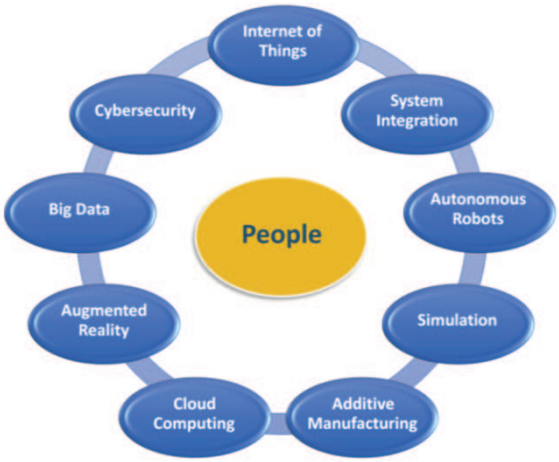


7. ábra: Az öt legnagyobb felvevő ország [15]

4 MILYEN KÉPZÉS KELL?

Kilenc olyan kulcstechnológiát lehet felsorolni, amelyek oktatása elengedhetetlen egy mai, a kor követelményeinek megfelelő, felsőfokú végzettséggel rendelkező szakember részére:

1. Szimulációs rendszerek (Process Simulation),
2. Kiterjesztett valóság (Augmented Reality),
3. Autonóm robotok (Autonomus Robots),
4. Additív gyártás (Additive Manufacturing) ,
5. A dolgok internete (Internet of Things),
6. Felhő alapú számítástechnika (Cloud Computing),
7. Big data és elemzés (Big Data Transfer and Processing),
8. Kiber biztonság (Cyber Security),
9. Horizontális és vertikális rendszer integráció (Horizontal and Vertical System Integration).



8. ábra: Az I4.0 és az emberek [13]

Jól látható, hogy túlnyomórészt az elektronika, informatika és kibernetika témakörei azok, amelyben előre kell lépni és a megfelelő laboratóriumok kialakításával, a hozzá illeszkedő tananyag elkészítésével – természetesen e-learning alapon – el kell érni az ipar számára értékes és hasznos szakemberek képzését. Nyilvánvaló, hogy a képzés nyertesei nemcsak a vállalatok, hanem a képzésben résztvevők is, hiszen munkaerő-piaci pozíciójuk magasan az ilyen képzést nem abszolválóké felett lesz.

Tudatosítanunk kell azonban, hogy a megszerzett tudást megerősítő gyakorlati készségek elsajátítását lehetővé tevő szakmai kapcsolatok megerősítése, új kapcsolatok létrehozása nélkül a laborok és a tantárgyi tematikák sem használhatók megfelelő hatékonysággal.

A modern oktatásban – és az itt szereplő sokféle tudományág miatt törvényszerűen – csak a projektorientált, önálló és kollektív feladatmegoldásokat lehetővé tevő módszertan alkalmazása hozhat megfelelő eredményt. A vállalatok, amelyek felismerték az I4.0–ban rejlő kihívásokat és piacvezető szerepet töltenek be az ipari automatizáció szegmensében, saját képzéseket indítanak. A képzések elsősorban a felnőttképzés kategóriájában kerülnek meghirdetésre, a felhasznált technológiák, oktatási módszerek és segédanyagok kiválóan alkalmazhatók a felsőoktatásban is. A vállalatok reagálnak arra a tényre, hogy az ipari automatizáció és az intelligens gyártórendszerek elterjedése rohamos – exponenciális fejlődésnek indult. Nincs idő megvárni a megfelelően képzett mérnökök megjelenését a munkaerőpiacon, annál is inkább, hiszen a felsőoktatás sincs még felkészülve az I4.0 szellemében folyó oktatásra, sem a humánerőforrás, sem az oktatási segédeszközökkel való ellátás szempontjából. Az egyetlen, amire az I4.0 bevezetését fontolgató vállalatok támaszkodhatnak, az a saját erőforráskészletük. Ahhoz, hogy szakmailag megfelelően képzett, a modern technológiát bevezetni, alkalmazni és fejleszteni képes mérnökök, szakemberek álljanak rendelkezésre, az ilyen témájú képzéseket szervező és megvalósító cégekre kell támaszkodniuk.

