ISSN 2676-9042

Vol 3, No 2, 2021.

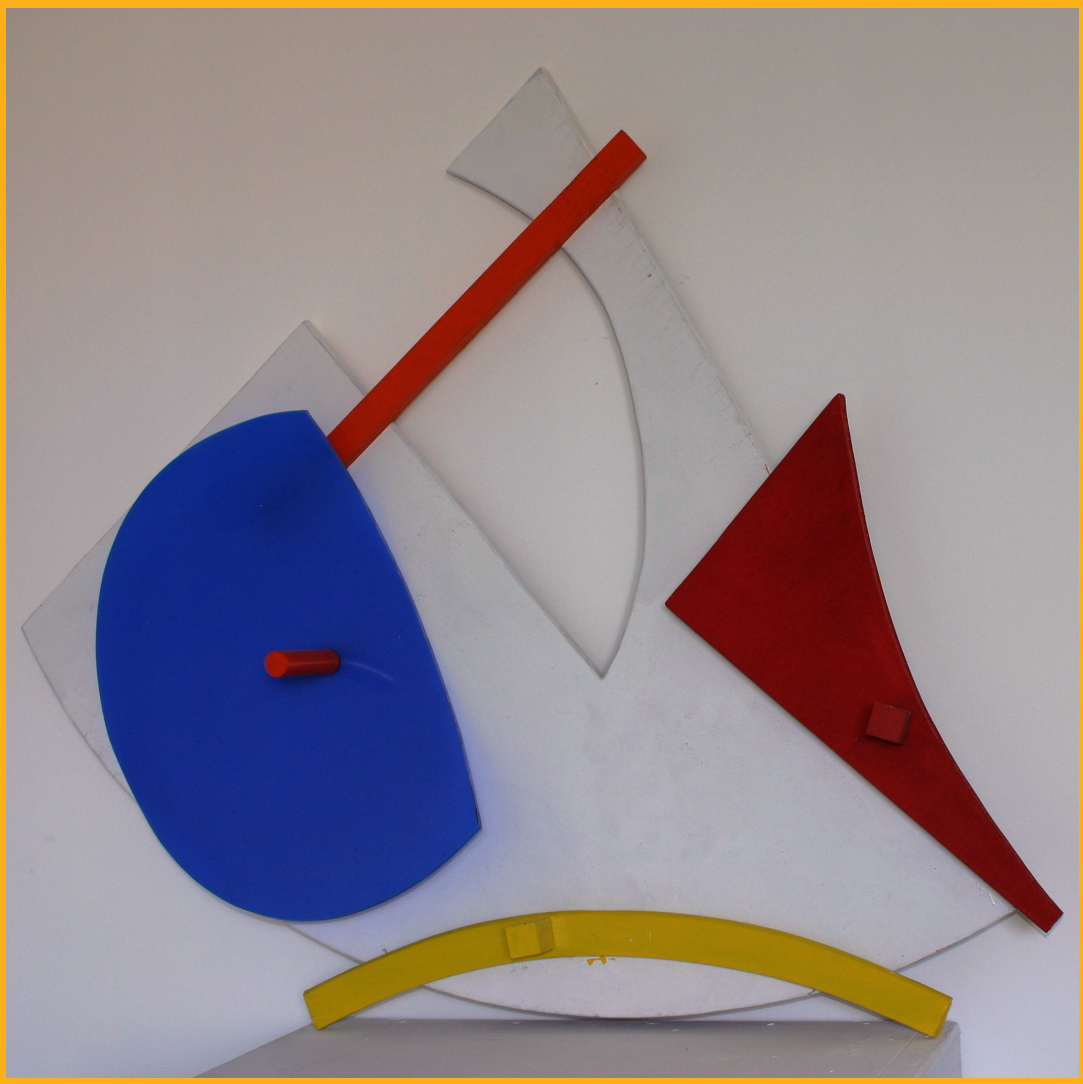
2021, III. évf. 2. szám

Safety and Security Sciences Review

international, peer-reviewed, professional and scientific journal of safety and security sciences

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata



https://biztonsagtudomanyi.szemle.uni-obuda.hu

On the cover can be seen | A borítón
ÉZSIÁS István
sculptor/szobrászművész
MADI relief | **MADI relief**
statue | című szobra látható

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

COLUMNS	ROVATOK
Material Safety	Anyagbiztonság
Philosophy and History of the Safety and Security	Biztonságfilozófia és -történet
Security Policy	Biztonságpolitika
Security Systems	Biztonságtechnika
Security Awareness	Biztonságtudatosság
Domotics	Domotika
Health Security	Egészségbiztonság
Food Safety	Élelmiszerbiztonság
Economic Security	Gazdasági biztonság
War Security and Law Enforcement	Hadbiztonság és rendvédelem
Information Security	Információbiztonság
Industrial and Operational Safety	Ipar- és üzembiztonság
Legal and Social Security	Jog- és társadalombiztonság
Book Review	Könyvismertetés
Security of Environment	Környezetbiztonság
Traffic Safety	Közlekedésbiztonság
Private Security	Magánbiztonság
Artificial Intelligence	Mesterséges intelligencia
Safety and Security in General	Munkabiztonság
Technical Security	Műszaki biztonság

The aim of the journal is to publish studies, research reports, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.	A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.
Published quarterly, typically in Hungarian, occasionally in a foreign language. Special and/or thematic issues related to conferences and topics are occasionally published in Hungarian or in foreign languages.	**Megjelenés** negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.
Only those papers will be published which reviewed by two independent reviewers and recommended suitable for publication in the Safety and Security Sciences Review. The submitted manuscripts must meet the requirements both of the form and the content which can be found in the journal's website. Please note: we will not return unapproved manuscripts.	A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.
Articles in the Safety and Security Sciences Review are archived in the Digital Archives of Óbuda University (ÓDA). The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).	A Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek. Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

ISSN 2676-9042
https://biztonsagtudomanyi.szemle.uni-obuda.hu

Editorial office | Szerkesztőség
Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi Doktori Iskola
1081 Budapest, Népszínház utca 8.

Publisher | Kiadó
Óbudai Egyetem, 1034 Budapest, Bécsi út 96/B.

Responsible for publishing | A kiadásért felel
Prof. Dr. KOVÁCS Levente
Rector of the Óbuda University | az Óbudai Egyetem rektora

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 2, 2021. | **2021. III. évf. 2. szám**

Authors of this issue | **E számunk szerzői**

BESZÉDES Bertalan

beszedes.bertalan@uni-obuda.hu

Bertalan BESZÉDES (1988) electrical engineer, mechatronics engineer, currently enriching his knowledge at the Doctoral School of Safety and Security Sciences on University of Óbuda. His field of research is high-reliability hybrid electronic circuits in the field of embedded systems. He is an assistant professor at the Óbuda University, Alba Regia Technical Faculty, Institute of Engineering.

BESZÉDES Bertalan (1988) villamosmérnökmérnök, okleveles mechatronikai mérnök, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit. Kutatási területe a nagy megbízhatóságú hibrid elektronikus áramkörök a beágyazott rendszerek területén. Az Óbudai Egyetem Alba Regia Műszaki Karán a Mérnöki Intézet egyetemi tanársegédje.

BORUZS Hunor

boruzsh@orfk.police.hu

I started my studies at the College of Police Officers and then graduated here as a law enforcement administration organizer. Already at this early point, I wrote my dissertation entitled "Armed Security Guarding in the Private Security Sphere". From 2011, I worked as a guard commander at the Armed Security Guard of the Media Services Support and Asset Management Fund for 5 years. Meanwhile, I continued my studies at the Master's Degree in Defense Administration at the National Civil Service University. I prepared my dissertation entitled "General and special fire protection of media service facilities". In 2017 I was asked to undertake the role of deputy commander of the armed security guard established within the organization of the National Police Headquarters. The guard currently performs object protection, security and escort duties in more than 200 police facilities, with about 2,000 people, and I also participate in the professional supervision of traditional armed security guards. From 2017 I've been holding trainings and lectures on armed security guards, and exams for our colleagues as the chairman of the examination committee.

Tanulmányaimat a Rendőrtiszti Főiskolán kezdtem, majd itt végeztem rendészeti igazgatásszervezőként. Szakdolgozatomat már ezen a korai ponton „A fegyveres biztonsági őrzés a magánbiztonsági szférában" címen készítettem el. 2011-től a Médiaszolgálatatástámogató és Vagyonkezelő Alap fegyveres biztonsági őrségénél 5 évig őrparancsnoki beosztásban dolgoztam. Eközben tanulmányaimat a Nemzeti Közszolgálati Egyetem védelmi igazgatási mesterképzési szakán folytattam. Diplomamunkámat a „Médiaszolgáltató létesítmények általános és speciális tűzvédelme" címen készítettem el. 2017-ben felkérést kaptam, hogy az Országos Rendőr-főkapitányság szervezetén belül létrejött fegyveres biztonsági őrségnél őrségparancsnok-helyettesként dolgozzak tovább. Az őrség jelenleg több mint 200 rendőrségi objektumban, mintegy 2000 fővel lát el objektumvédelmi, valamint személyőrzési- és kísérési feladatokat, valamint részt veszek a tradicionális fegyveres biztonsági őrségek szakmai felügyeletében is. 2017-től oktatásokat, előadásokat tartok a fegyveres biztonsági őrségekről, a vizsgabizottság elnökeként vizsgáztatom a kollegáinkat.

FÁBIÁN Péter

fabianpeter@topcopgroup.com

The author is a police officer, lawyer, criminologist, national security analyst. For many years he worked as a criminal intelligence officer at various police departments. He has been working as a leader in the private security sector for more than 20 years. Private forensic security expert, security consultant for several large multinational corporations. Expert of the PTE Center for Defense Research. He is a doctoral

A szerző rendőrtiszt, jogász, kriminológus, nemzetbiztonsági elemző. Sok évig bűnügyi hírszerzőként dolgozott a Rendőrség különböző szerveinél. Több, mint 20 éve a magánbiztonsági szektorban dolgozik vezetőként. Igazságügyi magánbiztonsági szakértő, több multinacionális nagyvállalat biztonsági tanácsadója. A PTE Védelmi Kutatások Központ szakér-

candidate of the Doctoral School of Security Sciences of the University of Óbuda. His research topic is private security.

tője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorjelöltje. Kutatási témája a magánbiztonság.

FOGARASI Attila

fogarasi.attila@phd.uni-obuda.hu

Attila FOGARASI (1967) is a lawyer, economist, security engineer and coordinator of internal control at the Wigner Physics Research Center. Research field; the interaction between information security standards, recommendations and the General Data Protection Regulation (GDPR). He is currently enriching his knowledge at the Doctoral School of Security Sciences of the University of Óbuda.

FOGARASI Attila (1967) jogász, közgazdász, okleveles biztonságtechnikai mérnök, a Wigner Fizikai Kutatóközpont belső kontroll koordinációs munkatársa. Kutatási területe; az információbiztonsági szabványok, ajánlások és az Általános Adatvédelmi Rendelet (GDPR) kölcsönhatása. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit.

GYÖRÖK György

gyorok.gyorgy@uni-obuda.hu

György GYÖRÖK (1958) electrical engineer. His field of research are the robust electronic solutions, synthesis of systems built from programmable analog circuits and unique applications of microcontrollers and programmable analog circuits. He is a professor at the Óbuda University, dean of Alba Regia Technical Faculty, director of the Institute of Engineering, head of the electrical engineering department.

GYÖRÖK György (1958) okleveles villamosmérnök, kutatási területe a robusztus elektronikai megoldások, a programozható analóg áramkörökből felépített rendszerek szintézise és a mikrokontrollerek és programozható analóg áramkörök egyedi alkalmazásai. Jelenleg az Óbudai Egyetem egyetemi tanára, Alba Regia Műszaki Kar dékánja, a Mérnöki Intézet igazgatója, a villamosmérnök szak felelőse.

HAJDU Beáta

hajdu.bea31@gmail.com

Beáta HAJDU (1977) PhD student at the Doctoral School of Security Sciences, in Óbuda University. His research area is the attitude of the human resources working in the call center, motivation possibilities in the non ewriday environment where working hours are continuously controlled. Title of research topic: Safety conscious behavior under constant control.

HAJDU Beáta (1977) Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási terület: a call centerben/telefonközpontban dolgozó humán erőforrás munkához való hozzáállása, motivációs lehetőségei abban a nem mindennapi környezetben, melyben a folyamatos kontrolláltság jellemzi a munkaidejüket. Kutatandó téma címe: A biztonságtudatos viselkedés folyamatos kontrol alatt.

HETYEI Csaba

hetyei.csaba@uni-obuda.hu

I started my college studies at College of Dunaújváros, where I obtained a bachelor's degree in mechanical engineering in 2013. After the BSc, I attended quality control engineering and mechanical engineering master programs, which I had completed at the University of Dunaújváros. After obtaining my MSc degree, I continued my studies at the Doctoral School on Safety and Security Sciences of the Óbuda University, where with my college and university professor dr. habil. Ferenc Szlivka, who accepted me

Dunaújvárosi Főiskolán kezdtem el főiskolai tanulmányaimat, ahol 2013-ban gépészmérnöki alapdiplomát szereztem. Ezt követően minőségügyi szakmérnöki majd gépészmérnöki mester képzésre járta, amit már a Dunaújvárosi Egyetemen fejeztem be. MSc-s diplomám megszerzése után tanulmányaimat az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytattam, ahol főiskolai és egyetemi tanárom dr. habil. Szlivka Ferenc témavezetésével Szélkerekek egymásra hatásának áramlástani model-

as his PhD student for the Modelling and optimization of the interaction of wind turbines PhD topic. After my BSc studies, I worked as an R&D engineer in an engineering office, then as a product support engineer for CAD and simulation (FEA, CFD) software.

lezése, optimalizálása doktori témával és az ezt kiegészítő tudományterületek megismerésével foglalkozom. BSc-s tanulmányaim után egy mérnökirodában K+F mérnökként dolgoztam, amit idővel a CAD és szimulációs (VEM, CFD) szoftverek terméktámogatása felváltott.

KERTI András

kerti.andras@uni-obuda.hu

I am dr habil András KERTI, an associate professor at the Faculty of Military Science and Officer Training of the University of Public Service. I have been participating in university education since 2006, before that I have performed various info-communication tasks at the units of the Hungarian Armed Forces. I have been involved in the work of the Óbuda University Doctoral School on Safety and Security Sciences since 2016. Research field: "Information security of public service organizations"

Dr. habil KERTI András vagyok, a Nemzeti közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék docense. Az egyetemi oktatásban 2006 óta veszek részt, előtte a Magyar Honvédség alakulatainál láttam el különböző infokommunikációs feladatokat. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola munkájában 2016-óta veszek részt. Kutatási területem: „A közfeladatot ellátószervezetek információbiztonsága”

KISS Csaba

publikacio.kisscsaba@gmail.com

Major Csaba KISS is the chief officer of the Reserve Training and Support Command of the Hungarian Armed Forces. He studied in the Soviet Union at the Ulyanovsk Military Signals University, where he graduated in 1986. In his final year at the university, he graduated as a Russian military interpreter. During his years of service in the Hungarian Army from 1986 to 1996, he completed a Staff Officer course and obtained the “C” type secondary language exam in German, which was extended with his military professions. From 1996 he worked in the Education Directorate of the Hungarian Telecommunications Company (MATÁV) in the Transmission Technology Department of the Technical Department. After obtaining the qualification of a teacher, he taught technical subjects. In addition to technical training, he also obtained a trainer's qualification, so he held various skills development and team building training. During the training, he used his self-developed computer-based skill development program (Octopus-32). In 2010, he won 2nd place with his skills development software in a “smart software” competition announced by the LUDUS project.

KISS Csaba őrnagy a Magyar Honvédség Tartalékképző és Támogató Parancsnokság főtisztje. Tanulmányait a Szovjetunióban végezte az Uljanovszki Katonai Híradó Egyetemen, ahol 1986-ban diplomázott. Az egyetem utolsó évében orosz katonai tolmács diplomát szerzett. 1986-tól 1996-ig a Magyar Hadseregben eltöltött szolgálati évek alatt Törzstiszti tanfolyamot végzett és német nyelvből megszerezte a katonai szakmaival bővített “C” típusú középfokú nyelvvizsgát. 1996-tól dolgozott a Magyar Távközlési Vállalat (MATÁV) Oktatási Igazgatóságán a Műszaki Osztály Átviteltechnikai részlegén. A tanári szakképesítés megszerzése után műszaki tárgyakat tanított. A műszaki oktatások mellett tréneri képesítést is szerzett így különböző készségfejlesztő, csapatépítő tréningeket tartott. A tréningek során használta a saját fejlesztésű számítógépre írt készségfejlesztő programját (Octopus-32). 2010-ben a LUDUS project által meghírdetett “okos szoftver” európai szintű pályázaton a 2. helyezést érte el a készségfejlesztő szoftverével.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Communications engineer, certified communications specialist, head of electronic information security, doctor of economics (PhD), consultant, coach,

Kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora

mediator. His research interests include the social aspects and economic impacts of the digital age, in particular the human dimension of information security, the development of information security awareness, human-robot interaction, smart city, artificial intelligence, and social credit system, domotics. He is an senior research fellow at the Óbuda University, lecturer and supervisor at the National University of Public Service Doctoral School of Military Engineering. He is a registered mediator of the Ministry of Justice, and is an examiner for professional qualification exams. He is a senior consultant, mediator and coach of PREMA Consulting, expert of the Hungarian Military Society and the National Association of Human Professionals. He has been a member of the Artificial Intelligence Consortium since Q4 2018.

(PhD), tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere, a domotika. Az Óbudai Egyetem tudományos főmunkatársa, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, témavezetője. Az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), elnök a szakmai képesítő vizsgákon (OKJ). A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

NAGY Barna

nagy.barna@blx.hu

Msc in Electrical Engineering (Budapest University of Technology and Economics) Engineer-Economist (Corvinus University) Legal studies for engineers (Eötvös Lóránt University) Information Security Engineer (Óbuda University). Certified Ethical Hacker (CEH). At the beginning of his professional career, he worked as a software engineer, software architect and maintenance engineer in the Hungarian telecommunication and financial sectors. He is currently working as a software architect and lead developer for Blumenthal Consulting Kft. He is responsible for the design and development of software products that support industrial safety and maintenance and automatic regulatory compliance. Areas of professional interest and research: implementing information security in the software development, information security issues in embedded systems, language processing (NLP) in legal documents.

Okleveles villamosmérnök (BME-VIK), mérnök-közgazdász (Corvinus Egyetem), jogi szakokleveles mérnök (ELTE-ÁJK), információbiztonsági szakmérnök (Óbudai Egyetem). Etikus hacker (CEH) és szoftvermérnök. Szakmai karrierének elején a magyar telekommunikációs és pénzügyi szektorban nagyvállalati információs rendszerek fejlesztésével, tervezésével és üzemeltetésével foglalkozott. Jelenleg a Blumenthal Consulting Kft szoftver architectje és vezető fejlesztőjeként dolgozik. Iparbiztonsági és karbantartási területeket támogató, illetve az automatikus jogszabályfigyelést megvalósító szoftverek tervezéséért és fejlesztéséért felelős. Szakmai érdeklődési és kutatási területei: információbiztonság megvalósítása a szoftverfejlesztésben, beágyazott rendszerek információbiztonsági kérdései, nyelvfeldolgozás (NLP) jogi környezetben.

NYÁRI Norbert

nyari.norbert@uni-obuda.hu

So far, I have studied mainly in the field of informatics, I have degrees in engineering, teaching and computer science. I have been working as a software developer for more than 10 years at a budgetary institution of the Hungarian public administration. Due to my studies and professional experience, I have extensive knowledge in the fields of application development, information security, and psychology. The aim of my doctoral research is to find tools, methods and solutions for strengthening the information security of the Hungarian public administration.

Eddigi tanulmányaimat alapvetően informatikai területen végeztem, rendelkezem mérnöki, tanári, programtervezői diplomákkal. Több mint 10 éve dolgozom szoftverfejlesztőként a magyar közigazgatás egyik költségvetési szervénél. Tanulmányaimnál és szakmai tapasztalatomnál fogva széleskörű ismeretekkel rendelkezem az alkalmazásfejlesztés, az információbiztonság, valamint a pszichológia területén. Doktori kutatásom célja a magyar közigazgatás információbiztonságának erősítését szolgáló eszközök, módszerek, megoldások felkutatása.

SZAKALI Miklós

mszakali@hotmail.com

Miklós SZAKALI (1963) lieutenant colonel, currently he is serving at the Hungarian Ministry of Defence, as a senior defence planner. His responsibility is the harmonisation of the national and the NATO's capability developments. He is a doctoral candidate of the Óbuda University Doctoral School on Safety and Security Science in Budapest. His field of research is the study of areas and interactions between security and defence planning. It includes new, complex forms of current security challenges and ways and possibilities to prevent and manage them. He also explores the applicability of NATO's defense planning system (and defense planning systems in general) to address the new types of challenges of our time.

SZAKALI Miklós (1963) alezredes, hívatásos katona, jelenleg a Honvédelmi Minisztérium Védelempolitikai Főosztály teljesít szolgálatot, mint védelmi tervező főtiszt. Felelősségi területe a nemzeti és a NATO képességfejlesztési tevékenységek harmonizálása. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit, mint doktorandusz hallgató. Kutatási területe a biztonság és a védelmi tervezés területeinek és kölcsönhatásainak vizsgálata. A napjainkban megjelenő biztonsági kihívások új, komplex formáit és azok megelőzésének és kezelésének lehetőségeit vizsgálja. Kutatja a NATO védelmi tervezési rendszerének (és általában a védelmi tervezési rendszerek) alkalmazhatósági lehetőségeit korunk új típusú kihívásainak kezelésére.

SZLIVKA Ferenc

szlivka.ferenc@bgk.uni-obuda.hu

I graduated in mechanical engineering with fluid dynamic specialization, and I worked within the same discipline during my doctoral studies. Since graduating, I have been researching in the fields of mechanical and agricultural sciences. Currently, I am a PhD supervisor at the Doctoral School on Safety and Security Sciences in Óbuda University, and I am a professor at the University of Dunaújváros and the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University. In addition to education and research, I was involved in founding the Kéményjobbítók Országos Szövetsége (National Association of Chimney Improvers), and the Országos Szélenergia Bizottság (National Wind Energy Commission), and I have been a member of COST MC since 2013.

Gépészmérnök képzést áramlástan szakirányon végeztem el, és ugyanezen a tudományágon belül tevékenykedtem doktori tanulmányaim alatt. Fokozatszerzésem óta a gépészeti és az agrárműszaki tudományokterületeken kutatok. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában vagyok témavezető, a Dunaújvárosi Egyetemen és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki karon egyetemi tanárként oktatok. Oktatás és kutatás mellett részt vettem a Kéményjobbítók Országos Szövetsége és az Országos Szélenergia Bizottság megalapításában, illetve 2013-óta COST MC tagja vagyok.

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Endre SZŰCS (1963) has a PhD degree in military science, graduate engineer on security technology, mechanical engineer and engineering teacher. He is currently a lecturer at the Óbuda University Doctoral School on Safety and Security Science in Budapest. His main subjects are history and the key events of security technology. He also gives lectures at the Donát Bánki Faculty of Mechanical and Security Engineering of the University of Óbuda, Institute of Mechanical and Security Sciences. His field of research: Possibilities of using renewable energy

SZŰCS Endre (1963) a hadtudomány PhD fokozatosa, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető, A biztonságtechnika történetének, eseményeinek áttekintése, elemzése című tantárgyat oktatja, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet óradója. Kutatási területe: A megújuló

sources in security technology. Exploring the milestones in the development of security technology.

energiaforrások alkalmazásának lehetőségei a biztonságtechnikában. A biztonságtechnika történetének vizsgálata.

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 3, No 2, 2021. | **2021. III. évf. 2. szám**

CONTENT | TARTALOM

DEVELOPMENT AND INTEGRATION OF MANAGEMENT SYSTEM STANDARDS

A SZABVÁNYOS IRÁNYÍTÁSI RENDSZEREK FEJLŐDÉSE, INTEGRÁCIÓJA

FOGARASI Attila[1] – SZŰCS Endre[2]

Abstract

The article presents the development of standard management systems, the essential elements of the most important management systems, emphasizing the importance of HLS standards. HLS (HLS = high level structure) standards have the same structure and contain many of the same concepts and definitions. The article analyzes new ways of standardization, its connection to the development of the legal system through the relationship between the certification system supported by the General Data Protection Regulation (GDPR) and the development of international standardization.

Keywords

management system standards, quality management, occupational health and safety, information security, General Data Protection Regulation

Absztrakt

A cikk bemutatja a szabványos irányítási rendszerek kialakulását, a legfontosabb irányítási rendszerek lényeges elemeit. Kiemeli az ún. HLS rendszerű szabványok jelentőségét. A magas szintű szerkezet szabványok (high level strukture, a továbbiakban: HLS) azonos felépítésűek, és sok azonos fogalmat és meghatározást tartalmaznak. A cikk elemzi a szabványosítás új útjait, kapcsolódását a jogrendszer fejlődéséhez az általános adatvédelmi rendelet (GDPR) által támogatott tanúsítási rendszer és a nemzetközi szabványosítás fejlődésének kapcsolatán keresztül.

Kulcsszavak

irányítási rendszer szabványok, minőségirányítás, munkahelyi egészség és biztonság, információbiztonság, általános adatvédelmi rendelet

[1] fogarasi.attila@phd.uni-obuda.hu | ORCID: 0000-0002-1585-7301 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | senior lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

A NEMZETKÖZI SZABVÁNYOSÍTÁS FEJLŐDÉSE

A termelési folyamatok összetettebbé válása, a termelésen belüli munkamegosztás, a munkafeladatok egymásutánisága már a társadalmi fejlődés korai szakaszában is megkövetelte a munkafolyamatokra vonatkozó szabályok rögzítését. A kontinuensen alkalmazott normák eleinte a termelői csoportokon belül validáltan jöttek létre. Amikor a termelési folyamatok a kis közösségeken túlnőttek, interkommunálissá váltak, különösen fontossá vált a normák globalizálódása. A megtermelt javak cserekereskedelmével megszületett az igény a szabályok általánossá tételére is.

Az egyik közösségen belüli termelési folyamat végterméke egy másik közösség termelési folyamatának nyersanyagává vált. Egy ilyen összetett folyamat csak az adott termékre vonatkozó normák összehangolása útján volt kezelhető eredményesen. A fejlődés eredményeként megjelentek az akkor még partikuláris hosszmértékek, súlymértékek, időmértékek. Később, az ipari forradalom, a tömegtermelés már elképzelhetetlen volt a részletes technológiai szabályok, szabványok alkalmazása nélkül.

A világ első nemzeti szabványügyi testülete Angliában, Mérnöki Szabványügyi Bizottság néven jött létre. A testületet Sir John Wolfe-Barry, a londoni Tower Bridge tervezője alapította, 1901-ben. Az intézet 1931-ben vette fel a mai nevét (British Standards Institution, a továbbiakban: BSI). [1]

A szabványosítás nemzetközi szervezetei közül először a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, a továbbiakban: IEC) alakult meg 1906-ban. A megalakulás előzménye az 1904-ben rendezett St. Louis-i világkiállításra datálható. A kiállításon ugyanis rendkívüli sikert aratott a „Villamos Palota", bár a kiállítók számtalan különböző feszültségű egyenáramú, 1-, 2-, 3 fázisú váltóáramú villamos rendszert alkalmaztak, a legkülönfélébb csatlakozókkal, dugaszokkal. A kiállítással párhuzamosan megrendezett tanácskozáson éppen ezért vetődött föl az ötlet egy állandó nemzetközi bizottság felállítására, amelynek feladata az elektromos készülékek és gépek minősítési feltételeinek és méréseinek meghatározása, egységesítése.

Az akkori tárgyalások eredményeként alapították meg Londonban az IEC-t, amely 1906. június 26–27-én tartotta első ülését a Hotel Cecilben, Alexander Siemens (A Siemens céget alapító Werner Siemens unokatestvére) elnökletével. Az alapító országok – Belgium, Kanada, Franciaország, Németország, Nagy-Britannia, Holland, Svájc, Spanyolország, Japán és az Egyesült Államok – között ott volt Ausztria-Magyarország is. Így hazánk már a szabványosítás hajnalán, az első országok között csatlakozott az új kezdeményezéshez.

A testület első titkára Charles Le Maistre lett, aki olyan megbeszéléssorozatot kezdeményezett, melynek köszönhetően 1926-ban megalapították a Nemzeti Szabványosító Egyesületek Nemzetközi Szövetségét (International Federation of the National Standardizing Associations a továbbiakban: ISA). A világháború után az ISA megszűnt és helyét az 1947-ben megalakult, Nemzetközi Szabványügyi Szervezet (Intarnational Standard Organisation a továbbiakban: ISO) vette át. [2] A nemzetközi szervezet megalapítása érdekében kifejtett munkásságáért, sokan Le Maistre-t tekintik a nemzetközi szabványosítás atyjának. [3]

A nemzetközi szabványügyi szervezetek megerősödésével párhuzamosan megszülettek a kisebb-nagyobb regionális szabványügyi szervezetek is, többek között az Európai Szabványügyi Bizottság (Comité Européen de Normalisation a továbbiakban: CEN) - 1975,

az Európai Elektrotechnikai Szabványügyi Bizottság (European Committee for Electrotechnical Standardization a továbbiakban: CENELEC) – 1973, illetve az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute a továbiakban: ETSI) 1988.

A kormányoktól független ISO-nak jelenleg 165 nemzeti szabványügyi testület a tagja. Az ISO központi titkárságának székhelye Genfben található. Az ISO működési elve azon alapszik, hogy tagjai segítségével szakértőket von be, akik megosztják egymással ismereteiket, és olyan önkéntes, konszenzuson alapuló, piaci szempontból releváns nemzetközi szabványokat dolgozzanak ki, amelyek támogatják az innovációt és megoldásokat kínálnak a globális kihívásokra [4].

A HAZAI SZABVÁNYOSÍTÁS RÖVID TÖRTÉNETE

A kiegyezést követő fellendülés, az építőipar rohamos fejlődése és az akkor korszerű építészeti módszerek, anyagok megjelenése következtében az építőanyagok szabványosítását 1875-ben kezdte el Magyar Mérnök- és Építészegylet, Ybl Miklós irányításával. Munkájuk eredményeként vált nyilvánvalóvá, hogy a szabványosítás intézményesített rendszerére is szükség lesz.

Az egész világon a legelsők között alakult meg 1921-ben hazánkban a szabványosítás első hivatalos szervezete, a Magyar Ipari Szabványosító Bizottság, amelynek alelnöki tisztségét Kandó Kálmán töltötte be. 1933-tól kezdett el működni a Magyar Szabványügyi Intézet. 1948-ban a Magyar Szabványügyi Intézetet államosították, és 1951-ben létrehozták a Magyar Szabványügyi Hivatalt, amely elvesztette függetlenségét és a közigazgatás részeként, hivatalként működött tovább. A független intézményi státusz kétségtelen előnyeit nem feledve, meg kell állapítanunk, hogy az állami intézményrendszerbe tagozódásnak is voltak előnyei. A hatósági jogkör lehetővé tette, hogy 1995-ig a szabványok betartása Magyarországon kötelező legyen.

Magyarország európai integrációjának részeként vállalt kötelezettsége volt a szabványosítás autonómiájának helyre állítása. A magyar szabványosítás rendszerét a nemzeti szabványosításról szóló 1995. évi XXVIII. törvény formálta át ismét, amely tulajdonképpen visszaállította a szabványosítás klasszikus alapelveit. Fontos sarokpontja lett az új szabályozásnak, hogy a szabványosítás nem kormányzati feladat. A törvény értelmében a korábbi Magyar Szabványügyi Hivatal (a továbbiakban MSZH) megszűnt és megalakult a Magyar Szabványügyi Testület (a továbbiakban: MSZT), mint Magyarország nemzeti szabványügyi szervezete.

A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény 4. § (1) bekezdése – máig ható érvénnyel – rögzítette a szabvány fogalmát is:

„A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely tevékenységre vagy azok eredményére vonatkozik, és olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amelyek alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb.” [5]

A JELENTŐS IRÁNYÍTÁSI RENDSZEREK A JELENLEG HATÁLYOS SZABVÁNYOK TÜKRÉBEN

A szabványosítás mára túlnőtt az ipari termelés, a szűken vett technológiai folyamatok paramétereinek meghatározásán. Jelenleg 21.584 db. ISO szabvány van érvényben.

A szabványok nemcsak számosságukban váltak meghatározóvá, de megjelentek a komplex rendszerek, szervezetek irányítását meghatározó ún. „menedzsment irányítási rendszerek" (*Management System Standards, a továbbiakban: MSS*) szabványai is. Ez a szabványosítási terület az, ami a technológiai fejlődés társadalmi hatásainak leggyorsabban változó tükre, a fejlődés értékmérője. Az ISO jelenleg több mint 80 ilyen szabványt tart nyilván [6] (a*z MSS szabványok teljeskörű listáját az 1. számú melléklet tartalmazza*).

Az irányítási rendszerek egy része ún. HLS szabvány. A HLS szabványok azonos felépítésűek, és sok azonos fogalmat és meghatározást tartalmaznak. Ez különösen hasznos azon szervezeteknek, amelyek úgy döntenek, hogy egyetlen „integrált" irányítási rendszert működtetnek, amely egyidejűleg képes megfelelni két vagy több irányítási rendszer szabvány követelményeinek.

- A szervezetirányításban jelenleg az alábbi, egyébként ún. HLS típusú irányítási rendszer szabványok a legáltalánosabbak:
- Minőségirányítási rendszer (továbbiakban: MIR) – *MSZ EN ISO 9001:2015*
- Környezetközpontú irányítási rendszer (továbbiakban: KIR) – *MSZ EN ISO 14001:2015*
- A munkahelyi egészségvédelem és biztonság irányítási rendszere (továbbiakban: MEBIR) – *MSZ ISO 45001:2018*
- Információbiztonsági irányítási rendszer (továbbiakban: IBIR) – *MSZ ISO/IEC 27001:2014*

„Az ISO 9001 minőségirányítási, az ISO 14001 környezetirányítási és az ISO 27001 információbiztonsági szabványok közös jellemzője a folyamatközpontúság. Mindegyik az ISO 9001 felépítését követi. A szabványok végén található mellékletek a tartalomjegyzékek pontjait követve ezt a kapcsolatot részletesen bemutatják. A szabványalkotók egyik célja az volt, hogy a szabványok –a többszörös szabályozást elkerülve -integráltan is bevezethetők legyenek. A kialakított integrált irányítási rendszer „egyszeres" auditálása is megoldható." [7]

Célunk a szervezetirányítás ezen meghatározó szabványainak, illetve azok egymáshoz kapcsolódásának elemzése.

MINŐSÉGIRÁNYÍTÁSI RENDSZER: ISO 9001-ES SZABVÁNY

A minőségirányítási ISO 9001 szabvány talán legfontosabb újdonsága a működés folyamatalapú megismerése, feltérképezése, a működés folyamatokon keresztüli megértése volt. A szabvány 1987 márciusában jelent meg. Hazánkban az első kiadása MSZ EN 9001:1992 néven, 1992-ben történt.

„Ez a nemzetközi szabvány a minőségirányítási rendszer kialakítása, bevezetése, valamint eredményességének és hatékonyságának fejlesztése során a folyamatszemléletű megközelítés alkalmazását segíti elő. Egy szervezeten belül a folyamatok egy rendszerének alkalmazása, e folyamatok meghatározásával, kölcsönhatásaival és irányításukkal együtt „folyamatszemléletű megközelítés"-nek tekinthető…

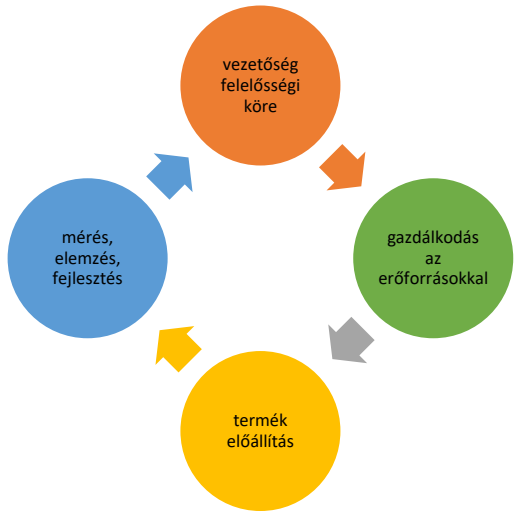
A folyamatszemléletű megközelítés egyik előnye az, hogy gondoskodik a rendszeren belül az egyes folyamatok közötti kapcsolatnak, továbbá a folyamatok kombinációjának és kölcsönhatásának folyamatos szabályozásáról." [8]

Ha ezt a megközelítést egy minőségirányítási rendszerben alkalmazzák, akkor ez kiemeli a következő szempontok fontosságát:

a) a követelmények megértése és teljesítése,
b) a folyamatok átgondolásának szükségessége a hozzáadott érték szempontjából,
c) a folyamat működésére és eredményességére vonatkozó adatok megismerése, valamint
d) a folyamatok folyamatos fejlesztése, objektív mérések alapján.

Az ISO 9001 szabvány bevezette azt a módszert, hogy minden folyamatot ún. Tervezés-Végrehajtás-Ellenőrzés-Intézkedés (Plan-Do-Check-Act, a továbbiakban PDCA) ciklusokban paraméterezünk. A szabvány röviden meghatározza a PDCA ciklus (1. ábra) elemeinek tartalmát is:

- **Plan**: (tervezés): azoknak a céloknak és folyamatoknak a megállapítása, amelyek a vevői követelményeknek és a szervezet politikájának megfelelő eredmények eléréséhez szükségesek;
- **Do**: (végrehajtás): a folyamatok bevezetése;
- **Check**: (ellenőrzés): a folyamatok és a termékek figyelemmel kísérése és összehasonlítása a politikával, a célokkal és a termékre vonatkozó követelményekkel, valamint az eredmények bemutatása;
- **Act**: (intézkedés): intézkedések megtétele a folyamat működésének folyamatos fejlesztésére. [8]



1. ábra PDCA ciklus az ISO 9001 szabvány szerint [8], saját szerkesztés

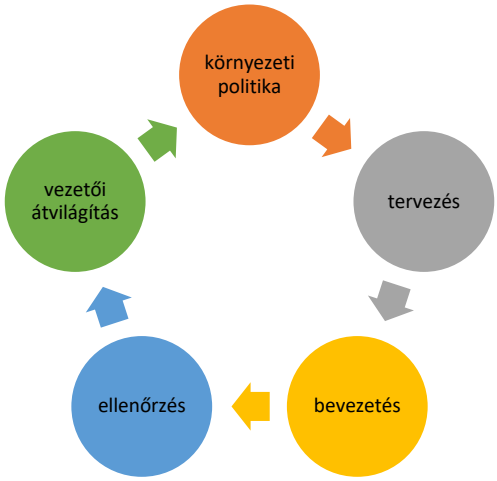
Az ISO 9001 ún. HLS szabvány, azaz meghatározásai, fogalmai a többi HLS szabvánnyal összeegyeztetettek.

KÖRNYEZETIRÁNYÍTÁSI RENDSZER (KIR): ISO 14001-ES SZABVÁNY

A KIR egy nagyon érdekes szabvány. Sokkal kevésbé egzakt követelményeket határoz meg, mint az ISO 9001, bár HLS szabványként a két szabvány alkalmas a szervezet irányítási rendszerének integrált kialakítására.

Magát az ISO 14001 szabványt a Nemzetközi Szabványügyi Szervezet 1996 szeptemberében adta ki először. A szabvány (*MSZ EN ISO 14001:1997*) már a következő évben, 1997-ben megjelent a Magyar Szabványügyi Testület gondozásában.

A szabvány deklarálja szoros kapcsolatát az ISO 9001 szabvánnyal. Átveszi, bár kissé módosítva a PDCA modellt is (*2. ábra*).



2. ábra PDCA modell az ISO 14001 szabvány szerint [9], saját szerkesztés

Az ISO 14001 szabvány nem tartalmaz abszolút követelményeket. Azt várja el a szervezettől, hogy legyen elkötelezett a jogszabályok maradéktalan betartásában. Vállalja a környezetvédelmi rendszerének folyamatos fejlesztését, illetve azt, hogy törekszik a környezetszennyezés minden formájának megelőzésére. Ez a megengedő szemlélet azt is lehetővé teszi, hogy két hasonló szervezet akkor is megfeleljen a szabványnak, ha környezetvédelmi teljesítményük színvonala egymástól lényegesen eltér.

Hangsúlyos eleme a szabványnak, hogy meghatároz néhány nagyon fontos környezet irányítási fogalmat. (*ISO 14001:2005*)

*„**Környezet**: A szervezet közvetlen környezete, amelyben az működik, beleértve a levegőt, a vizet, a földterületet, a természeti erőforrásokat, a növény és állatvilágot, az embereket és ezek kölcsönös kapcsolatait.*

***Környezeti tényező**: Valamely szervezet tevékenységének, termékeinek vagy szolgáltatásainak olyan eleme, amely kölcsönhatásba kerülhet a környezettel.*

***Környezeti teljesítmény**: Egy szervezet irányításának mérhető eredményei, a környezeti tényezők tekintetében.*

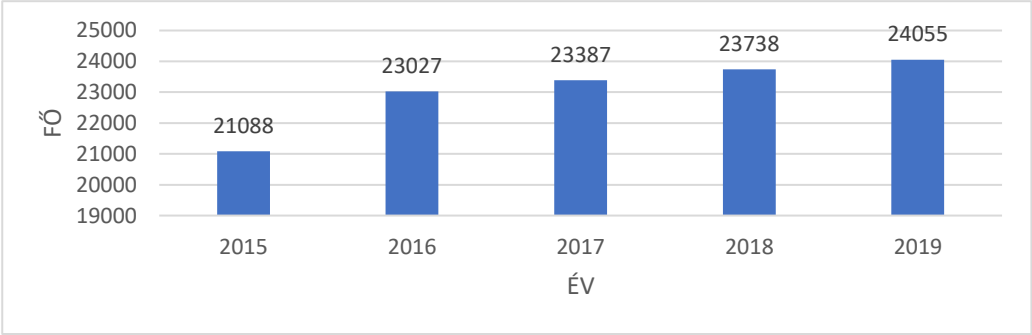
***Környezeti politika**: Egy szervezet környezeti teljesítményére vonatkozó általános szándékei és irányvonalai, ahogyan azt a vezetőség hivatalosan megfogalmazta.*

***Környezetközpontú irányítási rendszer (továbbiakban: KIR)**: Egy szervezet irányítási rendszerének aza része, amelynek az a szerepe, hogy kialakítsa és bevezesse környezeti politikáját és kezelje környezeti tényezőit."* [9]

A szabvány annak ellenére, hogy nem fogalmaz meg konkrét környezeti kritériumokat, maga a tanusítási folyamat, illetve a szabványból következő permanens fejlesztési igény arra sarkalja a szervezetet, hogy környezet terhelését folyamatosan optimalizálja.