5 HOGYAN TOVÁBB?

A főiskolai és egyetemi képzésnek nagyon gyorsan fel kell vennie a ritmust, meg kell keresni azokat az ipari partnereket, akik megfelelő infrastruktúrával és a képzéseket magas szinten művelő szakembergárdával rendelkeznek és szorosan, egymást támogatva, együttműködve olyan képzési formákat tudnak bevezetni, amelyek garantálják a gyors és hatékony képzést.

Az egyetemek és főiskolák finanszírozási rendszere szinte lehetetlenné tesz az önálló fejlesztéseket, megfelelő pályázatok indításával azonban ez megváltoztatható. Elképzelhetőnek tartom, hogy a felsőoktatási intézmények egymással együttműködve, koordináltan fejlesszék képzési bázisaikat, elosztva a képzési területeket és megfelelően átgondolt és megtervezett szervezettséggel specializálódva, csak a saját területre koncentráljanak. A hallgatók szempontjából átjárhatóvá kell tenni ezeket a képzéseket oly módon, hogy a már az előbbiekben kifejtett multidiszciplináris képzési portfóliót az egyes specializált egyetemi központokban elérhessék.

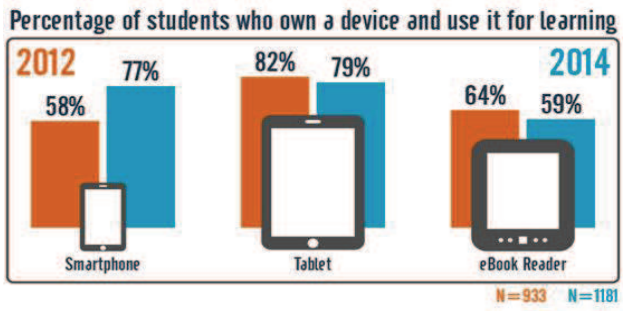
Az Óbudai Egyetemet vizsgálva egyértelmű, hogy olyan képzési portfóliót kell kialakítani, amely biztosan támaszkodik az eddigi tudományos, kutatási és oktatási profilra, megfelel az I4.0 követelményeinek és olyan kimeneti képzési követelményeket határoz meg, amelyek biztos és használható felkészülést jelent a jövő intelligens gyáraiban dolgozó fiatal és ambiciózus mérnökök számára.

Ahhoz, hogy meg tudjunk felelni az előttünk álló feladatoknak, a teljesség igénye nélkül sorolom fel a teendőket – hiszen egy rendkívül dinamikus folyamatról lévén szó, szinte hetek alatt változhatnak a követelmények:

⇒ megfelelő felszereltséggel rendelkező laboratórium kiépítése,
⇒ a laboratórium felszereltségéhez igazodó tantárgyi program (programok) kialakítása,
⇒ a megszerzett tudást megerősítő gyakorlati készségek elsajátítását lehetővé tevő szakmai kapcsolatok megerősítése, új kapcsolatok létrehozása,
⇒ projektorientált, önálló és kollektív feladat-megoldásokat lehetővé tevő módszertan alkalmazása,
⇒ a hallgatók bevonása a laborfelszerelés kialakításába,
⇒ Tudományos Diákköri Konferencia – témák kiírása,
⇒ megfelelő szakdolgozati témák kiírása,
⇒ az Ipar 4.0 szakterületeihez kapcsolódó tantárgyak projektorientált szervezése – laborfejlesztési feladatok, segédeszközök tervezése és gyártása,

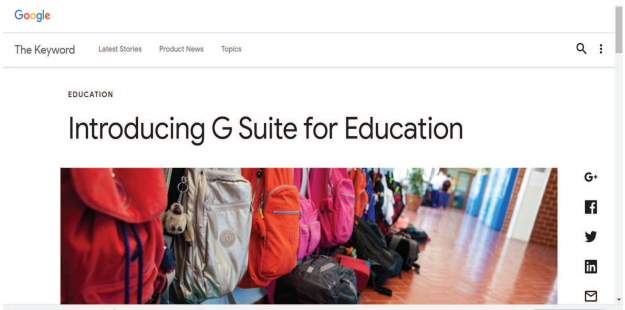
⇒ Kandó Kálmán, Neumann János és Bánki Donát együttműködése – közös projektek megfogalmazása,
⇒ pályázatok, valamint hallgatói és tanári mobilitás-programok szervezése.

Amint a felsorolásból is kitűnik, van mit tenni annak érdekében, hogy az Óbudai Egyetemen végzett hallgatók meg tudjanak felelni a velük szemben támasztott igényeknek. Az oktatás szempontjából a használt eszközök is kritikus jelentőségűek. Az alábbi ábrán egy érdekes statisztika látható, milyen eszközöket használnak a hallgatók a tanulás folyamatában, hogyan változott az eszközök portfóliója az évek során.



9. ábra: Okos eszközök a tanulás folyamatában [14]

Az egyre – másra megjelenő technológiák beépítése kritikus jelentőségű, hiszen a mai főiskolai, egyetemi hallgatók lételeme a digitális világ. A hagyományos oktatási módszerek – összehasonlítva a ma elérhető modern módszerekkel – rendkívül ingerszegények. A szinte percről percre változó igényeknek csak az olyan oktatási technológiák használata felel meg, amelyek képesek gyorsan emészthető formába önteni az elsajátítandó ismereteket. Az egyik ilyen példa – a széles körben ismert virtuális oktatási platformok mellett – a Google virtuális osztálya.



10. ábra: Virtuális osztály [16]

A felhő alapú tanulás, oktatás beépül mindennapjainkba, az elektronikus távoktatás fogja képezni az alapismeretek elsajátításának legelterjedtebb módját.

A rendelkezésre álló tananyagok, illetve a közeli jövőben kidolgozásra kerülők – a tananyag jellegének megfelelően – csak elektronikus úton lehetnek elérhetőek, olyan távoktatási platformokon, amelyek lehetővé teszik a rugalmas időbeosztást, a saját igények, lehetőségek és képességek szerinti előrehaladást, az állandó hatékony tudásszint-ellenőrzést. A gyors változások követése kizárólag az említett oktatási technológiák alkalmazásával lehetséges.

A tananyag megfelelő feldolgozása kulcsfontosságú. Az elektronikus tananyag összeállítása egy jól konfigurált csapat feladata, aminek összetétele a következő: szakmai vezető, a szakmai vezető asszisztense, didaktikai szakember, informatikus, (webreklám szakember – grafikus), médiaszakember, pszichológus. Csak egy ilyen team képes arra, hogy olyan tananyagot állítson elő, amely megfelel a modern kor szellemének, dinamikus, célzott ismereteket ad és felépítésével, szervezettségével garantálja a tudnivalók elsajátítását a kurzuson résztvevők részére.

Az előbbi alapelvek szerint felépített tananyag mellett természetesen elengedhetetlen a megfelelő laboratóriumok kiépítése is, hiszen az e-learning során elsajátított tudás mellett a készségeket is el kell sajátítani. Biztos elméleti alapokra építve könnyebb és tartósabb is a gyakorlati készségek elsajátítása és begyakorlása. A kreatív gondolkodás és proaktív problémamegoldás folyamatait csakis a megfelelően kiépített, az e-learning tananyagával összhangban működő laboratóriumok, gyakorlati munkahelyek támogatják hatékonyan.