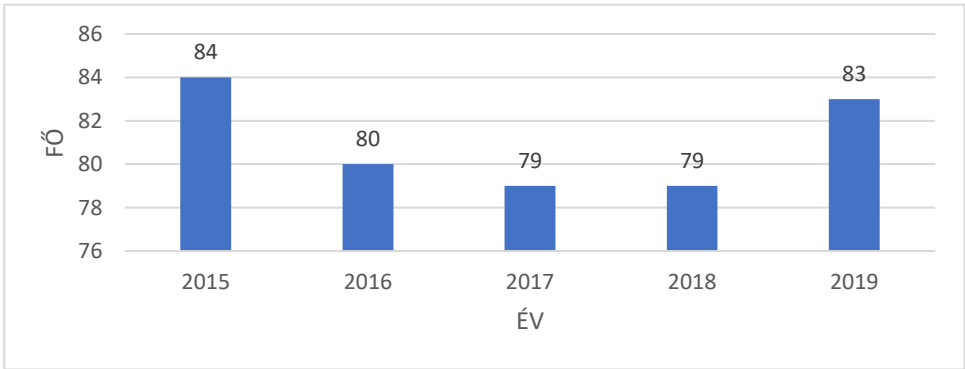
A MUNKAHELYI EGÉSZSÉGVÉDELEM ÉS BIZTONSÁG IRÁNYÍTÁSI RENDSZERE (MEBIR): ISO 45001

Évente sok ezer ember hal meg munkabalesetek, foglalkozási betegségek következtében. A sérülések, nem halálos megbetegedések száma pedig szinte felbecsülhetetlen. Az ENSZ szakosított szervezetének, a Nemzetközi Munkaügyi Szervezetetének (International Labour Organisation a továbbiakban: ILO) 2010. évi statisztikája szerint, az adatszolgáltató 56 országban több, mint 6 millió munkabaleset történt. Magyarország 2015-2019 közötti munkabaleseti statisztikája (*3. ábra*) szerint az éves munkabalesetek húszezer fő körüli létszámot érintenek.



3. ábra Az összes munkabaleset száma Magyarországon 2015-2019 [10], saját szerkesztés

Látható, hogy hazánkban évente egy közepes város lakosságát elérő számú munkavállalót ér munkabaleset, és közel száz ember hal meg munkabaleset következtében (*4. ábra*).



4. ábra Összes halálos munkabalesetek száma Magyarországon 2015-2019 [10], saját szerkesztés

A nemzetközi és a hazai szabványügyi szakemberek éppen ezért nagy fontosságot tulajdonítottak annak, hogy olyan szabványt fejlesszenek, amely évente csaknem hárommillió életet menthetnek meg és a HLS rendszerbe igazodván, a többi ISO-menedzsment rendszerhez hasonló módon felépítésüknek köszönhetően integrálhatóvá váljanak az olyan szabványokhoz, mint az ISO 14001 vagy az ISO 9001.

A BSI már az 1990-es években, a Nemzetközi Munkahelyi Egészségvédelmi és Biztonsági Értékelő Sorozat projektcsoport tagjaként kidolgozta és kiadta az első munkavédelmi és munkahelyi egészségvédelmi szabványát (*Occupational Health and Safety Assessment Series, a továbbiakban: OHSAS*) a BS OHSAS 18001 jelű szabványt. A szabványt 2007-ben megújították. Integrálták az ENSZ szakosított szervezetének, az ILO-nak az irányelveit és a munkabiztonság mellett egyre nagyobb hangsúlyt kapott a munkahelyi egészségvédelem. Ezt a brit szabványt emelte át a Magyar Szabványügyi Testület az MSZ 28001 jelű szabványba 2008-ban.

Az ISO csak 2018-ban hirdette ki az OHSAS szabványt, ISO 45001 címen. Az új számozást a BSI és a Magyar Szabványügyi Testület is átvette. A most hatályos számozás: MSZ ISO 45001:2018.

Érdekesség, hogy az ISO azért nem használhatta a BSI jól bevált 18001-es sorozatszámát, mert az már foglalt volt, ISO 18001:2004 néven a *rádiófrekvenciás azonosítás* témakörében érvényes szabvánnyal rendelkezett, így a brit szabványt az új, 45001 sorszámon hirdették ki. Magyarországon szintén foglalt volt a 18001-es sorszám (*MSZ 18001:1986 Gumi védősapka közúti járművek hidraulikus dobfékének nem ásványolajbázisú fékfolyadékkal működtetett kerékfékhengereihez 120 °C üzemi hőmérsékletig),*így nálunk eredetileg a szabvány a 28001-es sorszámot kaphatta csak meg. Szerencsére ma már mindenki az egységes, 45001-es sorszámot használja (*Egyébként megjegyezzük, hogy MSZ EN 45001:1990 Vizsgálólaboratóriumok működésének általános feltételei címen európai és magyar szabvány is volt már kihirdetve, amit időközben visszavontak…*)

A szabvány fontos eleme, hogy a szervezet képes legyen más érdekelt felek (munkavállalók, szerződéses partnerek, hatóságok) elvárásainak felismerésére. Fontos, hogy meghatározzák a tevékenységükben rejlő kockázati tényezőket és megoldásokat adjanak azok kezelésére. Mindez nem valósulhat meg a felső vezetés elköteleződése nélkül, ha nem vesz aktívan részt a szereplők elszámoltatásában, a folyamatok felmérésében.

INFORMÁCIÓBIZTONSÁGI IRÁNYÍTÁSI RENDSZER (IBIR): ISO 27001

Az informatikai rendszerek egyszerre szolgálják és veszélyeztethetik cégek, szervezetek, közösségek működését. Az új szolgáltatások, felhőalapú megoldások, mesterséges intelligencia, okosvárosok, IT támogatású, automatizált döntéshozatali folyamatok megjelenése, rohamos terjedése újszerű kockázatokkal jár. A korábban megszokottnál jóval több figyelmet kell fordítani az informatikai biztonságra.

„ *2017 végén világszerte mintegy 3,8 milliárd internetfelhasználó volt, szemben a 2015-ös 2 milliárddal. A Cybersecurity Ventures úgy becsüli, hogy 2022-ra 6 milliárd internetező lesz (amely az addigra 8 milliárdra gyarapodó népesség 75%-a), 2030-ra pedig a számuk eléri a 7,5 milliárdot is (amely a jósolt 8,5 milliárdos lakosság 90%-a).*

2016-ban minden 39. másodpercre jutott egy hekkertámadás. A személyes adatok megszerzésére irányult sikeres támadások 95%-a három területre összpontosult: a

kormányzatra, továbbá a kereskedelmi és technológiai cégekre. 2016-ban a cégek 64%-a szenvedett el webalapú támadásokat, melyek 43%-a főként kisvállalkozásokra összpontosult. Tavaly összesen egymilliárd személyes profilt sikerült feltörni.
A Cybersecurity Ventures 2017-es jelentése szerint 2015-ben 3 milliárd dollár volt a kiberbűnözés okozta károk mértéke, és ez az összeg 2021-re meg fog duplázódni. A védekezésre költött összeg pedig öt éven belül el fogja érni az 1 milliárd dollárt." [11]

Nagyságrendben csak a kiberbűnözés okozta kár eléri Magyarország éves költségvetését. És akkor még nem is beszéltünk a látens, lappangó cselekményekről, illetve a bűnözés okozta erkölcsi, pénzben ki nem fejezhető károkról.

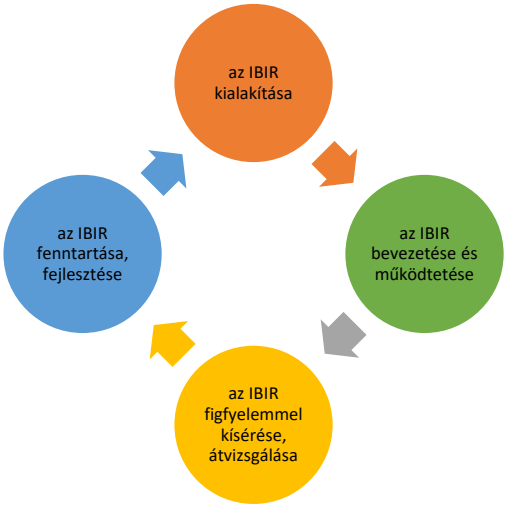
A szervezetek élete, működése ma már elképzelhetetlen informatikai rendszerek használata nélkül. Sőt az egyes jogi és szociológiai szempontból autonóm szereplők az IT rendszereiket, az internet közvetítésével, egymással összekapcsolva használják. Az így kialakuló nagyrendszrek működtetése megteremtette az illeszkedést segítő technológiai és irányítási szabványok kialakulásának szükségességét.

Az információbiztonság általánosan elfogadott irányítási rendszre az ISO 27001 szabvány lett. 2005 októberében jelent meg az első nemzetközi információbiztonsági irányítási rendszerre vonatkozó szabvány az ISO 27001:2005.

Az ISO / IEC 27001: 2005 minden típusú szervezetre kiterjedt. Alkalmas arra, hogy üzleti vállalkozások, kormányzati szervek, nonprofit szervezetek is bevezethessék. Az ISO / IEC 27001 szabvány szintén ún. HLS szabvány, így az ISO 9001 szabvánnyal összhangban meghatározza a dokumentált információbiztonsági irányítási rendszer létrehozásának, végrehajtásának, működtetésének, megfigyelésének, felülvizsgálatának, karbantartásának és fejlesztésének követelményeit. Fontos eleme a folyamatok feltérképezése, az azokban rejlő kockázatok felmérése és kezelése. Meghatározza az egyes szervezetek vagy azok részeinek biztonsági ellenőrzéseinek végrehajtási követelményeit is.

Az ISO 9001 szabványból örökölten az ISO 27001 szabvány is megalkotja a fejlesztésnek a PDCA cikluson keresztüli megvalósításoi modelljét (*5. ábra*) [12]

Tervezés (PLAN) (az IBIR kialakítása)	**Olyan IBIR-politika, -célok, -folyamatok és -eljárások kialakítása, amelyek lényegesek annak érdekében, hogy a kockázat kezelése és az információbiztonság fejlesztése a szervezet általános politikájával és céljaival összhangban lévő eredményeket tudjon felmutatni.**
Végrehajtás (DO) (az IBIR bevezetése és működtetése)	Az IBIR-politika, -intézkedések, -folyamatok és eljárások bevezetése és működtetése.
Ellenőrzés (CHECK) (az IBIR figyelemmel kísérése és átvizsgálása)	A folyamatok teljesítményének értékelése, és ahol lehetséges, mérése az IBIR-politikával, -célokkal és gyakorlati tapasztalatokkal összevetve, továbbá az eredmények jelentése a vezetésnek átvizsgálás céljából.
Beavatkozás (ACT) (az IBIR fenntartása és fejlesztése)	Helyesbítő és megelőző tevékenységek végrehajtása a belső IBIR-átvizsgálás (audit) és vezetőségi átvizsgálás eredményei, illetve egyéb lényeges információk alapján az IBIR folyamatos fejlesztése érdekében.



5. ábra A PDCA-modell az Információbiztonsági Irányítási Rendszer (IBIR)-folyamatokra alkalmazva [12], saját szerkesztés

ISO 27001:2005

„ ***Rendelkezésre állás (availability):*** *Olyan tulajdonság, amely lehetővé teszi, hogy az adott objektum, feljogosított entitás által támasztott igény alapján, hozzáférhető és igénybe vehető legyen.*

Bizalmasság, titkosság (confidentiality): *Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására.*

Sértetlenség (integrity): *A vagyontárgyak pontosságának és teljességének védelmét biztosító tulajdonság.„* [12]

Az információbiztonság éppen ezen pillérek védelme, megőrzése.

Az információbiztonság (information security) fogalma: Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése. Az információbiztonság fogalmi pillérei mellett, ezek a kiegészítő egyéb jellemzők is meghatározzák az információ biztonságát. Ilyen kategória többek között az információhoz hozzáférő azonosíthatóságát és az információ megváltoztathatatlanságát is biztosító hitelesség, számonkérhetőség, megbízhatóság is.

Az információbiztonsági irányítási rendszer (information security management system: továbbiakban: ISMS) az információbiztonságot szolgáló és „szavatoló” minőségirányítási szabvány. A rendszer, ahogy ezt az erről szóló MSZ ISO/IEC 27001 szabvány is rögzíti, az átfogó irányítási rendszernek az a része, amely egy, a működési kockázatokat figyelembe vevő megközelítésen alapulva kialakítja, bevezeti, működteti, figyeli, átvizsgálja, fenntartja és fejleszti az információvédelmet. [12]

A szabvány nagy előnye, hogy a mellékletében szinte sorvezetőt, check listát ad a szabványt bevezetni szándékozó kezébe, hogy elősegítse a megfelelésre felkészülést.
A szabályozás fő céljai és területei:

- A biztonsági szabályzat, politika kidolgozása.
- Az információbiztonság szervezetének meghatározása.
- A vagyontárgyak osztályozása, a felelősség meghatározása.
- Az emberi erőforrás biztonsága.
- A fizikai védelem kérdései.
- Kommunikációs, üzemeltetés irányítási feladatok meghatározása.
- Hozzáférés ellenőrzés.
- Az IT rendszerek biztonsági követelményei.
- Az információbiztonsági események kezelése.
- Az IT rendszerek üzletfolytonos működtetése.
- Compliance tevékenység szabályozása.

Mint a fenti listából látható, a szabvány nagyon alaposan és széles körben felméri, elemzi és értékeli a szervezet működési folyamatait.

2016. április 27-én megszületett a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet – GDPR). A rendelet az Európai Unió tagállamaiban a 2018. május 25-től kell alkalmazni.

A GDPR alaposan megmozgatta az unió lakosainak, információbiztonsággal foglalkozó szakértőinek életét, gondolkodását. A rendelet ugyan „csak" a polgárok személyes adatainak kezelésével kapcsolatban határoz meg kötelező szabályokat, ám a rendkívül magas bírságoktól való félelem a szervezet alkalmazkodási hajlandóságát jelentősen felerősítette. Sorra születtek az adatvédelmi tájékoztatások, információbiztonsági szabályzatok.

A GDPR 42. cikke foglalkozik a tanúsítás kérdésével. Az (1) bekezdés szerint:
*„A tagállamok, a felügyeleti hatóságok, a Testület, valamint a Bizottság – különösen uniós szinten – **ösztönzik olyan adatvédelmi tanúsítási mechanizmusok**, valamint adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek e rendelet előírásainak."*

Az ISO nem titkoltan annak érdekében, hogy a 42. cikk szerinti tanusítást elősegítse, azon szervezetek számára, akik már rendelkeznek ISO 27001 tanusítással, 2019 augusztusában kiadta az ISO/IEC-27701:2019-et (Privacy Information Management Systems a továbbiakban: PIMS) szabványt. A szabvány a szervezeten belül meghatározza a személyes adatvédelemi irányítási rendszer létrehozásának, fenntartásának szabványos követelményrendszerét. A GDPR alapelvi keretrendszerét konkrét kontrollokra és megoldásokra fordítja le.

A GDPR előírásokat tartalmaz arra nézve is, hogy olyan technikai intézkedéseket kell bevezetni és fenntartani, ami alkalmas arra, hogy az adatvédelmi incidenseket megelőzze. Azonban a rendelet nem nyújt támaszt a jogalkalmazónak ahhoz, hogy mik lehetnek ezek a technika mai állása szerint elfogadható védelmi intézkedések, melyek bevezetését a jogalkotó elvárja. Az ISO 27701 szabvány e területen is nyújt IT technológiai kapaszkodót a szervezetek számára.

„A Microsoft az EU-s GDPR-jogok globális kiterjesztése iránti elköteleződésének következő lépéseként a Microsoft Azure és az Office 365 szoftvereiben is megvalósítja a PIMS-et (személyes adatok védelmének irányítási rendszerét) és támogatja ügyfeleit és partnereit ezen interoperabilitási modell alkalmazásában." [11]

ÖSSZEGZÉS

Megállapíthatjuk, hogy a szabványosítás az eltelt több, mint száz éves történelme során nagy utat járt be. Az ipari fejlődés, a globalizáció, a nemzetközi termelési együttműködés már el sem képzelhető a jól működő nemzetközi szabványügyi együttműködés és a nemzetközi szabványok nélkül.

A szabványosítás magasabb szintjén jöttek létre az első irányítási rendszer szabványok. Ezen szabványok már nem csak az ipari termelés szervezetttségét, koordinációját segítették elő, de más szervezetek számára is kinyitották az együttműködés kapuit nemzeti és nemzetközi szinten is.

Létrejöttek a HLS szabványok, ahol már nem csak a szervezetek együttműködését segítették elő a szabványok, de a szabványok egymás közötti „együttműködése", egymásra épülése is magvalósult. Így egy megszerzett tanusítás a következő előszobája lehet, ezzel is promotálva a vezetői és szervezeti elköteleződést a szabványok mellett.

A GDPR rendelet megjelenése újabb mérföldkőhöz vezetett a szabványosítás történetében. A szabványosítás igénye már elszakad a termelési folyamatoktól. A GDPR egy kísérlet a személyes adatok védelmét szolgáló, országközi jogi szabályozás megteremtésére, oly módon, hogy a strikt jogi norma alkalmazkodni tudjon az egymástól redikálisan eltérő nemzeti jogrendszerekhez. Az egyszerű alkalmazkodás helyett a normakultúrába beépülés, a társadalmi értékrend formálása, a folyamatok önszabályozóvá válása is a célok között volt.

Ilyen rugalmas, önszabályozó rendszerek kialakításában nyugodtan hagyatkozhatunk a nemzetközi szabványosítás százéves hagyományaira, építhetünk sikereire. Ezért is várta a szakmai közönség az új nemzetközi szabvány megjelenését, ami az általános információbiztonsági szabványra ráépülve biztosítja a GDPR megfelelést. A szabvány elterjedése nagy segítség lesz a szervezetek gördülékeny együttműködése és egyidejűleg a rendeletnek megfelelés elérése területén.

IRODALOMJEGYZÉK

[1] British Standards Institution (BSI), „BSI; Our history," 2021.
[2] Nemzetközi Elektrotechnikai Bizottság (IEC), „IEC History," 2021.
[3] Kuert, Willy, FRIENDSHIP AMONG EQUALS (Recollections from ISO's first fifty years), Genf, Svájc, 1997, p. 16.
[4] Nemzetközi Szabványügyi Szervezet (ISO), „ISO About Us," 2021.
[5] A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény, 1995.
[6] Nemzetközi Szabványügyi Szervezet (ISO), „https://www.iso.org/management-system-standards-list.html," 2021.
[7] Michelberger Pál, Vállalkozásfejlesztés a XXI. században III. / Vállalatbiztonság pp. 35-52., D. N. I. Zoltán, Szerk., Budapest: Óbudai Egyetem, 2013, pp. 35-52.
[8] MSZ EN ISO 9001:2001, 2001.

[9] MSZ EN ISO 14001:2005, 2005.
[10] Innovációs és Technológiai Minisztérium Munkavédelmi Főosztály, „TÁJÉKOZTATÓ A MUNKABALESETEK ALAKULÁSÁRÓL A FELDOLGOZOTT MUNKABALESETI JEGYZŐKÖNYVEK ALAPJÁN 2020. első félév," 2020. [Online]. Available: http://www.ommf.gov.hu/index.php?akt_menu=223 [Hozzáférés dátuma: 01 10 2021]. [Hozzáférés dátuma: 10 01 2021].
[11] Magyar Szabványügyi Testület, „Személyes adatok védelméről készült úttörő szabvány," 09 2020. [Online]. Available: https://prod.mszt.hu/hu-hu/szabvanyositas/hirek/2019/09/szemelyes-adatok-vedelmerol-keszult-uttoro-szabvany. [Hozzáférés dátuma: 09 01 2021].
[12] MSZ ISO/IEC 27001:2006, 2006.
[13] L. Berek, T. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.