Nem szabad azonban alábecsülnünk a fenntartás, illetve a folyamatos fejlesztés költségeit sem. Az ipari környezet exponenciális fejlődési üteme meghatározza a tananyagok és a laboratóriumok fejlesztési ütemét is. Ebben a vonatkozásban ismét előtérbe kerülnek a jó ipari kapcsolatok, a fejlesztésben érdekelt vállalatok bekapcsolása a képzés és a tananyagfejlesztés folyamatába. A már említett finanszírozási problémák miatt kiemelt jelentőségű lehet azoknak a vállalatoknak a bevonása, amelyek megfelelő infrastruktúrával rendelkeznek egy-egy kihelyezett gyakorlati képzési pont kialakításához, valamint rendelkeznek olyan szakemberekkel, akik képesek a gyakorlati képzést vezetni ezeken a pontokon.

6 A JÓ GYAKORLATOK PÉLDÁJA

Követendő példaként szeretném bemutatni néhány vállalat megoldását, amelyek az I4.0 alapelveit hivatottak bemutatni és megtanítani mindazoknak az érdeklődőknek – elsősorban a felnőttképzés területén – akiknek munkájuk során szükségük van az Ipar 4.0-val kapcsolatos ismeretekre.

Az egyik ilyen példa a Bosch Rexroth Csoport képzési portfóliója és műszaki háttere. Idézem a cég vonatkozó elképzelését: „A vállalatcsoport azonban nemcsak fejleszti, hanem gyáraiban alkalmazza is a koncepciót és az ezzel kapcsolatos új megoldásokat. Az így gyűjtött tapasztalatok alapján a Drive & Control Academy szakemberei kifejlesztették az mMS4.0 oktatóberendezést, amelynek segítségével az Ipar 4.0 a gyakorlatban is könnyen modellezhető. A berendezés egy teljes termelési rendszer összes funkcióját tartalmazza. A rendszer moduláris, további cellák, például egy hat szabadságfokú robot is egyszerűen hozzáadható. Az Open Core Engineering segítségével a tanulók magas szintű programnyelveken programozhatják a Rexroth PLC-ket, az anyagáramlás RFID-rendszer segítségével követhető és a termelési adatok összeköthetők a különböző vállalatirányítási rendszerekkel (pl.: ERP, MES, SAP). Ezen felül a könnyebb megértés érdekében a Rexroth modern, animációkkal és videókkal színesített e-training oktatóanyagot is kínál az Ipar 4.0-hoz. A Bosch Rexroth oktatási csomagja és az mMS4.0 oktatóberendezés segítségével a tanulók és a szakemberek már ma

elsajátíthatják a jövő gyárában szükséges tudást és képességeket." [17]

A másik rendkívül érdekes példa a SmartFactoryKL projekt, amely egyfajta, gyártófüggetlen, demonstrációs és kutatási platform, ahol az ígéretes, innovatív információs és kommunikációs technológiákat (IKT) kutatják, fejlesztik és mutatják be valós ipari termelési környezetben. Az Ipar 4.0 megvalósítása megköveteli a kreativitást, a kísérletezéshez és az együttműködéshez való proaktív hozzáállást. Az együttműködő cégek, valamint a kutatási és oktatási intézmények felismerték az együttműködésben rejlő lehetőségeket, az erős hálózatban fontos tapasztalatokat szereztek, gyakorlati megoldásokat fejlesztettek ki, és fontos szerepet játszottak az intelligens gyár jövőjének kialakításában. [18]

7 Összegzés

Az elmondottak alapján megállapíthatjuk, hogy a munkaerő szerepe megváltozik. A passzív gépkezelői-operátori tevékenység átalakul aktív, kreatív, problémamegoldó, optimális innovatív megoldásokat kereső munkává, melynek feltételeit az egyetemi képzésben nagyon gyorsan meg kell teremteni. Abban az esetben, ha a szemléletváltás, a környezet innovációja, az új tanulmányi programok, tantárgyak nem épülnek be az oktatásba belátható (1-2 év) időn belül, visszafordíthatatlanul a lemaradás és a kimaradás folyamata fog elindulni és lavinaként maga alá temeti a megújulásra képteleneket.

Percentage of Use of Industry 4.0		
Industrial Sector	**Now (%)**	**In Five Years (%)**
Electronics	45	77
Aerospace/Defense	32	76
Industrial manufacturing	35	76
Chemicals	32	75
Forest products/Paper	38	72
Transportation	28	71
Engineering/Construction	30	69
Automotive	41	65
Metals	31	62

11. ábra: Az I4.0 térhódítása [12]

A vállalati szféra bevonása a képzésbe kulcsfontosságú, hiszen, egyre növekszik azoknak a vállalatoknak a száma, amelyek saját szakemberképzést indítanak, saját erőforrásaikat képezik ki. Nagyon fel lehetne gyorsítani a felkészítés ütemét, ha erős szövetségben az erre nyitott vállalatokkal közös platformokon el lehetne indítani képzéseket, amelyekre a későbbiekben biztosan lehet építeni.

Nagyon jó példa a vállalati együttműködésre a Bánki Donát Gépész és Biztonságtechnikai Mérnöki karon megvalósuló projekt. Az Enterprise Communications Magyarország Kft. -vel közösen, a vállalat hathatós támogatásával indul egy képzés, CAD-CAM a gyakorlatban címmel. A képzésben 12 hallgató vesz részt, illetve a képzést támogató tanárok és demonstrátorok is. 12 munkaállomáson telepítésre került a SolidEdge illetve az EdgeCAM programcsomag, a hallgatók szabad labor formájában is hozzáférhetnek az eszközökhöz. A munka során létrehozott, megtervezett 3D modell-termékre a résztvevők elkészítik a megfelelő megmunkálóprogramot és a terméket a kar rendelkezésre álló gépein le is gyártják, így kézzelfogható eredménye lesz az elméleti alkotó munkának.

Irodalomjegyzék

[1] http://www.industry4.hu/hu/ipar4
[2] https://autopro.hu/trend/
[3] https://www.i40platform.hu/
[4] http://www.festo-didactic.com
[5] https://www.boschrexroth.com/hu/hu/felnottkepzes/ipar-4-0-oktatas/
[6] http://smartfactory.de/en/
[7] http://www.cnc.hu/digitalization/
[8] http://www.techmonitor.hu/
[9] http://bruegel.org/2017/12/the-growing-presence-of-robots-in-eu-industries/
[10] https://www.npr.org/sections/money/2015/05/21/408234543/will-your-job-be-done-by-a-machine
[11] http://halvorsen.blog/documents/technology/industry40/
[12] https://www.quora.com/What-will-be-the-top-10-industries-that-will-change-in-2017-due-to-Industry-4-0
[13] http://menawat.com/industry-4-0-what-it-is-and-what-to-expect/
[14] https://er.educause.edu/articles/2015/6/students-mobile-learning-practices-in-higher-education-a-multiyear-study
[15] https://ifr.org/ifr-press-releases/news/ifr-forecast-1.7-million-new-robots-to-transform-the-worlds-factories-by-20
[16] https://blog.google/topics/education/introducing-g-suite-education/
[17] https://www.boschrexroth.com/hu/hu/felnottkepzes/ipar-4-0-oktatas/trends-und-themen-2
[18] http://smartfactory.de/en/
[19] https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
[20] https://www.penzcentrum.hu/karrier/sirhatnak-a-magyar-pincerek-videon-a-gyori-robot-ami-elveheti-a-munkajukat.1070096.html
[21] http://www.automotor.hu/motor/onvezeto-motorkerekpart-keszitett-a-bmw/

2018 Reviewers

ANCZA Erzsébet
BAKOSNÉ DIÓSZEGI Mónika
CZIFRA Árpád
BEREK Lajos
DRÉGELYI-KISS Ágota
FARKAS Gabriella
GONDA Viktor
HORVÁTH Richárd
KERTI András
KISS Gábor
KOVÁCS Tibor
KOVÁCS Tünde
ŐSZI Arnold
MIKÓ Balázs
MOLNÁR Ildikó
MUCSI András
NAGY Rudolf
POKORÁDI László
RAJNAI Zoltán
SZABÓ József Zoltán
SZAKÁCS Tamás
SZŰCS Endre
SZLIVKA Ferenc