OPPORTUNITY TO COPE WITH COMPLEX SECURITY CHALLENGES

LEHETŐSÉG A KOMPLEX BIZTONSÁGI KIHÍVÁSOK KEZELÉSÉRE

SZAKALI Miklós [1] – SZŰCS Endre [2]

Abstract

In this article, we would like to draw attention to the emergence of complex security challenges and crises, and offer one possible way to address them. Illegal migration and the ongoing coronavirus epidemic provided the actuality of the study. Due to the nature of the challenges, we consider it important to change attitudes and follow a complex approach to security in its interpretation. It is even more important than changing the theoretical approach to provide the forces and capabilities needed to coop with complex security challenges. Since, it has become clear that neither international organizations nor states have been prepared for a comprehensive response to the crisis. It seems that this statement is currently still valid. We consider the foresight and systematic development of critical infrastructures as the potential basis for managing complex security challenges and crises, which is why we have outlined the foundations of a civil security strategy and planning system in this article.

Keywords

complex security, security challenge, resilience, strategy, planning

Absztrakt

A cikkben a komplex biztonsági kihívások és válságok megjelenésére és kezelésük egyik lehetőségére hívjuk fel a figyelmet. Az illegális migráció és a jelenleg is zajló koronavírus járvány adták a téma vizsgálatának aktualitását. A kihívások jellege miatt fontosnak tartjuk a biztonság értelmezésében is a szemléletváltást és a biztonság komplex megközelítésének térnyerését. Az elméleti megközelítés megváltoztatásánál is fontosabb, hogy az összetett biztonsági kihívások kezeléséhez szükséges képességek is biztosításra kerüljenek. Ugyanis bebizonyosodott, hogy sem a nemzetközi szervezetek sem pedig a nemzetállamok nem voltak és jelenleg sincsenek felkészülve a felmerült válsághelyzet átfogó kezelésére. A kritikus infrastruktúrák előrelátó és szisztematikus fejlesztésében látjuk a komplex biztonsági kihívások és válságok kezelésének az alapját, ezért egy polgári biztonsági stratégia és tervezési rendszer alapjait körvonalaztuk a cikkben.

Kulcsszavak

komplex biztonság, biztonsági kihívás, resilience, stratégia, tervezés

[1] mszakali@hotmail.com | ORCID: 0000-0002-8983-3855| PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu| ORCID: 0000-0003-2818-262X | senior lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

A BIZTONSÁG KOMPLEX MEGKÖZELÍTÉSE

A világ 2020 első napjaitól kezdve folyamatosan harcban áll egy különleges ellenséggel, Kínától az USA-ig a világ minden részén szedi áldozatait ez a háború, amelyben ugyan egyetlen lövés sem dördült el, de a koronavírus járvány (COVID-19) már eddig is olyan veszteséget okozott emberéletben, gazdasági és társadalmi tekintetben egyaránt, amely joggal hasonlítható a legnagyobb háborús konfliktusok pusztításaihoz. A koronavírus járvány túlnőtt a kizárólag egészségügyi veszélyhelyzet szintjén és egy komplex globális biztonsági válságot idézett elő. A járvány a kialakulását követően kizárólag egészségügyi fenyegetést jelentett, de rohamos terjedése és súlyos következményei, illetve a védekezésként bevezetett rendszabályok hatásai rövid időn belül gazdasági és pénzügyi válsághoz vezettek. A munkahelyek tömeges bezárása pedig növelte az egyéni létbizonytalanságot és a társadalmi feszültségek elmélyülését idézte elő. A válság kezelése a nemzeti kormányokra hárult, amelyek többsége nem volt felkészülve a járvány okozta egészségügyi veszélyhelyzet kezelésére sem, de különösen nem egy komplex válsághelyzet megoldására. Így a válság átgyűrűzött a politikai szférára is, Európa több országában (Olaszország, Spanyolország, Németország, stb.) erőszakos tüntetéseken tiltakoztak a kormányok válságkezelési politikái ellen, illetve Szlovákiában a kormány működésképtelennek bizonyult és a helyzet politikai, kormányzati széteséssel fenyegetett. A jelen helyzet alapján kijelenthetjük, hogy korunkban már nincsenek elszigetelődött, egy komponensű biztonsági kihívások és válságok. A mai globalizált, információs társadalmakban a biztonsági kockázatok és fenyegetések gyors kiterjedését más szektorokra, így egy biztonsági kihívás vagy válság kiterjedésének irányát, sebességét és hatásait, vagyis komplexszé válását nagyon nehéz előre jelezni és még nehezebb megakadályozni. Mindezek ellenére a járvány okozta válsághelyzet kialakulása, elterjedése és kezelése több rendszerszintű biztonsági problémára is felhívja a figyelmet.

A nemzetek nem voltak felkészülve a járvány fertőzőképességében és halálosságában rejlő globális veszélyhelyzet felismerésére és a megelőzéséhez nélkülözhetetlen nemzetközi és hazai tájékoztatás és adatszolgáltatás biztosítására. A nemzetek jelentős része a nemzeti érdekek megóvására hivatkozva csak – miután már nem tudták tovább titokban tartani - jelentős késéssel jelentette be a járvány meglétét és pusztítását. Ezzel is növelték a nemzetközi szervezetek és a környező nemzetek reagálási idejét és elősegítették a járvány továbbterjedését. Hozzáállásukat követően megkérdőjeleződött az egyéni és a közösségi biztonságtudatosság és felelősségvállalás, illetve a nemzetek közötti együttműködés és szolidaritás értéke.

A fenti hozzáállás is nehezítette a nemzetközi szervezetek munkáját, ez azonban nem magyarázat az alapvető funkcióik végrehajtásában tapasztalt jelentős hiányosságokra. Nem volt olyan nemzetközi szervezet, amely időben figyelmeztette volna az európai nemzeteket és vezette volna a megelőző tevékenységet. 2020. január 22-én a kínai hatóságok bejelentették a járvány kínai gócpontjának, a 11 milliós Wuhan városának a lezárását, ekkor még az Egészségügyi Világszervezet (WHO) genfi központjában kijelentették, hogy a koronavírus által okozott helyzet nem tekinthető nemzetközi szintű közegészségügyi veszélyhelyzetnek. Hosszas megfontolás után 2020. március 11-én a szervezet világjárvánnyá (pandémia/pandemic) nyilvánította a koronavírus-járványt, ekkor még a vezetőjük, Tedrosz Adamon Gebrejeszusz bizakodóan nyilatkozott a járvány kontroll alatt tartásának lehetőségeiről. Azonban pár nappal később március 25-én egy genfi sajtótájékoztatón már drámaian

érzékeltette a járványhelyzet súlyosságát. „Ez a vírus az első számú közellenség. Egy hónappal, két hónappal ezelőtt lett volna itt a cselekvés ideje... „ [1].

Az első kínai jelentések idején Brüsszelben és Európa nagy részén még csak úgy tekintettek a járványra, mint egy távoli kockázati tényezőre. Ennek a bizakodásnak az volt az alapja, hogy a korábbi egészségügyi fenyegetések, mint a SARS, Ebola vagy a MERS nem terjedtek el és nem okoztak európai, vagy világszintű járványt. Így 2020. februárja még a globális diplomácia jegyében telt az EU vezetői körében. Időközben egy súlyos katonai incidens történt. Szíriában több mint harminc török katona vesztette életét egy bombatámadásban, ezért a török elnök bejelentette, hogy ezen túl nem tartja vissza a menekülteket az EU-ba áramlástól, és megnyitja határait Görögország és Bulgária felé. Ez egy menekültválság kialakulását vetítette előre, amely nagyobb nyugtalanságot okozott az EU vezetői között, mint a koronavírus.

A „tiszta kép" érdekében ismernünk kell a döntés hátterét, hogy jobban megértsük miért volt az EU vezetés olyan buzgó a menekültválság megakadályozásában és tekintette másodlagosnak a vírus okozta helyzetet. A 2015-ös migrációs válság és az azt követő vita, valamint a megegyezés hiánya sokkal jobban próbára tette az EU egységét, mint a SARS és az Ebola járványok kezelése.

A NATO, mint az Euró-atlanti térség biztonságának szavatolója egy politikai-katonai szervezet, melynek deklarált célja a katonai fenyegetések elleni védelem. Így nem is lehet alapvető elvárás vele szemben az egészségügyi helyzet figyelemmel követése és az arra történő reagálás. A Szövetség elsősorban katonai erőit és képességei fejlesztésére fókuszál, nem pedig a polgári/polgári védelmi képességek kialakítására. A polgári készenlét (civil preparadness) keretében kizárólag azoknak a civil képességeknek és kapacitásoknak a fenntartását és fejlesztését várja a tagországoktól, amelyek szükségesek lehetnek egy szövetségi művelet támogatásához. Ugyanis a szövetséges műveletek sikere jelentős mértékben függ a nemzeti polgári eszközök és szolgáltatások mennyiségétől, minőségétől és rendelkezésre állásától.

A járvány romba döntötte az egyének megélhetését és létbiztonságát, ezzel együtt az országok társadalmi és a gazdasági biztonságát egész Európában és világviszonylatban. Jelenleg felbecsülhetetlen a keletkezett kár, és fel kell készülni a válsághelyzet kiterjedésére és elhúzódására. Hogy lehet az, hogy a fejlett nyugati világ figyelme elsiklott egy ekkora biztonsági fenyegetés felismerése és megelőzése, illetve lelassítása felett? De tovább lehet folytatni a kérdést, hogy lehet, hogy a fejlett nyugat nincs felkészülve egy komplex, nemkatonai biztonsági fenyegetés kezelésére? Úgy tűnik, hogy visszatértünk ahhoz a régi biztonsági felfogáshoz (vagy el sem mozdultunk erről a pontról), amely a II. Világháborút követően az 50-60-as években kezdett kibontakozni, de lényegében a hidegháború végéig tartotta magát és a biztonságot csak a háború és béke kölcsönhatásában, a katonai erő kérdéseivel azonosította. A 20. század közepén már megjelent, majd a hidegháborút követő évtizedekben kibontakozott a biztonságot tágabban értelmező gondolkodás, így a katonai biztonság kiegészítésre került a politikai, gazdasági, társadalmi és környezeti biztonsági dimenziókkal [2]. Ez a bővített biztonsági felfogás nem vert gyökeret a biztonságpolitikai gondolkodásban és valószínűleg ezért nem is került átültetésre a gyakorlatba. Jól látszik, hogy jelenleg Európa biztonságában érintett egyetlen nemzetközi szervezet sem képes a nem-katonai biztonsági dimenziókat is a katonai dimenzióval azonos súllyal kezelni és

azokra is kiterjeszteni szerepvállalását. Azonban ebben a kérdésben is meghatározó szerepük van a szervezetek tagállamainak, mivel szuverenitásuk védelme érdekében nem hatalmazták fel a nemzetközi szervezeteket a biztonság valamennyi dimenzióját átfogó hatáskörrel és intézkedési jogkörrel. Továbbra is elsődleges szempont a szuverenitás védelme mellett a szervezet nyújtotta előnyök kihasználása a lehető legkisebb ráfordítás mellett. Így a szervezetek kezei is meg vannak kötve, legjobb akarattal sem biztosíthatnak átfogó megoldásokat a fenyegetések és biztonsági kihívások ellen. A biztonságpolitikai előrejelzésekben visszatérő megállapítás, hogy a biztonsági kihívások rendkívül összetettek és gyorsan változnak, ezért csak sokoldalú közös képességek fejlesztésével és közös fellépéssel van esélyünk megfelelni a komplex kihívásoknak. Azonban, ha ilyen nagyságrendű és komplex hatású kihívást, mint a járvány és annak következményeinek megoldása az egyes nemzetekre marad, akkor a koordinált, közös fellépés és összefogás szép elvei csak üres szólamok maradnak.

Véleményünk szerint a 2015-ös migrációs válságot követően (amely megismétlődésének elhárítása a mai napig nincs megnyugtató módon nemzetközileg szabályozva és egységesen kezelve) a jelenlegi járvány a következő olyan kihívás, amely érinti egész Európát és nincs közös válasz egyetlen szervezettől sem, a válság kezelésének megoldása az egyes nemzetekre hárult. Ez óhatatlanul felveti a nemzetközi szervezeteknek a biztonsági szavatolásában betöltött szerepük felülvizsgálatának szükségességét. Jaume Duch az Európai Parlament szóvivője nyilatkozatában is ez a gondolat köszön vissza „Úgy gondolom, hogy ez a válság egyértelműen azt mutatja, hogy együtt erősebbek vagyunk. A vírus átlépi a határokat, és sajnos minden országot érint. Ha ilyen közös kihívásokkal vagy bármilyen típusú válsággal szembesülünk, akkor nyilvánvaló, hogy a válasznak is közösnek kell lennie. A válság után, ha azt akarjuk, hogy az EU erőteljesebben reagáljon, meg kell vitatnunk annak lehetőségét is, hogy az EU-nak eszközöket és hatásköröket adjunk ehhez” [3]. Jelenleg az EU is és a NATO is a katonai erők és képességek fokozására ösztönzik a tagországokat ezzel is a biztonság katonai dimenzióját erősítve, a többi dimenzió (és ezekből van több) kezelése úgy tűnik, hogy a nemzetekre marad. A nemzetek nem tekinthetik megfelelőnek a katonai biztonságra fordított kiadásaik ár-érték arányát sem, mivel nagy pénzügyi befektetésért csak a biztonság „egy szeletét” kapják, illetve a költséges katonai erők és képességek ráadásul csak részben, vagy egyáltalán nem használhatóak a nem-katonai kihívások és válságok kezelésére.

A KRITIKUS INFRASTRUKTÚRÁK KÉRDÉSEINEK NATO, EU ÉS HAZAI MEGKÖZELÍTÉSE

Véleményünk szerint a komplex biztonsági kihívások kezelésének alapvető feltétele a szükséges erők és képességek rendelkezésre állása, mind a katonai, mind pedig a civil biztonsági dimenziót illetően. Azonban a kihívások komplexitása, elemeik összefonódásai, valamint a biztonsági dimenziók közötti átfedések, amelyek alakulása esetleg nem is látható előre, nem teszik lehetővé, hogy minden egyes elem kezelésére külön specifikus képességet fejlesszünk ki. Ugyanakkor a specifikus képességek fejlesztésének költséghatékonysága is kérdéses, tekintettel a képességfejlesztés hosszú időtartamára, bonyolultságára és az ezzel járó magas költségekre, valamint a speciális képességek korlátozott felhasználhatóságára. Azonban nem csak speciális képességek, de komplex képességcsomagok fejlesztésére sincs

mód, mivel előre nem látható egy kihívás vagy válság komplexitásának alakulása. Úgy gondoljuk, hogy ha nincs lehetőség speciális képességek, vagy komplex képességcsomagok előzetes fejlesztésére, akkor a biztonságot szavatoló alapstruktúrák –kritikus infrastruktúrák - előrelátó és tervszerű fejlesztésére kell fektetni a fő hangsúlyt. Így olyan stabil alapot lehet elérni, amely bármilyen biztonsági kihívás azonosításához és elsődleges kezelésének megkezdéséhez képes biztosítani az alapvető képességeket. A szilárd alap egyben megteremti a lehetőségét a helyzethez nélkülözhetetlen specifikus erők vagy képességek (vakcina, tömeges oltás, műszaki határzár, stb.) előállítására. Felhívjuk a figyelmet a kritikus infrastruktúrákra, mivel a kritikus infrastruktúrák területe az a közös többszörös, amely a túlélőképesség biztosítására hivatott minden körülmények között, ezért kitüntetett figyelmet érdemel a terület kezelése. Erre láttunk több példát is a koronavírus-járvány első hullámának kezelése kapcsán, több nemzet (olasz, spanyol, magyar) elrendelte a létfontosságú termelést végző gyárak, üzemek és szolgáltatások biztosítását, illetve a "nem elsődlegesen szükséges" ágazatok szüneteltetését. Általában a létfontosságú ágazatok közé sorolták az egészségügy, a mezőgazdaság, az élelmiszeripar, az áruszállítás az áram-, gáz-, vízellátás, a gyógyszeripar, a telekommunikáció és a sajtó tevékenységét. Magyarországon még külön akciócsoportot is létrehoztak a kritikus infrastruktúra működésének segítésére és biztosítására a honvédelmi miniszter vezetésével.

A katonai biztonsági dimenzió közelmúltban bekövetkezett változásai (a Krím-félsziget megszállása és a hibrid hadviselés megjelenése) kellettek ahhoz, hogy szövetségi szinten ismét előtérbe kerüljön a kollektív védelem és az ahhoz kapcsolódó stratégiák, így a kritikus infrastruktúrák biztosítása is. A kihívásra válaszul olyan védelmi stratégia kidolgozására volt szükség, amely a katonai erő mellett magában foglalja a kormányzat polgári szerveit és a magán szektor kulcsszereplőit is, vagyis össztársadalmi megközelítésre épül. A walesi döntést [4] követően a szövetség kidolgozta az alapkövetelményeket a nemzeti resilience-re (Baseline Requirements for National Resilience) [5], amely hét területet határozott meg a nemzetek részére, amelyen fenn kell tartani a működőképességet a NATO katonai erőfeszítéseinek támogatása és a nemzeti hátországok alapvető életfeltételei biztosítása érdekében. A NATO megközelítés mellett ugyanezek a területek biztosítják a társadalom részére is a minimálisan elvárt szintű biztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartását válsághelyzetben, függetlenül attól, hogy a válsághelyzet a katonai vagy a nem-katonai biztonsági dimenzióhoz köthető. Ezek a következők:

- a kormányzati tevékenység folyamatossága,
- az energiaellátás fenntartása,
- a civil kommunikációs szolgáltatások fenntartása,
- az élelmiszer-, és vízellátás biztosítása,
- képesség a tömeges migráció kezelésére,
- képesség a tömeges sérültellátásra,
- a polgári szállítási rendszerek fenntartása.

Szövetségi szinten ezeket az alapkövetelményeket - főleg a közös műveletek támogatása szempontjából - ítélték fontosnak, de emellett a nemzetek saját érdekeik figyelembevételével más területeket/ágazatokat is kritikus fontosságúnak minősíthetnek.

Hazánkban a kritikus infrastruktúrák azonosításának és védelmük lehetőségeinek szabályozása szorosan kapcsolódik az EU-s szabályozáshoz. A 2004. évi madridi és 2005. évi londoni terrortámadásosokat követően az Európai Tanács a kritikus infrastruktúrák védelmét szolgáló átfogó stratégia kialakítására kérte fel a Bizottságot. Ennek keretében a Bizottság előbb közleményt fogadott el „A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben" címmel, majd a Zöld Könyvben [6] fogalmazta meg a Kritikus Infrastruktúra Védelem Európai Programjának (EPCIP) általános célkitűzésit.

A közösségi szintű tanácsi irányelv azt a célkitűzést szolgálta, hogy kiegészítse a nemzetek létfontosságú infrastruktúráinak védelmét célzó már meglévő programjait. Azonban akkor még a létfontosságú infrastruktúrákkal kapcsolatos tevékenység szabályozása hiányzott a magyar jogrendszerből, akárcsak az Európai Unió tagállamainak többségében. A kritikus infrastruktúrák azonos értelmezése érdekében és a nemzeti jogalkotás könnyítésére a Zöld Könyv mellékleteként ajánlást adtak ki a kritikus infrastruktúrák szektorairól és azok által biztosított termékekről és szolgáltatásokról. Magyarországon 2012-ben elfogadták a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényt [7]. Ez a törvény az EU Zöld Könyvében kiadott ajánlásoknak megfelelően készült, de a nemzeti sajátosságoknak megfelelően néhány tekintetben eltér az ajánlástól. A szabályozás tartalmazza az időközben megjelent 2008-as [8] és 2016-os [9] irányelveket az európai kritikus infrastruktúrák azonosításáról, kijelöléséről és védelmük fokozásáról, valamint a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintet biztosító intézkedésekről. Meg kell említeni még a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló törvényt [10], amely meghatározza a létfontosságú intézmények és szolgáltatások működtetésének és védelmének rendjét és felelőseit a különleges jogrend bevezetése esetén.

Jelentős különbség figyelhető meg a NATO és az EU koncepciók között, míg a NATO a széleskörű biztonsági kihívásokkal szembeni katonai műveletek támogatását helyezi előtérbe a resilience kiépítésével, addig az EU a nemzetközileg közösen használt kritikus infrastruktúrákra és a társadalmi és közösségi szintű működőképesség megóvására koncentrál. Ugyanakkor az EU megközelítése és ebből adódóan a hazai törvényalkotás is a védelemre, azon belül is a terrorizmus, hibrid és kiber fenyegetések elleni védelemre és következményeinek kezelésre összpontosít, nem pedig a kritikus infrastruktúra által nyújtott termék, vagy szolgáltatás esetleges válsághelyzet alatti folyamatos biztosítására. Ezért sem az EU, sem pedig a nemzeti szabályozás nem határoz meg követelményt a működőképesség folyamatos fenntartása érdekében a tartalékképzésre, a pótlásra, illetve az infrastruktúra kiesése, megsemmisülése esetén a kritikus termék vagy szolgáltatás más forrásból, ágazattól történő időszakos vagy huzamosabb időn keresztül való biztosítására. Mindezen eltérések ellenére a jelenlegi magyar szabályozás biztosítja a megfelelő alapokat a válsághelyzetek kezelésére, azt azonban messze nem állíthatjuk, hogy minden a legnagyobb rendben lenne és nincs mit fejleszteni a szabályozáson, illetve a szabályozás végrehajtásán.

A KRITIKUS INFRASTRUKTÚRÁK TERVSZERŰ FEJLESZTÉSÉNEK SZÜKSÉGESSÉGE

Egy válság kitörése esetén kizárólag a már meglévő erőkkel, eszközökkel és képességekkel lehet felvenni a harcot és megkezdeni a válság kezelését, kiterjedésének megakadályozását. Adott esetben egy szükséges eszközt vagy anyagot be lehet szerezni a piacon,

de egész rendszerek és infrastruktúrák kialakítása ad hoc jelleggel nem biztosítja a válságkezelés hatékonyságát. Különösen igaz ez olyan helyzetekben, amikor az emberi tudás és tapasztalat meghatározó egy helyzet kezelésében (kutatás, informatika, egészségügy, stb) és ezeket a kompetenciákat nem lehet egyik napról a másikra „előállítani". Csak az előrelátó és összehangolt fejlesztések biztosíthatják a szükséges képességek rendelkezésre állását egy válság megelőzéséhez vagy kezeléséhez. Ugyanakkor tudatában kell lenni annak a ténynek is, hogy a képességek kialakítása általában nem rövid távú folyamat, általában 6-10 évről beszélünk egy képesség kialakítása kapcsán, beleértve az infrastruktúra, humán erőforrás, jogi, pénzügyi és szakmai eljárásrend biztosítását illetve szabályozásuk kidolgozását, tesztelését és bevezetését. Ezért a tervezésnek legalább közép és hosszútávra kell meghatároznia a fejlesztendő irányokat és a tervekben biztosítani a végrehajtáshoz szükséges feltételeket.

Néhány példa, amely bemutatja, hogy hazánkban is rányomta bélyegét a járvány kezelésére a kritikus infrastruktúrák fejlesztése területén tapasztalható közép és hosszú távú tervezés hiánya. Nem lehetett figyelmen kívül hagyni, hogy az egészségügy, amely a kritikus infrastruktúrák egyik elemét képezi, az első hullámban nem volt felkészülve a járvány kezelésére. Nem rendelkeztek védő-, és teszteszközökkel (maszk, tesztek, védőruházat), lélegeztető gépekkel, ventilátorokkal, intenzív kezelésre alkalmas kórházi ágyakkal. Folyamatos szállítással, tonnaszámra kellett beszerezni a védő-, és egészségügyi eszközöket abból a Kínából, ahonnan a járvány kiindult. Így nem volt kockázatmentes az eszközök beszerzése és alkalmazása, nem csak a vírus terjedése miatt, hanem a hirtelen felfuttatott termelés miatt sem, amely gyakran hibás termékek előállításához vezetett. A sürgősséggel lefolytatott beszerzés csak megerősíti a válságkezelésre való előzetes felkészülés fontosságát. Amennyiben nem készülünk fel tervszerűen a válságok (bármilyen jellegű) kezelésére, akkor időt vesztünk, késünk a hatékony reagálással, amely súlyos veszteségekhez vezethet, mind emberélet, mind gazdasági és társadalmi tekintetben. A szerencsén múlhat, hogy rövid idő alatt be tudunk-e szerezni megfelelő mennyiségű és minőségű anyagokat és eszközöket egy hirtelen, világviszonylatban megnövekedett kereslet megjelenése esetén. A beszerzések gazdasági hátteréről még nem beszéltünk, az azonban biztos, hogy a nagy kereslet és a sürgősség jelentős árfelhajtó tényezőkké váltak, így lényegesen drágábban lehetett az említett eszközöket beszerezni, mintha ez még évekkel korábban a felkészülés részeként történt volna.

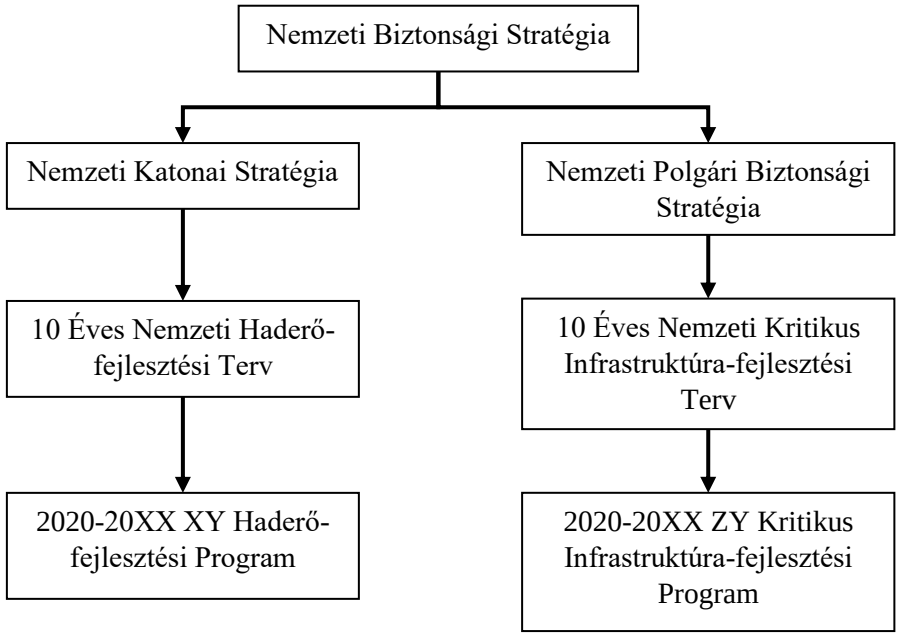
Nagy vitát váltott ki a kórházi ágyak felszabadítása orvos-szakmai és lakossági körökben egyaránt, mindez szintén azt mutatja, hogy ez a művelet nem volt előre leegyeztetve a kórházakkal, a kórházak nem voltak előre kijelölve és felkészítve egy ilyen feladatra. Eddig még nem is említettük a humán tényezőt, az orvosokat, ápolókat és egyéb kórházi személyzetet, akik példamutatóan és folyamatosan helytállnak a válsághelyzetben, pedig közismert az egészségügyet sújtó munkaerőhiány. Az OECD által közölt adatokból ki lehet számolni, hogy 2009 és 2017 között itthon nagyjából 12 ezer orvost és háromszor ennyi nővért képeztek. Orvosból azonban mindössze kétezerrel, ápolóból pedig csak 1500 dolgozott több Magyarországon 2017-ben, mint nyolc évvel korábban [11]. Az első hullám tapasztalatai alapján javulás mutatkozott a második hullámra való felkészülésben. Azonban a szűk keresztmetszet ismét megmutatkozott az emberi erőforrások korlátozott rendelkezésre állása tekintetében. Ez a tény megerősíti, hogy nem lehet ad hoc módon biztosítani olyan létfontosságú erőforrásokat és képességeket, amelyek kialakításához hosszú idő szükséges. Különbséget kell tenni a pénzen, még ha drágábban is, de beszerezhető anyagok és

eszközök, valamint a hosszas tanulást, gyakorlatot igénylő képességek biztosítása között. Sajnos az utóbbi képességeket még jelentős ráfordítás esetén sem lehet „leemelni a polcról" és azonnal felhasználni, csak hosszútávú tervszerű tevékenységgel lehet elérni hadrafoghatóságukat.

Valamelyest hasonló képet mutatott a létfontosságú létesítmények és szolgáltatások kijelölésének és bejelentésének helyzete is. A honvédség - a különleges jogrend alapján - feladatot kapott mintegy 140 létfontosságú intézmény tekintetében a katonai irányítás bevezetésére, ez főleg az alapvető szolgáltató- és gyártókapacitások, közlekedési, energetikai, gyógyszeripari cégek meghatározott körét érintette. Mint látjuk, ezek mind a kritikus infrastruktúrák részeit képezik és szerepelnek a fenti táblázatban. A cégek kijelölése és a kapcsolatfelvétel rövid idő alatt megtörtént, amelyet az érintettek döntő többsége tudomásul vett, illetve néhány cég önként kérte is „létfontosságúvá" minősítését. Azonban általában aggályosnak értékelték az üzleti titok körébe tartozó gazdasági és pénzügyi adatok kezelésének kérdéseit. Ugyanakkor a kritikus infrastruktúrák tulajdonosainak és működtetőinek jelentős része nincs felkészülve/felkészítve egy válsághelyzetben várható feladataira, jogi, irányítási és együttműködési kötelezettségeire.

Az eddig leírtak alapján arra a következtetésre jutottunk, hogy a kritikus infrastruktúra folyamatos működésének és túlélőképességének biztosítása hosszútávú biztonsági követelmény. Ezért nagyobb szerepet kell kapnia a biztonsági stratégiák kidolgozásában, tervezésében is. Magyarországon nincs nagy hagyománya a stratégiaalkotásnak, a rendszerváltást követően, 1990-töl kezdődött a magyar biztonságpolitika alapvetéseinek a lefektetése a Magyar Köztársaság biztonság-, és védelempolitikai országgyűlési határozatban való megjelentetésével. Azonban a nyugati értelemben vett stratégiaalkotás NATO tagságunkat követően kezdett meghonosodni a magyar biztonság-, és védelempolitikában, amelyet jól mutat, hogy 2002-ben jelent meg az első Nemzeti Biztonsági Stratégia (NBS) és jelenleg a 2020 februárjában elfogadott NBS [12] a negyedik a sorban. Jelentős előrelépés történt a katonai biztonsági dimenzió előrelátó tervezésében, mivel részt veszünk a NATO védelmi tervezési rendszerében, amelyben jelenleg 2036-ig határoznak meg katonai erők és képességek fejlesztésére vonatkozó úgynevezett képesség-célokat. Ezeket a célokat beépítjük a nemzeti védelmi tervezés rendszerébe, tízéves időhorizontra bontjuk és forrásokat rendelünk hozzájuk. Mint látjuk magyar szabályozás szerint tíz évre előre rendelkezésre állnak a haderő fejlesztésére vonatkozó tervek, elgondolások, amelyek megvalósítása esetén egy olyan katonai képességet kapunk, amely képes megfelelni az adott időszakra valószínűsített főleg katonai-biztonsági kihívásoknak. Ez az előrelátó stratégiai szintű tervezés hiányzik a polgári képességek (kritikus infrastruktúra) fejlesztésének vonatkozásában. A 2012-ben kiadott Nemzeti Biztonsági Stratégia (NBS) [13] célkitűzéseit és követelményeit csak a katonai oldal bontotta le a Nemzeti Katonai Stratégiában (NKS) [14], a 10 Éves Haderőfejlesztési Tervben és a Nemzeti Haderőfejlesztési Programban. A polgári képességek vonatkozásában nincs egységes tervezési rend, amely az NKS-hez hasonlóan tartalmazná a polgári képességek 10 éves fejlesztésének célkitűzéseit, főbb irányait és prioritásait, ezzel biztosítva a „biztonsági érem" másik oldalát. A 2020-ban megjelent Nemzeti Biztonsági Stratégia 2020 tartalmazza hazánk biztonsági érdekeit és átfogó módon meghatározza azokat a biztonságra veszélyt jelentő kockázatokat és fenyegetéseket, amelyek kezelésére fel kell készülnünk. A honvédelmi miniszter nyilatkozata szerint a katonai oldal megkezdte a bizton-

sági stratégia katonai vonatkozásainak a feldolgozását és a Nemzeti Katonai Stratégia kidolgozását. Ugyanakkor nincs jele egy átfogó Polgári Biztonsági Stratégia kidolgozásának. Az NBS ugyan tartalmaz olyan ajánlást, hogy a tárcák vegyék figyelembe az NBS megállapításait stratégiáik kidolgozásánál. Ez azonban nem biztosítja az egységes biztonsági fókuszú megközelítését a szakpolitikai stratégiák kidolgozásához, illetve a polgári képességek (kritikus infrastruktúrák) fejlesztésének egységes elgondolását egy dokumentumban összefoglalva. Márpedig csak egy ilyen komplex megközelítés képes biztosítani azokat a képességeket, amelyek lehetővé teszik a komplex kihívások kezelését hosszú távon. A katonai oldal nem létezhet polgári képességek nélkül és ez fordítva is igaz, együtt alkotják a „biztonsági érem két oldalát." A mai komplex kihívások világában csak komplex válaszadás lehetséges a katonai és a nem-katonai dimenziók együttes alkalmazásával. Ezért a következő struktúrát javasoljuk az egységes nemzeti biztonsági tervezési rendszer kialakításához:



1. Ábra: A nemzeti biztonság tervezésének struktúrája (saját szerkesztés)

Az NBS rendeltetése, hogy a biztonsági környezet és a várható biztonsági kihívások elemzése alapján meghatározza azokat a nemzeti célokat, azok elérésének módját és az átfogó kormányzati eszközrendszert, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.

A NKS és a Nemzeti Polgári Biztonsági Stratégia (NPBS) az NBS által meghatározott célok és irányelvek alapján az országot érintő fenyegetéseket és kihívásokat, illetve azok kezelésének lehetőségeit bontják le ágazati szintű stratégiai feladatokra és célkitűzésekre. Az NBS által megjelölt biztonsági fenyegetések és kihívások alapján forgatókönyv/ek és cselekvési változatok kerülnek kidolgozásra, amelyek alapján modellezik a haderő és a kritikus infrastruktúra ágazatainak alkalmazási rendjét és prioritásait. A model-

lezés eredményei alapján pedig meghatározzák a haderőfejlesztés, illetve a kritikus infrastruktúra ágazati fejlesztéseinek fő irányait, prioritásait, valamint a szükséges eszközöket és forrásokat.

A 10 éves fejlesztési stratégiák/tervek az NKS-ben meghatározott haderőfejlesztési irányokon belül az egyes szolgálati ágakra, illetve az NPBS-ben megjelölt ágazatokra lebontva tartalmazzák a fejlesztés minőségi, mennyiségi szervezeti és egyéb követelményeket, illetve a fejlesztések nagybani időrendjét és forráselosztását. A kritikus infrastruktúra tekintetében a fejlesztések és források egymáshoz rendelése természetesen bonyolultabb feladat, mint a katonai oldal esetében, lévén, hogy a kritikus infrastruktúrában több ágazat érintett és az ágazatok között nem csak állami tulajdonú cégek vannak, hanem szép számban magán és multinacionális vállalatok is. Ezekkel szemben szélesebb eszközrendszer alkalmazására van szükség a kívánt irányú fejlesztések, beruházások elérésére. A törvényi szabályozáson kívül pénzügyi, gazdasági és egyéb ösztönzők bevezetésével, vagy pedig állami biztonsági beruházások által lehetséges a stratégiai célkitűzések elérése.

A fejlesztési programok pedig mindkét esetben a végrehajtási programterveket jelentik, amelyek tartalmazzák minőségi követelményeknek megfelelő eszközök beszerzését, darabszámot, árat, fizetési feltételeket, határidőket, személyzet kiképzését, betanítását, használati eljárások kidolgozását, stb. Véleményünk szerint a polgári képességek fejlesztéséhez is hasznos lehet a NATO által elfogadott DOTMLPFI[3] katonai képességek fejlesztésére alkalmazott megközelítést, amely végrehajtása esetén használható képességet eredményez.

A biztonság átfogó értelmezése és bevezetése a stratégiai tervezés nemzeti rendszerébe jelenleg egy nagybani elgondolás, amely a hosszú idő óta működő katonai biztonsági dimenzió tervezési rendszerének rugalmas adaptációja a nem-katonai biztonsági dimenzió elemeire a dimenziók közötti különbségekből adódó sajátosságok figyelembe vételével. A fent vázolt struktúra és eljárásrend megfelel a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. Rendeletben [15] foglaltaknak, amely lehetőséget biztosít az egyes ágazatok tervezése mellett az ágazatok közötti összhang megteremtésére a horizontális együttműködés kialakítására. A részletes tervezési eljárásrendet a résztvevők bevonásával ki kell dolgozni és biztosítani kell a megfelelő szabályozását. A nemzeti biztonság átfogó tervezését egy ágazatok fölötti szervezetnek célszerű végrehajtani, vagy koordinálni, mivel, szinte elkerülhetetlen az ágazatok közötti súrlódások, érdekérvényesítési villongások megjelenése mivel több ágazat a jogkörének csorbításaként, illetve pluszforráshoz jutási lehetőségként értelmezné ezt a tevékenységet. Azonban tudomásul kell venni, hogy a válságkezelés egy összkormányzati feladat, amelyben az ágazati jogkörök jelentős és lényegi része kikerül ágazati kezelésből, ezért célszerű, hogy a válsághelyzetre való tervezés és felkészülés is központi irányítással-vezetéssel történjen. Ugyanakkor az egyes ágazatok stratégiái ki kell, hogy egészüljenek az ágazat számára meghatározott stratégiai biztonsági feladatok és fejlesztések tervezésével, végrehajtásával és ellenőrzésével.

[3]DOTMLPFI - Doctrine/Doktrína, Organisation-Szervezet, Training/Kiképzés, Material/Anyagok-Eszközök, Leadership/Vezetés, Personnel/Személyzet, Facilities/Létesítmények-Infrastruktúra, Interoperability/Interoperabilitás.

ÖSSZEFOGLALÁS

Kimondhatjuk, hogy a megváltozott biztonsági körülményekre való tekintettel szemléletváltásra van szükség, egyforma súllyal kell kezelni a katonai és a nem-katonai biztonsági dimenziókat, hiszen ezek összességében képezik a biztonságot.

Mindezt a biztonság szavatolásában érintett nemzetközi szervezetek felhatalmazása és feladatrendszere tekintetében is felül kell vizsgálni, mivel a koronavírus járvány rövid időn belül a második válsághelyzet (első a tömeges migráció), amelynek előrejelzésében, megelőzésében és egységes kezelésében a nemzetek magukra maradtak. Ez természetesen a nemzetek szándékától is függ, amennyiben a szuverenitásuk érdekében ragaszkodnak a jelenlegi helyzet fenntartásához, akkor jelentős ráfordítással csak a biztonság „egy szeletéhez" a katonai biztonsághoz jutnak és elesnek a komplex kihívások nem-katonai biztonsági dimenzióra is kiterjedő, közös kezelésétől.

Nemzeti vonatkozásban is szükségesnek tartjuk a biztonság tágabb értelmezését követni és a biztonsági dimenziókat átfogóan értelmezni. Mindennek részeként a nem-katonai dimenziókat célszerű beemelni a biztonság stratégiai tervezési rendszerébe és a honvédelmi ágazatban bevált tervezési rendszert alkalmazni a területre, a szükséges rugalmasság és jellemző sajátosságok figyelembe vételével. Egy hosszabb távra (10 évre) történő összehangolt prioritásokra épülő fejlesztési terv biztosíthatná, hogy a költségvetési források tervszerű felhasználásával olyan célzott képességek, kapacitások és eszközállomány kerüljön kialakításra, amely nagyobb eséllyel biztosítja a komplex kihívások kezelését egy válsághelyzet kialakulása esetén.

A biztonság stratégiai tervezésének részletes eljárásrendjét a résztvevők bevonásával ki kell dolgozni és biztosítani kell a megfelelő szabályozását a kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. Rendeletben foglaltakkal összhangban.

FELHASZNÁLT IRODALOM

[1] Index, „https://index.hu/kulfold/2020/03/25/who_koronavirus_cselekves_ideje_egy_ honappal_ezelott/," Budapest, 2020.
[2] Vida Csaba, „A biztonság és a biztonságpolitika katonai elemei," Nemzetbiztonsági Szemle, MMXIII/I évf. I szám, 91-92. o., 2009.
[3] Index, „https://index.hu/kulfold/eurologus/2020/04/12/ep_szovivo_koronavirus_ jarvany_eu_valsag_jaume_duch/," Budapest, 20. 03. 2020.
[4] NATO, „Wales Summit Declaration", Brüsszel, 2014.
[5] ACT, Building Resilience, Norfolk (USA), 2017.
[6] EU Bizottság, Zöld Könyv a kritikus infrastruktúra védelmének európai programjáról, Brüsszel, 2005.
[7] Országgyűlés, CLXVI. tv. (2012) A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, Budapest, 2012.
[8] EU Bizottság, Tanácsi irányelvek az EU kritikus infrastruktúrák azonsításáról és kijelöléséről, Brüsszel, 2008.
[9] EU Bizottság, EU parlamenti és tanácsi irányelvek a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, Brüsszel, 2016.

[10] Országgyűlés, CXIII. tv. (2011) A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, Budapest, 2011.
[11] Jandó Zoltán, „Magyar orvosok ezrei, nővérek tízezrei hagyják el a pályát vagy az országot", G7.hu, Budapest, 2019.
[12] Magyarország Kormánya, 163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, Budapest, 2020.
[13] Magyarország Kormánya, 1035/2012. (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájának elfogadásáról, Budapest, 2012.
[14] Magyarország Kormánya, 1656/2012. (XII.20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájának elfogadásáról, Budapest, 2012.
[15] Magyarország Kormánya, 38/2012. (III.12.) Korm. rendelet a kormány stratégiai irányításáról, Budapest, 2012.

THE INEVITABLE REFORMS OF THE UN IN THE LIGHT OF THE FAILURES OF CRISIS MANAGEMENT OPERATIONS

AZ ENSZ ELKERÜLHETETLEN REFORMJAI A VÁLSÁGKEZELŐ MŰVELETEK KUDARCAINAK TÜKRÉBEN

FÁBIÁN Péter[1]

Abstract

Since its inception in 1945, the UN has not only had success stories behind it, but many failures and negative experiences have surrounded its nearly 75-year existence. In my dissertation, I analyze the UN peacekeeping and crisis management operations, and then examine the reasons behind the organization's efficiency problems. In addition, I am looking for a link between the successful adoption and adaptation of each reform proposal and the failure of initiatives. My hypothesis is that the organizational and operational structure of the United Nations has not kept pace with the changes of recent decades, resulting in structural, political, economic, and social fault lines that would require almost immediate intervention to remedy. In the course of my research, I am also looking for the answer to whether individual participating countries pay the sums of money and other contributions imposed on them, or whether they may fail to do so or refuse to do so.

Keywords

UN, Security Council, peacekeeping operations, pandemic, budget

Absztrakt

Az ENSZ 1945-ös létrehozása óta nemcsak sikertörténeteket tudhat a háta mögött, hanem megannyi kudarc és negatív tapasztalat övezi közel 75 éves fennállását. Dolgozatomban az ENSZ békefenntartó és válságkezelő hadműveleteit elemzem, majd azt vizsgálom, milyen okok állhatnak a szervezet hatékonysági problémáinak hátterében. Ezen felül összefüggést keresek az egyes reformjavaslatok sikeres elfogadása, adaptációja, valamint a kezdeményezések bukása között. Hipotézisem szerint az ENSZ szervezeti és működési struktúrája nem követte le az elmúlt évtizedek változásait, s emiatt olyan strukturális, politikai, gazdasági és társadalmi törésvonalak alakultak ki benne, amelyek orvoslása szinte azonnali beavatkozást kívánna. A kutatás során arra is keresem a választ, hogy az egyes részes országok teljesítik-e a rájuk kirótt pénzösszegek és egyéb hozzájárulások befizetését, vagy esetleg elmulasztják, megtagadják ezek teljesítését.

Kulcsszavak

ENSZ, Biztonsági Tanács, békefenntartó hadműveletek, világjárvány, költségvetés

[1] fabianpeter@topcopgroup.com| ORCID: 0000-0003-0640-6557 | founder, Top Cop Group | alapító, Top Cop Group

MOZGÁSBAN AZ ENSZ

Az Egyesült Nemzetek Szervezete (a továbbiakban: ENSZ) egy olyan nemzetközi szervezet, amely célja a béke és a biztonság fenntartása, a nemzetállamok közötti egyenjogúság garantálása, a szabadságjogok biztosítása, valamint a világbéke megteremtése különböző soft power eszközök (gazdasági fejlődés elősegítése, emberi jogok tiszteletben tartása, békefenntartás) segítségével. Az ENSZ struktúrája 5 pilléren nyugszik. Az első a Közgyűlés, ahova minden részes állam 5-5 képviselőt delegálhat. A második a Biztonsági Tanács, amely 15 taggal dolgozik. A 15 tagból 5 állandó tagország (Kína, Franciaország, Oroszország, Egyesült Királyság, Egyesült Államok) vesz részt a szervezet munkájában, s további 10 tagot kétévente választanak a részes felek közül. Fontos kiemelni, hogy az 5 állandó tagnak minden kérdésre kiterjedő vétójoga van, valamint azt is érdemes jelezni, hogy a Biztonsági Tanács döntései kötelező érvényűek minden tagországra. Harmadik pillérként a Gazdasági és Szociális Tanács említhető, amely a jólét, a szociális egyenlőség és gazdasági stabilitás előmozdításáért fáradozik. Negyedik elemként a Gyámsági Tanácsok érdemes kiemelni. Ez a szerv a gyámság alatt álló nemzetek ügyeivel foglalkozik. Végül, de nem utolsó sorban a Titkárságra is ki kell térni. A Titkárság vezetője a főtitkár, akinek a munkáját szakképzett tisztviselői kar segíti. 2017. január 1-jétől a szervezet főtitkára António Guterres, Portugália korábbi miniszterelnöke. Az 5 darab szervezeti egységen felül számos szakosított szerv is dolgozik az ENSZ sikeréért, valamint egyéb autonóm szervek is hozzájárulnak a mindennapi működéshez. Az intézmény integráns részét képezik a békefenntartó hadműveletek, amelyek mára az ENSZ profiljával egyenlők lettek. Napjainkban a szervezet a világ számos pontján teljesít békefenntartó szolgálatot, amellyel a béke és biztonság megteremtéséért küzdenek.

Az ENSZ égisze alatt jelenleg (2020. december 31-i adatok szerint) 94 484 személy vesz részt a tizenkét békefenntartó műveletben. 1948. óta a szervezet 71 hadműveletet bonyolított le, és négyezernél több ember vesztette életét a különböző missziók során. A jelenleg is futó 13 hadművelet ezidáig 1674 személy életét követelte. A 2019. július 1-je és 2020. június 30-a közötti időszakra jóváhagyott költségvetés körülbelül 6,5 milliárd dollár volt. [1] A 2020 decemberi állás szerint négy térségben folyik békefenntartó hadművelet: hat Afrikában, három a Közel-Keleten, kettő Európában, egy pedig Ázsiában. A műveletekben 125 ország katonái (csapatkontingens, szakértők, törzstisztek) rendfenntartói, civil személyek, valamint önkéntesek vesznek részt. Érdekességként azt is fontos megemlíteni, hogy az Egyesült Államok Kormányzati Felügyeleti Hivatalának (U.S. Government Accountability Office) számítása szerint az Egyesült Államok számára nyolcszor költséghatékonyabb egy békefenntartó hadműveletet anyagilag támogatni, mint saját erőit kihelyezni. [2]

A jelenlegi 12 békefenntartó hadművelet közül az UNTSO (az ENSZ Fegyverszüneti Ellenőrző Szervezete) és az UNMOGIP (az ENSZ Katonai Megfigyelő Csoportja Indiában és Pakisztánban) missziók nevezhetők a klasszikus, első generációs békefenntartó akcióknak, amelyek immár 75 éve zajlanak. Az UNDOF (az ENSZ Csapatszétválasztási Megfigyelő Hadereje), az UNFICYP (az ENSZ Ciprusi Békefenntartó Hadereje), valamint az UNIFIL (az ENSZ Ideiglenes Libanoni Hadereje) missziók az 1970-es években indultak, s ezek mondhatók az első generációs műveletek érettebb változatának.

A MINURSO (az ENSZ Nyugat-szaharai Népszavazási Missziója) és az UNMIK (az ENSZ Ideiglenes Adminisztrációs Missziója Koszovóban) békefenntartó missziók második generációs ENSZ-hadműveletek. Lezárásuk a mai napig nem valósult meg. A harmadik generációs műveletek közé azok az akciók sorolhatók, amelyek a 2000-es években indultak el: UNAMID (az Afrikai Unió és ENSZ Hibrid Művelete Darfúrban), UNMISS (az ENSZ Szudáni Missziója), valamint UNISFA (az ENSZ Ideiglenes Biztonsági Erő Abjejben).

Negyedik generációs békefenntartó akciónak nevezhetők azok a kezdeményezések, amelyek 2010-ben vagy még később indultak el. Itt már nemcsak „egyszerű" békefenntartásról van szó, hanem az ott szolgáló katonák sokkal összetettebb feladatokat látnak el, a műveleti feladat sok esetben sokkal veszélyesebbek, mint az előző generációkban tapasztalhatók, illetve az erők összetettsége is jelentősebb. Ebbe a kategóriába sorolható a MINUSCA (az ENSZ közép-afrikai missziója), továbbá a MONUSCO (az ENSZ Stabilizációs Missziója a Kongói Demokratikus Köztársaságban) is. Az említett akciók közül a Kongói Demokratikus Köztársaságban tapasztalhatók a mai napig a legvéresebb összecsapások, így az ottani műveleti terület instabil állapota miatt ez az egyik legveszélyesebb, jelenleg is futó békeművelet. [3]

AZ ENSZ REFORMOKRA SZORUL

Sok szakértő és a politikus szerint az ENSZ azóta szorul reformokra, amióta létrehozták. Struktúrájánál és belső szerkezeti felépítésénél fogva olyan gátló tényezők és hatékonyságnövelést akadályozó elemek találhatók benne, amelyek 75 éve hátráltatják a szervezet működését. A legszembetűnőbb nehézséget a Biztonsági Tanács koncepciója jelenti.[4] A második világháborúból győztesként kikerült – korábban említett − felek a mai napig teljes vétójoggal, s állandó tagként döntenek a szervezet sorsáról. Ezek az országok egyébként jellemzően jó helyen végeznek a katonai kiadásokat kimutató listákon. A globális katonai kiadások 60 százalékát Kína, Franciaország, Oroszország, Egyesült Királyság és az Egyesült Államok teszi ki, míg ebből 40 százalékot az Amerikai Egyesült Államok egyedül vállal. A Biztonsági Tanács látlelete azt is hűen tükrözi, hogy az elmúlt évtized demográfiai változásait mennyire nem követte le a szervezet – Afrika és Latin-Amerika egyáltalán nem rendelkezik állandó tagsági pozícióval. Megkérdőjelezhető tehát, hogy az ENSZ hogyan szeretne világbékét és jólétet teremteni úgy, hogy közben két földrész lakosságát szinte teljes mértékben kihagyja a döntéshozatalból.

A következő blokk, amelyik szintúgy nem rendelkezik permanens képviselettel, azok az arab országok. Kihagyásuk a mai globalizált világban aggályos lehet nemcsak biztonsági, katonai és politikai okokból, hanem gazdasági érdekekből egyaránt.[5]

Fontos rávilágítani arra is, hogy a vétójog mennyire hátráltatja, s a legtöbb esetben mennyire aláássa a fair tárgyalás és döntéshozás koncepcióját. Mivel egyetlen állandó tag vétója elegendő ahhoz, hogy egy adott határozatot elvessenek, ezért sok esetben az adott javaslat plénum elé tárása előtt informális, átláthatatlan és követhetetlen zártajtós tárgyalások zajlanak az érintett felek között. Továbbá az is trendszerűvé vált, hogy az adott államnak nem tetsző, saját politikai érdekeit nem szolgáló döntéseket egyszerűen nem támogatnak.

Ennek kapcsán példaként említhető, hogy az Egyesült Államok eddig 32 olyan határozatot szavazott le, amelyek Izraelt kritizálták.

A liberális felfogás térhódítása miatt egyre kevésbé jellemző, hogy azok az országok, amelyek nem tartják be a határozatban elfogadott döntéseket, valamilyen retorzióval, büntetéssel kellene szembenézniük. Példaként említhető a srebrenicai mészárlás vagy épp a darfúri krízis, amelyek után végül egyik országot sem szankcionálták meg. Később a szervezet elismerte, hogy komoly hibákat követtek el a srebrenicai ügy kapcsán, valamint a darfúri konfliktust sem megfelelően kezelték. Hannah Buckley nemzetközi kapcsolatok szakértő szerint épp itt lenne az ideje, hogy az ENSZ Biztonsági Tanácsának tagjai félretegyék politikai meggyőződésüket és valóban az univerzális béke és biztonság megteremtéséért munkálkodjanak. Úgy látja, hogy a világ katonailag legerősebb öt államának − további országokkal kiegészülve − képesnek kell lennie arra, hogy a stabilitás útjára vezesse a Föld lakóit. Szerinte egyszerűen nem lehet politikai érdekekről beszélni akkor, amikor milliók élete forog kockán. Buckley szerint lehet, hogy ez a felfogás túl idealisztikusnak tűnik, ám ha valódi sikereket akarunk elérni, akkor az csakis összefogással történhet meg.[6]

A békefenntartás témakörére való áttérés előtt fontos volt bemutatni, hogy a Biztonsági Tanácsban milyen törésvonalak húzódnak. Az ellentétek egyik fontos kiindulópontja a nyugati államok és Oroszország közötti súrlódás.

A szíriai háború mutatott rá leginkább, hogy míg Oroszország Bassár el-Aszad elnököt támogatta, addig az Egyesült Államok, az Egyesült Királyság és Franciaország az ellenzéki erőket. A két pólus előretolt hadszínterévé változott az ország. Az ENSZ Biztonsági Tanácsa pedig annak ellenére nézte végig tétlenül a háborús bűnöket és mészárlásokat, hogy folyamatosan értesült a térségben történtekről.[7]

A fenti példákból is jól látszik, hogy az ENSZ szervezeti működése, döntési- és végrehajtási mechanizmusa sokszor nem megfelelő módon működik. Ennek egyik legszembetűnőbb példája az, hogy a békefenntartó műveletek sok esetben mennyire elhúzódnak, milyen nagy pénzügyi ráfordítások árán sikerül kivitelezni egy-egy missziót, valamint a veszélyesség miatt hány halálos áldozattal járnak ezek a kezdeményezések. A sokasodó problémákat észlelve a szervezet 1992-ben oda jutott, hogy reformlépések bevezetését látták szükségesnek. Az ENSZ békefenntartás javítását szorgalmazó kezdeményezéseket 6 csoportba lehet osztani. 1992-ben született meg a Békeprogram (Agenda for Peace), amely Butrosz Butrosz-Gáli ENSZ-főtitkárhoz kapcsolható. Javaslatában egy ténymegállapításon, megelőző lépéseken, béketeremtésen, békefenntartáson- és építésen nyugvó béketevékenységi modellt vázolt fel. A kezdeményezés azonban kudarcba fulladt, mivel a nemzetközi közösség nem támogatta eléggé a főtitkár javaslatát az 1995-ös módosítások ellenére sem. Az ENSZ számára egyébiránt az 1990-es évek súlyos mélypontot jelentettek, hiszen ekkor történtek olyan borzalmas események, mint az 1994-es ruandai népírtás, a boszniai békefenntartók elleni elkövetett atrocitások, valamint az 1995-ös srebrenicai tömeggyilkosság. A következő reformjavaslat Lahdar Brahimi algériai politikus nevéhez köthető, aki Kofi Annan ENSZ-főtitkár felkérésére jelentésében nemcsak elméleti, hanem gyakorlati útmutatást is tett arra vonatkozólag, hogy hogyan válhatna hatékonyabbá az ENSZ. A Brahimi-jelentés három pillérre támaszkodott. Egyrészt szorgalmazta a szorosabb politikai együttműködést, a fragmentáltság elkerülését. Ezen felül olyan strukturális átszervezést javasolt, amely az ENSZ egészére kihatott.

Harmadik pontként pedig a pénzügyi, támogatási metódus radikális átszabását kell megemlíteni. Brahimi azt is hangsúlyozta, hogy a békefenntartók munkakörülményein is

javítani kell, a művelet körülményeit, időtartamát és céljait világosan kell meghatározni, valamint több erőforrásra van szükség ezek fedezéséhez.

A jelentés másik lényeges eleme az volt, hogy a békefenntartók számára engedélyezte a lőfegyver használatát önvédelem esetén. A Brahimi-jelentés – mint utólag kiderült – mérföldkővé vált az ENSZ reformjai sorában, mivel számos javaslat megvalósulása miatt valóban hozzájárult a szervezet fejlesztéséhez, költséghatékonyabbá tételéhez, valamint átláthatóságához. Ahogy arra a Felix Haass − Nadine Ansorg szerzőpáros is rávilágít, az ENSZ békefenntartó hadműveletek során jócskán csökkenhet a civil áldozatok száma, ha a szervezet jól képzett, megfelelő felszereléssel rendelkező, diplomáciai támogatással bíró kontingenseket küld a konfliktusos zónákba. [8]

Ennek megfelelően 2005 és 2007 között koncepcionális és fejlesztési reformok zajlottak le. 2006-ban Kofi Annan kezdeményezésére a Közgyűlés létrehozta a Békeépítési Bizottságot, amely a gyenge, széthullóban lévő államokat és régiókat vizsgálja megelőzési szándékkal. A Brahimi-jelentés 10 éves évfordulója alkalmából az ENSZ vezetése mindenképp egy aktuálisabb, s a jelenre reagáló reformcsomagot akart kidolgozni. Ennek gyakorlati megvalósulása lett a 2009-ben elkészült Új Horizont program. A javaslat arra szólította fel a részes államokat, hogy gondolják újra az ENSZ politikai és stratégiai céljait, valamint fejlődési irányait. A dokumentumban megfogalmazott „professzionális békefenntartás" igénye, valamint a „robosztus, globális partnerség" kialakítása a résztvevő országok között inkább csak jól csengő felvetéseknek bizonyultak. Az Új Horizont projekt pár éven belül elvesztette lendületét, majd a teljes érdektelenséget elkerülendő lépésként az új főtitkár, Ban Ki Mun 2014 októberében egy független testületet (HIPPO) hozott létre. A szervezet vezetője elkészítette a HIPPO-jelentést, amely az ENSZ átfogó értékelésén és elemzésén felül a szervezet jövőjével kapcsolatban is tesz prognózisokat.

A dokumentum ezeken felül vizsgálta a „konfliktusok változó jellegét, a béketeremtés és a politikai műveletek kihívásait, a megbízások (mandátumok) fontosságát, a vezetői és az igazgatási megállapodásokat, a tervezést, a partnerségeket, az emberi jogokat és a polgári lakosság védelmét." [9] A jelentés azonban napjainkban egyre inkább veszít erejéből. Nemcsak azért, mert Donald Trump elnök jócskán visszavágta a szervezet finanszírozását, hanem azért is, mert a Biztonsági Tanácsban résztvevő felek egyre inkább megosztottak a felmerülő kérdések kapcsán.

AZ EGYESÜLT ÁLLAMOK TÁMOGATÁSA NÉLKÜL NEM MEGY?

A szervezet működését nagymértékben befolyásolja a részes államok által befizetett pénzösszeg nagysága. A 2018/2019-es büdzsé az utóbbi évtized legszűkebb költségvetése volt. A legtöbb hozzájárulást befizető ország az Egyesült Államok, mivel évi 2,4 milliárd dollárral járul hozzá az ENSZ funkcionálásához: az általános célú költségvetés 22 százaléka, a békefenntartó missziók költségvetésének 28 százaléka Washingtonból érkezik. Aligha meglepő, hogy már 2015-től csökkentette az akkori elnök a befizetés mértékét, azonban Donald Trump volt az, aki a befizetett összegből 285 millió dollárt lefaragott. Szemléltetésképp meg kell említeni, hogy melyek azok az országok, amelyek a legtöbb hozzájárulás fizetik be az ENSZ kasszába.

A szervezet éves költségvetésének 28,47 százalékát az Egyesült Államok, 10,25 százalékát Kína, 9,68 százalékát Japán, 6,39 százalékát Németország, 6,28 százalékát az

Egyesült Királyság, míg 3,99 százalékát Oroszország fizeti. Ennek fényében tehát jól látható, hogy az ENSZ miért ennyire kitett az Amerikai Egyesült Államok befizetési hajlandóságának.

Ezen felül az is jól kivehető, hogy a korábbiak során hagyományosan nagy adakozókedvvel bíró országok, mint például India, Pakisztán, Nepál vagy Egyiptom egyre kevésbé hajlandó a nagyobb hozzájárulással támogatni az ENSZ-t. A kiszámíthatatlan biztonsági környezet, a növekvő veszteségek, valamint a műveletek komplexitása mind hozzájárul ahhoz, hogy egyre kevesebb anyagi támogatást nyújtsanak a részes felek. Összességében az a tendencia bontakozott ki, hogy Kína egyre nagyobb részt vállal a befizetésből. Ezzel természetesen a nyomába se ér az Egyesült Államok által garantált összegeknek, azonban jól kivehető az ország szándéka arra vonatkozólag, hogy még nagyobb befolyást akar magának szerezni a szervezetben. [10]

Könnyű belátni, hogy a befizetések elmaradása, illetve visszafogása meglehetős veszélyeket rejt magában. António Guterres 2019-ben a következőket nyilatkozta a téma kapcsán: „Az aktív békefenntartó hadműveleteknek rövid időn belül likviditási problémákkal kell szembenézniük a késői befizetések és elmaradások miatt. A hátralék összege jelenleg körülbelül 2 milliárd dollárra rúg, és ez az összeg várhatóan növekedni fog." [11] 2019 októberében pedig bejelentette: „ebben a hónapban elérjük az évtized legnagyobb deficitjét", majd még ezt is hozzáfűzte: „lehet, hogy novemberben arra sem lesz elég pénzünk, hogy kifizessük az alkalmazottainkat." [12] Kétségbeesett felszólalása indokolt volt, a 2019-es, mintegy 3,3 milliárd dolláros költségvetésbe – az ENSZ szerint – Washingtonnak 674 millió dollárt kellett volna befizetnie a korábbi költségvetésekből adódó további 381 millió dolláros elmaradása mellett, erre azonban októberig nem került sor, miként néhány további korábbi nagy befizető, így Dél-Korea, Irán, Izrael, Brazília, Mexikó, Szaúd-Arábia és Uruguay is elmaradt a teljesítéssel.[13]

Elemzők szerint a Trump-adminisztráció ezen a módon is igyekezett nyomást gyakorolni az ENSZ-re, hogy az csökkentse a szervezet működését, és ebbéli törekvése aligha volt független a Trump-kormány azon gyakorlatától, mellyel igyekezett minél szélesebb körben leépíteni országa nemzetközi kötelezettségvállalásait. [14]

De nemcsak Donald Trump adminisztrációjának döntése miatt csökken folyamatosan az ENSZ békefenntartásra költhető összege. Kihasználva az elnök akcióját, más nagyhatalmak is vonakodnak megadni a korábbi támogatási normát, másrészt katonákat se szívesen küldenek a békemisszió soraiba. Ennek az az oka, hogy több nagyhatalom, hogy saját befolyását is biztosítsa, inkább egyedül törekszik a béke megteremtésére, és az elmúlt időszakban, főleg a hidegháború megszűnésével felértékelődtek a regionális és kontinentális összefogások. Ezek közé sorolandók a NATO által indított akciók, de az Afrikai Unió is részt vesz a Száhel-övezet stabilizálásában, és az Európai Unió is egyre gyakrabban lép fel békefenntartói szerepben. Másrészt a legjelentősebb gócpontokban, például a Közel-Kelet szír és izraeli-arab konfliktusaiban a térségben szerepet játszó erők és a nyugati hatalmak inkább saját hadseregeik egységeit használják, mivel ezzel növelni lehet az adott terület stabilitását. Érzékletes szám, hogy 2015 óta az ENSZ kötelékébe tartozó békefenntartók száma 90 ezerről 20 ezerre csökkent. A folyamatok pedig bizonyosan nem fognak itt megállni. [15]

Ezzel kapcsolatban nem érzékelhető a közvélemény részéről sem pozitív szolidaritás, amely megfontolásra késztetné a politikusokat. Ez pedig abból adódik, hogy az ENSZ

sokszor megmutatta, képtelen fenntartani a békét. Bár a szervezet megkapta a Nobel-békedíjat, de a Szovjetunió összeomlását követő háborúkban és polgárháborúkban betöltött szerepük rávilágított, mennyire erőtlenek. A srebrenicai mészárlás, a ruandai genocídium, vagy éppen a Mogadishuban elkövetett tömeggyilkosságok mind annak a bizonyítékai, hogy a békefenntartók, akik a helyszínen voltak, nem tettek semmit, hogy megakadályozzák az eseményeket. Jugoszlávia, Szomália és Ruanda a mai napig fontos szimbólumok: a nagy elvárásokkal induló békefenntartó mozgalom ezekben az országokban és régiókban mutatott teljesítménye alapján vált mára mellőzötté. Jelenleg a leginkább a Szahara déli, délkeleti régióiban, illetve Délkelet-Ázsiában teljesítenek szolgálatot a kékkabátosok.[16]

A békefenntartók helyzetét tovább nehezítette a koronavírus megjelenése és globális terjedése. Egyrészt ez hátráltatta a műveletek pontos és következetes végrehajtását, másrészt tovább csökkentette a multilaterális kapcsolatokat. A globális pandémia, amely végigsöpört a fejlődő világon is, arra kényszerítette az ENSZ vezetését, hogy lépéseket hozzon. António Guterres főtitkár a harcoló feleket arra kérte, hogy szüntessék be a fegyveres összetűzéseket, és inkább koncentráljanak a járvány megfékezésére. Ennek érdekében a békefenntartók rotálása sem valósulhatott meg, ezt három hónappal el kellett csúsztatni, hogy ne terjesszék a fertőzést, nem vehetett részt több kékkabátos a missziókban, másrészt részt kellett venniük más nem kormányzati szervezetekkel a humanitárius akciók szervezetésében. További biztonságot csökkentő tényező, hogy a kevesebb békefenntartó nem tudja távoltartani az ellenséges feleket, akik között vannak olyanok, akik úgy gondolják, hogy a vírus okozta helyzetet ki tudják használni saját befolyásuk növelésére, ezért összecsapásokat provokálnak az ellenségeikkel.[17]

Várhatóan a járvány végeztével sem érnek véget ezek a konfliktusok, sőt fokozódhatnak. Az IMF számításai szerint a járvány világgazdaságra gyakorolt hatása hozzávetőleg három százalékos gazdasági visszaesést prognosztizál, amely ezeken a területeken hatványozottan fog jelentkezni, ez pedig újabb fegyveres harcokat generálhat. Ezzel egyidőben az egyes államoktól érkező juttatások is csökkenhetnek, hiszen minden ország saját egészségügyének és gazdaságának újraindítására fog törekedni, és nem az ENSZ támogatását fogja prioritásként kezelni. Másrészt a bezárások és a távolságtartás azt jelentette sok ország számára, hogy ezeket a problémákat csak egyedül, vagy regionális együttműködésben tudják megoldani, és mivel a gyors terjedés egyik okának a globalizációt jelölték meg, a jövőben többen is próbálják gyengíteni a multilaterális kapcsolatokat. [18] Nem segíti, hogy a világjárvány kitörése óta a WHO, amely az ENSZ egyik szervezete, teljesen inkompetens volt, nem tudott hatékony válaszokat kialakítani a krízisre. Egy példát hoznék csak: a WHO vezetője dicsérte a kínai fellépést, miközben más források szerint a kínaiak kozmetikázott adatokat közöltek. [19]

Az mindenesetre tény, hogy az ENSZ Biztonsági Tanácsa csak hosszas késlekedés után szólalt meg – 2020 áprilisában – a világjárvány ügyében, egy globális videokonferencia keretében, [20] feltehetően nem függetlenül attól, hogy Trump elnök bejelentette, tanulmányozzák annak lehetőségét, hogy az Egyesült Államok felfüggessze a WHO-nak nyújtandó támogatást. [21]

A nemzetközi szervezetnek segíthet, hogy 2021. január 20-án beiktatták hivatalába Joe Biden elnököt, aki arra készül, hogy visszavonja elődjének számos intézkedését, így például egyik első intézkedéseként már alá is írta országa párizsi klímaegyezményhez való visszatéréséről szóló rendeletet [22]

ZÁRÓ GONDOLATOK

Egyetértek Ayodeji Bayo Ogunrotifa-val, aki szerint a szuperhatalmak összefogása, elköteleződése, tenni akarása sikerre vihetné a békefenntartó akciókat úgy, hogy politikai és gazdasági érdekeiket félreteszik egy jobb ügy érdekében. [23] A napjainkban tapasztalható realitás ezzel szemben az, hogy az ENSZ olyan szerkezeti és politikai fragmentáltsággal küzd, amelyet valóban csak radikális reformokon keresztül lehetne legyőzni. A reformjavaslatok kronologikus sorban való megjelenítése, s elemzése arra mutatott rá, hogy az ENSZ-műveletek politikai és anyagi támogatása nélkül szinte tehetetlenné válik a szervezet. Nemcsak azért, mert a Biztonsági Tanácsban egy tagország vétója is elég ahhoz, hogy egy egész javaslatot elvessenek, hanem azért is, mert jól láthatóan az Egyesült Államok pénzügyi hozzájárulása nélkül egyre nehezebbé válik a konfliktusos területeken zajló békefenntartó akciók támogatása. Kutatásom azt is világossá tette, hogy az ENSZ-t számos kritika érte „tehetetlensége" miatt, valamint azért is, mert olyan események fölött hunyt szemet például, mint a ruandai népírtás. Véleményem szerint a szervezet strukturális átszervezésével, a vétójog átgondolásával, a pénzügyi hozzájárulások stabilizálásával, a békefenntartó műveletek céljainak pontos meghatározásával, a műveleti környezetek stabilizálásával olyan pozitív változásokat lehetne elérni, amelyek mindenképp sikerre vihetnék az ENSZ működését.

FELHASZNÁLT FORRÁSOK

[1] United Nations Peacekeeping, „Global peacekeeping data." 2020. Forrás: https://peacekeeping.un.org/sites/default/files/peacekeeing_factsheet_12_2020_english_1.pdf (letöltés ideje: 2021.01.22.)

[2] United Nations Foundation, „7 key facts about UN peacekeeping." Forrás: https://unfoundation.org/blog/post/7-key-facts-un-peacekeeping/ (letöltés ideje: 2019.05.27.)

[3] Szenes Z., Apáti Z., Drót L., „Jubileumi évfordulók: ENSZ-békefenntartás és a magyar honvédség." Honvédségi Szemle, 2019/1. szám, pp. 21-22.

[4] R. Mcentee, „Criticism Of The United Nations." Forrás: http://www.lovearth.net/criticismoftheunitednations.htm (letöltés ideje: 2019.05.27.)

[5] H. Buckley, „A critique of the United Nations Security Council." Fordham Political Review, 2013. Forrás: http://fordhampoliticalreview.org/a-critique-of-the-united-nations-security-council/ (letöltés ideje: 2019.05.27.)

[6] H. Buckley, „A critique of the United Nations Security Council." Fordham Political Review, 2013. Forrás: http://fordhampoliticalreview.org/a-critique-of-the-united-nations-security-council/ (letöltés ideje: 2019.05.27.)

[7] S. Sengupta: „The United Nations Explained: Its Purpose, Power and Problems." New York Times, 2017. Forrás: https://www.nytimes.com/2017/09/17/world/americas/united-nations-un-explainer.html (letöltés ideje: 2019.05.27.)

[8] F. Haass, N. Ansorg, „Better peacekeepers, better protection? Troop quality of United Nations peace operations and violence against civilians." Journal of Peace Research, Vol. 55, Iss. 6, 2018. pp.756-757.

[9] Szenes, Apáti, Drót (2019) i.m. pp. 16–19.

[10] Szenes, Apáti, Drót (2019) i.m. pp. 23–24

[11] L. M. Goldberg, „UN Peacekeeping Faces Massive Funding Shortfall. UNDispatch", 2019. Forrás: https://www.undispatch.com/un-peacekeeping-faces-massive-funding-shortfall/ (letöltés ideje: 2019.05.28.)
[12] J. Guy, R. Richard, „UN warns that staff could go unpaid next month as member states fail to pay dues." 2019.10.09. Forrás: https://edition.cnn.com/2019/10/09/world/un-budget-crisis-scli-intl/index.html (letöltés ideje: 2012.01.22.)
[13] G. Wilson, „The US plays a unique role in UN solvency." November 14, 2019. Forrás:https://qz.com/1746703/without-us-funding-the-un-budget-crisis-will-hurt-africa-most/ (letöltés ideje: 2021.01.22.)
[14] E. Watkins, „Haley touts reduced UN budget." 2017.12.26. Forrás: https://edition.cnn.com/2017/12/26/politics/nikki-haley-un-budget/index.html (letöltés ideje: 2021.01.22.)
[15] P. Hille, „UN peacekeepers: Numbers are going down" DW. Forrás: https://www.dw.com/en/un-peacekeepers-numbers-are-going-down/a-53603652 (letöltés ideje: 2021.01.04)
[16] Ibid
[17] T. Buitelaar, D. den Dunnen, D. Salama, „The impact of the corona virus on UN peacekeeping at the field, state, and global level." The Hague University. Forrás: https://www.thehagueuniversity.com/about-thuas/thuas-today/news/detail/2020/06/15/the-impact-of-the-corona-virus-on-un-peacekeeping-at-the-field- state-and-global-level (letöltés ideje: 2021.01.04.)
[18] Ibid
[19] N. P. Walsh, „The Wuhan files. Leaked documents reveal China's mishandling of the early stages of Covid-19." CNN.com. Forrás: https://edition.cnn.com/2020/11/30/asia/wuhan-china-covid-intl/index.html (letöltés ideje: 2021.01.04.)
[20] UN.org, „Secretary-General's remarks to the Security Council on the COVID-19 Pandemic."09 April 2020. Forrás: https://www.un.org/sg/en/content/sg/statement/2020-04- 09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered (letöltés ideje: 2021.01.22.)
[21] MTI/Népszava, „Donald Trump kijelentette, hogy tanulmányozzák a WHO-nak nyújtott támogatás felfüggesztését." 2020.04.08. Forrás: https://nepszava.hu/3073839_donald-trump-kijelentette-hogy-tanulmanyozzak-a-who-nak-nyujtott-tamogatas-felfuggeszteset (letöltés ideje: 2021.01.22.)
[22] MTI/Hvg.hu, „Biden azonnal munkához látott, már a klímaegyezmény, a bevándorlás és a koronavírus miatt is intézkedett." 2021.01.21. Forrás:https://hvg.hu/vilag/20210121_joe_biden_bevandorlas klimaegyezmeny koronavirus (letöltés ideje: 2021.01.22.)
[23] O. Ayodeji Bayo, „The Factors Behind Successes and Failures of United Nations Peacekeeping Missions: A Case of the Democratic Republic of Congo." Journal of Alternative Perspectives in the Social Sciences, Vol. 3, Iss. 4, 2012. pp. 914-928.

SPREAD OF SNEEZING AND COUGHING IN A SUBWAY CAR

TÜSSZENTÉS ÉS KÖHÖGÉS TERJEDÉSE METRÓKOCSIBAN

HETYEI Csaba[1] – SZLIVKA Ferenc[2]

Abstract

Throughout human history, epidemics have occurred in many cases, which have also affected society and the economy. At the end of 2019, the COVID-19 or SARS-CoV-19 virus appeared and caused a pandemic in 2020, which resulted in unprecedented changes both globally and individually. In our article, we were analysing the spreading and evolution of a violent expiratory event (sneeze, cough) in a subway car. In our research, we followed a sneezed/coughed air using a computational fluid dynamics (CFD) software, thus it became visible in which directions the coughed volume spreads. Using our results, passengers' sense of security can be increased, therefore if someone sneezes in the studied subway car, the passengers can decide that the sneezing is a real risk of infection for them or not.

Keywords

CFD simulation, Coughing and sneezing, COVID, Health security, Public transportation, Traffic safety

Absztrakt

Az emberiség történelme során számos esetben előfordultak járványok, melyek hatással voltak a társadalomra és a gazdaságra is. 2020-ban a 2019-es év végén megjelenő COVID-19, azaz a SARS-CoV-19 vírus okozott világjárványt. A 2020-as pandémia eddig nem látott világméretű járványügyi intézkedéseket eredményezett, mely az országok és az egyének életét is nagyban befolyásolták. Cikkünkben egy erőteljes légúti kilégzést (tüsszentés, köhögés) terjedését vizsgáljuk Budapest egyik legnagyobb lélekszámban használt közlekedési eszközén, az M3-as metró egyik kocsijában. Kutatásunk során egy numerikus áramlástani szoftver segítségével feltérképeztük a kiköhögött/kitüsszentett levegő útját, így láthatóvá vált, hogy mely irányokba terjed a kitüsszentett levegő. Eredményeinket felhasználva az utazók biztonságérzete növelhető így, ha a metrókocsiban valaki tüsszent, az utazók eldönthetik, hogy az a tüsszentés valós fertőzésveszélyt jelent-e számukra.

Kulcsszavak

CFD szimuláció, COVID, Egészségbiztonság, Köhögés és tüsszentés, Közlekedésbiztonság, Tömegközlekedés

[1] hetyei.csaba@uni-obuda.hu | ORCID: 0000-0003-2915-4540 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szlivka.ferenc@bgk.uni-obuda.hu | ORCID: 0000-0002-3298-4142 | professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

Thought the human history, there have been pandemics, which was a biological thread for mankind. In the last centuries, the pandemics were endangering the whole world due to the word trade and tourism. Epidemics in addition to human lives can cause economic crises [1], the developing and the slow responding countries are in the greatest danger [2]. In our modern days, the pandemics also can cause panic and anxiety in thwe individual's life both in the real and in the virtual life [3]. In the last decades, the diseases were able to travel around the world in a few days by infected peoples. Just to mention a couple of diseases from the last two decades which hit mankind: SARS in 2003, H5N1 in 1997 and 2005, H1N1 in 2009, MERS in 2012, Ebola in 2014 and right now with COVID-19 (SARS-CoV-2) which started to spread at the end of 2019 [4].

The first mathematical model for the infectious disease was made by Daniel Bernoulli in 1760 for the spread of smallpox [5], with time in 1927 William Ogilvy Kermack and Anderson Gray McKendrick published their epidemic model [6]. The compartment model of Kermack and McKendrick contained the SIR notations, where S is susceptible, I is infective and R is removed or recovered class. By this model, when a member of the S class is infected, it is going to the infected (I) group, when this individual cured, he is going to the R stock, where he has immunity against the pathogen. The SIR flow can see in Figure 1.

Figure 1. The flow of the SIR model

The mathematical description for the SIR model was presented 1932 [7] and 1933 [8] by Kermack and McKendrick with the following equations:

$$\frac{dS}{dt} = -\frac{\beta \cdot S \cdot I}{N}$$

$$\frac{dI}{dt} = \frac{\beta \cdot S \cdot I}{N} - \gamma \cdot I$$

$$\frac{dR}{dt} = \gamma \cdot I$$

$$R_0 = \frac{\beta}{\gamma}$$

In the previous equations and Figure 1, *S*, *I* and *R* are the previously introduced susceptible, infective and removed or recovered compartments, *N* is the sum population of these three groups, R_0 is the initial number or the R class, β is the transmission rate and γ is the removal rate.

The SIR model is a simple form of a disease transmission when the member of the population can infect only once. In this case, if the R_0 is less than 1, the herd immunity may develop and the disease dies out, if R_0 is more than 1, the epidemic is spreading [9]. For different diseases different infection types exist, which can describe with the S, I and R

classes, e.g., SIS, is when the patent is cured of the infection and he can become newly infected, or extending the model with the D, E and M classes, where D is the deceased class, E, the exposed class, when there is an incubation period between the infected and the infectious condition and M is the materially-derived immunity class [9].

For decreasing the infections, in the metric word generally the 1.5 meters social distance is the required [10], in the regions where the imperial system is used, usually the safe distance is 6 feet (1.8 meters) [11], while the WHO suggest at least 1-meter distance [12]. The origin of the safety gap was made by Carle Flügge in 1897 who found the most of the large droplets expelled from the nose and mouth fell to the ground within 3 to 6 feet of the person with infection [11]. Since Flügge, researchers have begun to study the diseases transmission mechanism, for easier and more precise understanding its physics and they are arranged the droplets by their sizes. The "large droplet" transmission route is when the target tissue has direct contact with the pathogen-bearing droplets, the "small droplets" and the airborne transmission is an indirect contact via inhalation of pathogen-bearing droplets. Generally, the size association for the "small" droplets are droplet nuclei which can form from via evaporation and they diameter are less than 5 μm, when the diameter of the droplet is between 5 μm and 10 μm they are respiratory droplets, if the droplet size is more than 10 μm they are "large" droplet [13]. Approached from elsewhere the "large" droplets are settling by gravity and the small droplets are not [14].

Fluid dynamic studies shown the cloud of the violent respiratory events (sneeze and cough) are multiphase turbulent flows and they are traceable with schlieren optics. Lydia Bourouiba *et al.* [15] was observed the evolution of a respiratory event with a high fps camera, which is shown in Figure 2.

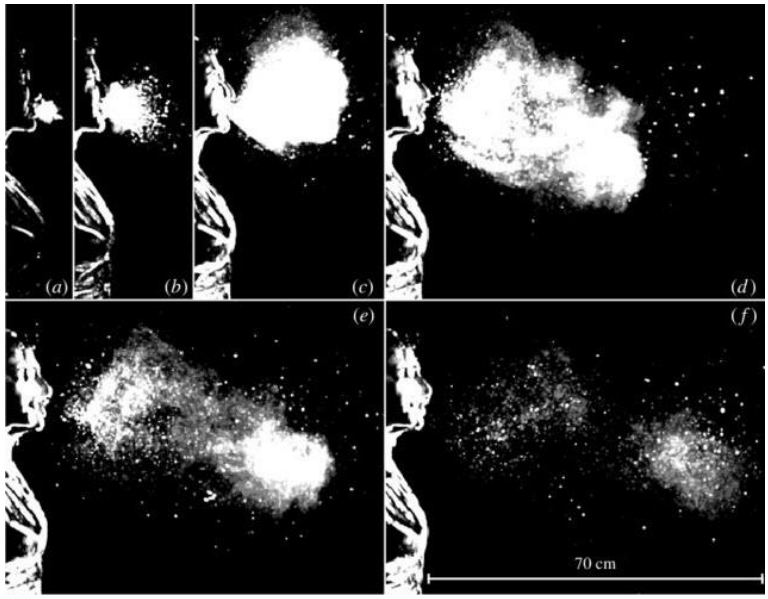


Figure 2. Sneezing in different time moments, a, 0.006 sec; b, 0.029 sec; c, 0.106 sec; d, 0,161 sec, e, 0.222 sec and f, 0.341 sec [15]

The schematic evolution of a respiratory event by Bourouiba *et al.* [15] shown in Figure 3.

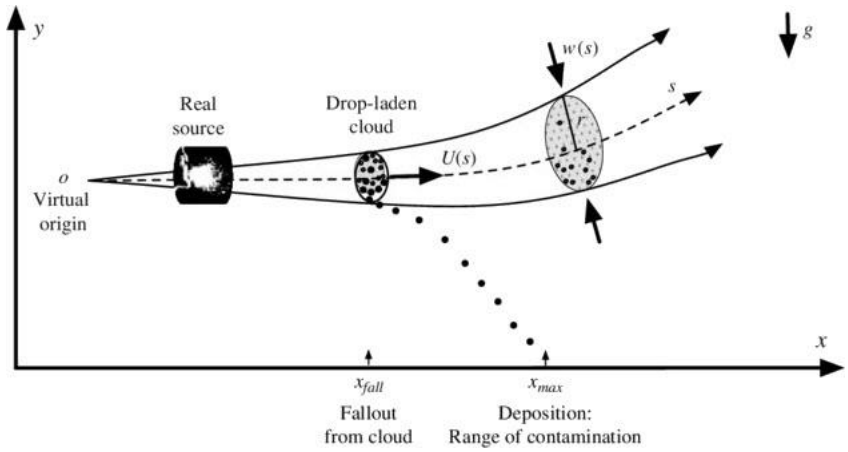


Figure 3. Evolution of a sneeze or cough [15]

On the previous figure, we can observe a virtual origin where a sneeze or cough starts, then its exit on a real source (nose and mouth), then with distance, the large droplets starts to fall out from the cloud, the small droplets which remain in the puff of moist by the buoyant force start to rise, until they evaporate. During the lifetime of a cough, the puff cloud has a self-similarity describe by the plume theory [16, 17], and represented in Figure 3. with the expanding envelop curve.

Lydia Bourouiba *et al.* [15] using their images and the existing knowledge, they created both discrete and continuous fallout models for different particle sizes and they were compared against experimental results which showed a good match. The particle size distribution can depend on the sneezing speed and its humidity. A droplet size distribution for a cough is shown in Figure 4.

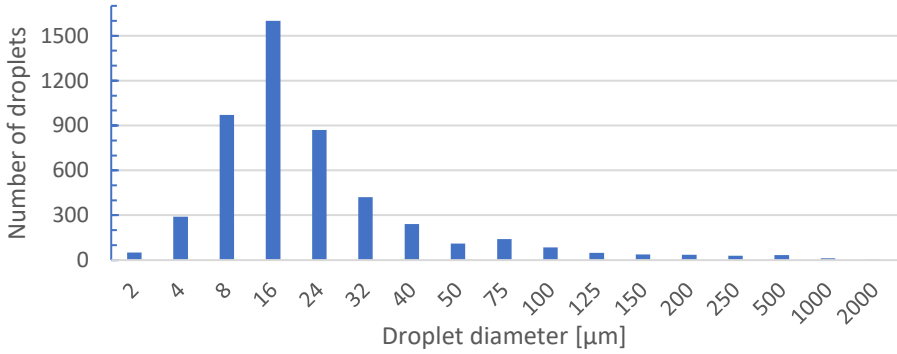


Figure 4. Droplet size distribution [18]

During the evolution of a sneeze or a cough the unsteady fluid fragmentation occurs due to the hydrodynamic instabilities, e.g. Kevin – Helmholtz type instability appears when

there is differential of speed at interfaces, Plateau – Rayleigh type instability driven by surface tension or Reyleight – Taylor instability which is the result of different fluid densities. Due to the instabilities, the fluid sheet of the wet cough fragments into rim, then ligament and to droplets [19, 20], hench viruses and other pathogens do not settle, due evaporation they can travel farther and they can stay in the air for a longer time.

Using a mask can protecting us and others to reducing exposed droplets. The used mask quality can depend on its manufacturing technology, e.g. for the N95 mask the requirement is filtering at least 95% of solid and liquid aerosols. Researchers from Wake Forest Institute for Regenerative Medicine tested 13 different design from approximately 400 masks made by community volunteers. They find the worst cloth mask filtered 1% of the particles and the best cloth mask performed with 79% filtration, the industrial made surgical mask achieved 62-65% filtration and the best N95 mask had 97% [21]. Examining the best performing masks researchers from Sydney [22, 23] and Duke [24] find similar results than the researchers from the Wake Forest Institute, the higher filtration level comes with the two or more layers, they have a tight weave and they made of heavyweight cotton fabric. The best-performing industrial masks are the N95, and the other respirator masks e.g. FFP2, KN95, P2, KF94, etc. [25] which are critical supplies for the healthcare workers, therefore the general recommendation is for the people to wear cloth mask in public with social distancing [26]. Researchers also find, the aerosol production during speech is more when we use plosive consonants like “p” “b”, and it is less when we use milder consonants like “m”. They also find the droplet quantity can be reduced with lip balm [27]. A comparison between the produced droplets of speaking, sneezing, and coughing with and without covered mount shown in Figure 5.

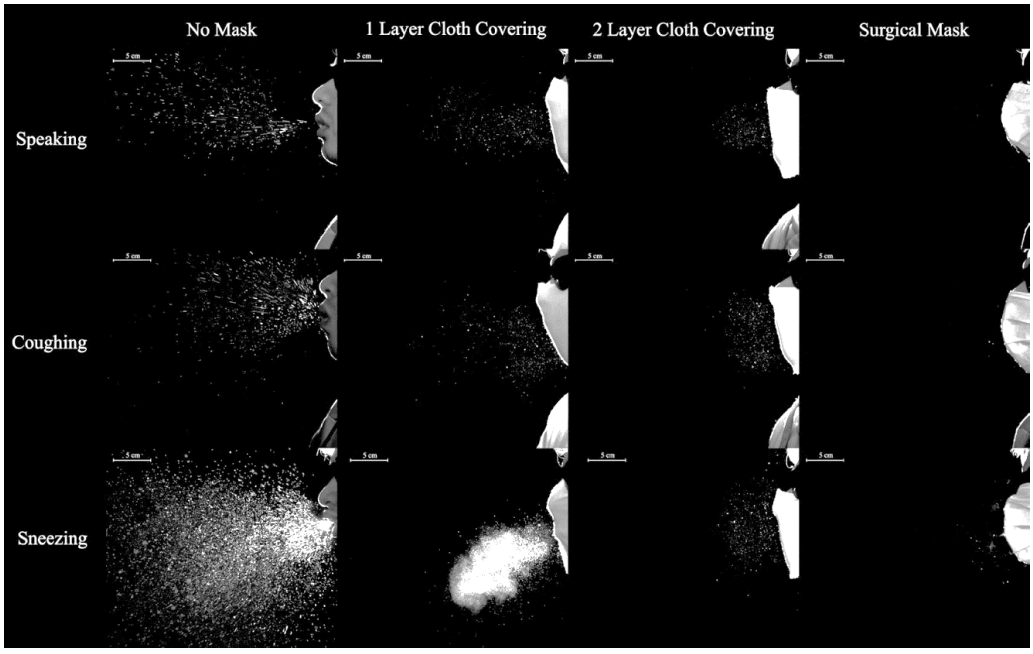


Figure 5. Droplet comparison for speaking, coughing and sneezing, without a face mask, with covered face by 1 and 2 layer cloth and by surgical mask [22]

The key factor of the droplet filtering is to use properly the face mask. The mask should cover the mouth and the nose, and it should fit tightly to the face. In any hole between the face and the mask the droplets could exit, and it can infect others. The outlet flow from a mask [28] is shown in Figure 6.

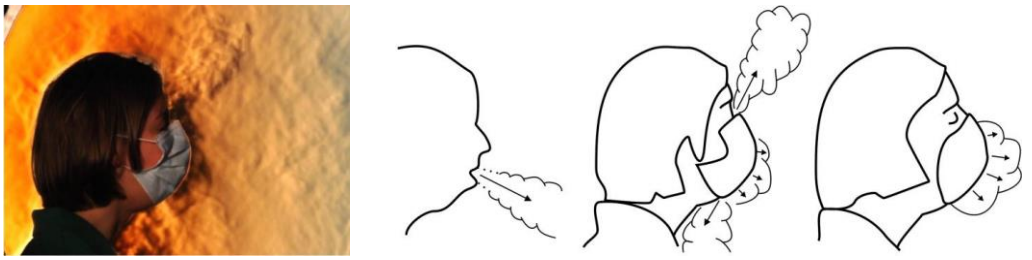


Figure 6. Outlet flow from a facemask captured by schlieren optic and a schematic image for cough spreading without a face mask and with different face masks [28]

MOTIVATION

In Budapest the Metro Line 3 or shortly the M3, before its renovation (November 2017), it has the highest transport capacity in peak hours (26 326) and the highest passenger number in peak hours (17 300), in addition to the greatest traveller number, it has the longest line (17.06 km) and the largest number of stations (20) [29].

While using the subway, the passengers may feel less safe during the viral period, and if someone sneezes, it can cause panic among passengers. Our goal to simulate a sneeze or a cough in a subway car and visualize its path and for reducing anxiety and increase travel security.

For creating the worst-case scenario, we created a CAD model of the M3 train (shown in Figure 7) with passengers, wherefrom the simulation we used only one people, the others and the tubular handrail, was used just for visualization. The violent expiratory event happened in the "corner" of the subway car and it could spread harshly in just one direction. The sneeze or cough occur in a realistic way as passengers usually travel and are likely to sneeze, towards the inside of the metro and not longitudinally.

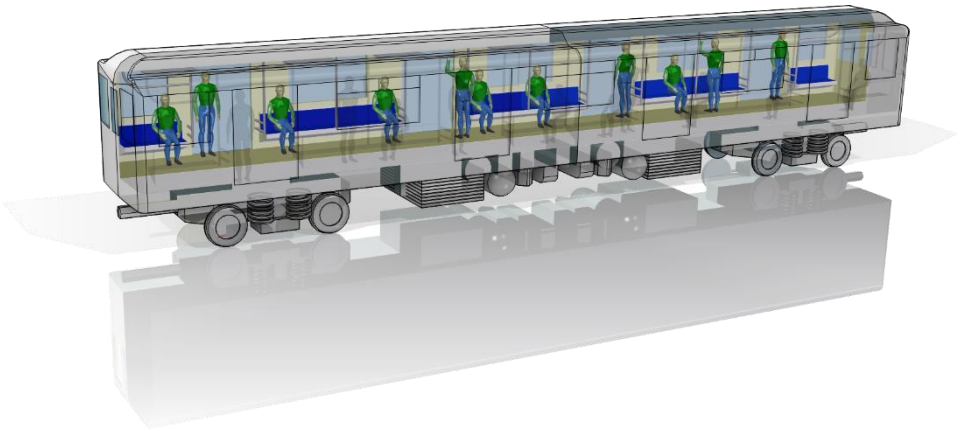


Figure 7. M3 metro train with travellers

For comparison, we were simulated cases both with and without a face mask, with and without AC (air conditioning), and with opened and closed windows. The estimated droplet route (yellow lines) and the opened and closed windows (inside the red rectangles) shown in Figure 8. We choose a detailed mannequin (shown in Figure 9) for the simulation, so its geometry provides more realistic results than an exaggerated man-like one, built of cylinders and rectangles.

For the simulation we would like to model and visualize just the fluid dynamic effects, therefore the particle deposition on the surfaces was not examined.

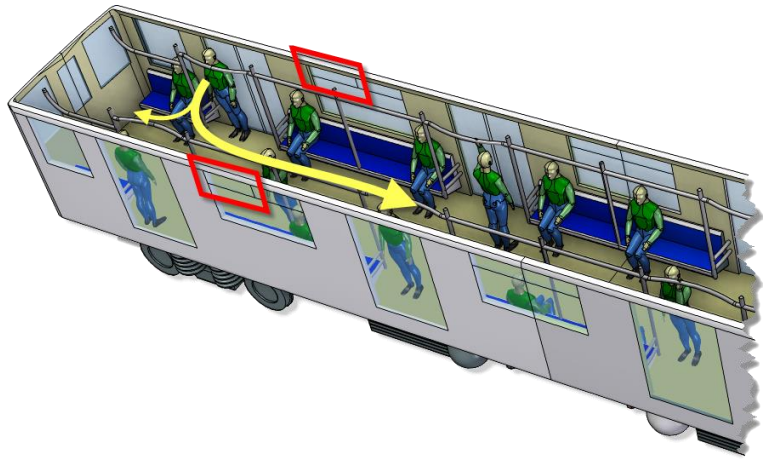


Figure 8. Estimated sneeze route and the opened/closed windows

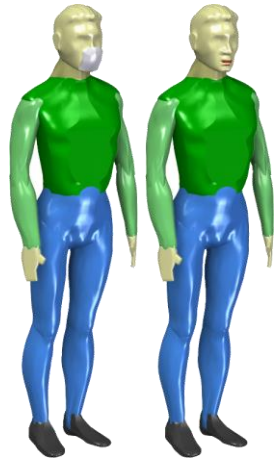


Figure 9. Mannequin with and without a face mask

FOUNDATIONS OF COMPUTATIONAL FLUID DYNAMICS

The computational fluid dynamics (CFD) simulation is a tool to mimic the physical world. For our research, we used a finite volume method (FVM) based CFD software, which method divides the computational domain into finite volumes, within it is using the continuity, momentum, and energy equations to compute the flow field's properties. Based on

the tree previous equations the FVM based CFD codes generally use the following transport equation:

$$\frac{\partial}{\partial t}\int_V U\,dV + \oint_A \underline{F}\,d\underline{A} - \int_V S_V\,dV - \oint_A \underline{S_A}\,d\underline{A} = R$$

In this equation, *V* denotes an arbitrary enclosed control volume, *A* denotes the surface of this control volume, *U* is a conserved quantity (e.g.: mass), *F* is the same quantity's flux over the *A* surface, S_V is the volumetric source of quantity *U* over volume *V*, S_A is the surface source of quantity *U* over surface *A*, and *R* is the error of the equation (residual).

The previous equation can be written for every cell of the mesh and solved in a system of equations. To do so, CFD codes utilise iterative methods that converge to a solution by reducing the residuals of the equations.

SIMULATION PROPERTIES

For simulation we used Mentor Graphics' frontloaded CFD software the FLOEFD integrated into Siemens' Solid Edge CAD software.

For the default fluid, we choose "Air" from FLOEFD's material database, the ambient temperature was 20.05°C and the environmental pressure was 1 atm (101 325 Pa). The gravity was defined in a downwards direction perpendicular to the floor. The sneezing mannequin body temperature was 38.3°C.

Due to the needed computational resource for the simulation, we cut the model in half, and the farther half was modelled with an environmental pressure boundary condition (BC), which can be both inlet and outlet depending on its environment.

When the windows were open, the speed of the external air was 8.5 $m \cdot s^{-1}$ (30.6 $km \cdot h^{-1}$), which is the average travel speed of M3.

When the AC (air conditioning) was running, the air enters into the computational domain with environmental temperature (20.05°C), with 0.5 $m \cdot s^{-1}$ speed, and with 50% relative humidity. The 0.5 $m \cdot s^{-1}$ airspeed is a twice than the recommended velocity [30], which we chose for faster air exchange, and the 50% of relative humidity is a recommended humidity value for ACs during the summer [30].

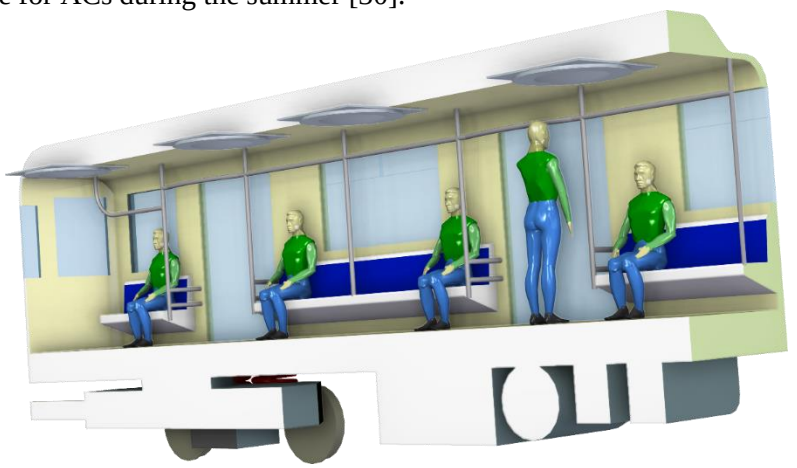


Figure 10. M3 metro train with ACs

For sneezing or coughing, we define a time-dependent volume flow BC, with 2, 4, and 5 litres total volume. We defined this value by the average human lung capacity, which is 6 litres for man and 4 litres for women [31]. The sneezing or coughing was simulated in a transient simulation with a trapezoid distribution within 0.25 seconds. For the volume flow of 5 litres coughed air, the sneezing function shown in Figure 11.

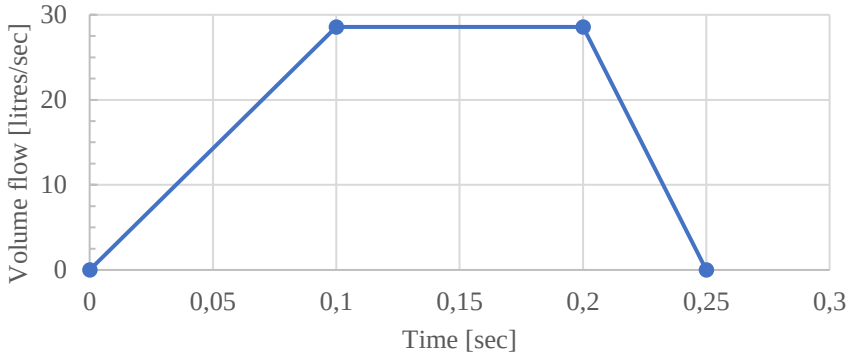


Figure 11. Sneeze distribution during the sneezing

The sneezing was starting at 1 second with 100% of relative humidity and with 38.3°C fluid temperature. For clarity, the density of the 100 % humid air is lighter than the dry air and it can be determined by the following formula [32]:

$$\rho_{humid\ air} = \frac{p_d}{R_d + T} + \frac{p_v}{R_v + T}$$

In the previous equation $\rho_{humid\ air}$ is the humid air density, p_d is the partial pressure of dry air, p_v is the pressure of water vapour, R_d is the specific gas constant for dry air, R_v is the specific gas constant for water vapour and T is the temperature. The $\rho_{humid\ air}$ for 20°C is 1.1936 kg m^{-3}, and 1.1215 kg m^{-3} for 35°C, until the density of the dry air is 1.2041 kg m^{-3} for 20°C and 1.1455 kg m^{-3} for 35°C.

The mask was an isotropic porous media with 0.5 porosity and with a linear pressure difference versus mass flow rate function.

For each case, we started the simulation in steady-state and it was running until the 3000th iterations. When the steady-state simulation terminated its values was transferred to a transient (time-dependent) simulation for initial value, which was running until 6 seconds.

In each simulation started with an initial basic mesh, which contains approx. 1.8 million cells, then it was refined with an adaptive mesh refinement algorithm until 3.3 million cells during the steady-state and time-dependent simulations. The refinements for steady-state occurs in every 500th iterations after the 1000th iteration, for transient it occurred at 0.4, 0.8, 1.35, 2, 3, 4.15, and 5 seconds. The initial mesh in the region of the mannequin shown in Figure 12.

In each simulation, the k-ε turbulence model was used with a two-scale wall function based on the Van Driest model.

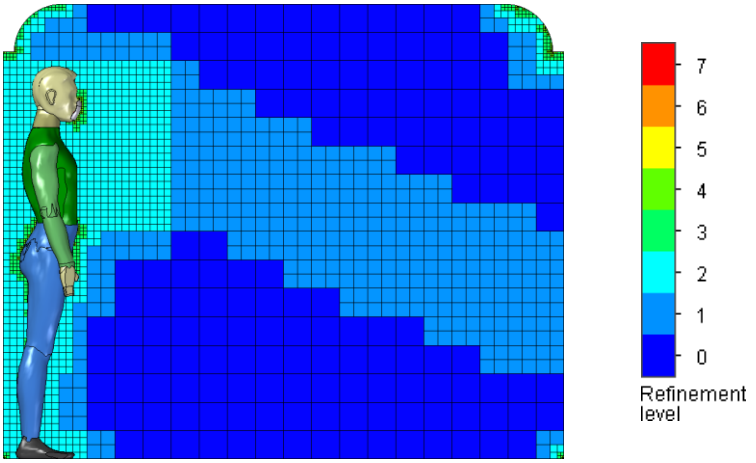


Figure 12. Initial mesh in the region of the mannequin

RESULTS

Before the results for clarity, the simulation was done with a finite volume method (FVM) based computational fluid dynamics (CFD) software, where the cough/sneeze was simulated with a continuum. By the used method we are able the represent the cough puff and its evolution due time, however, the particle-based approach and evaluation not feasible. If we would like to run the simulations with particle tracking a discrete element method based simulation approach is required, e.g. the SPH (smoothed particle hydrodynamics) method or an FVM based VOF (volume of fluid) method with a Lagrangian Multiphase (LMP) resolved transition model.

Each simulation approach has advantages and disadvantages, e.g. simulating the cough as a continuum benefit are lower computing resource requirements and the mathematical model for the porous media, which allows us to use a simplified mask geometry instead of modelling the real geometry of the mask without holes and porous channels. The particle-based approaches benefits are the cough or sneeze simulation with different particle sizes and with this method, the simulation with mask show a realistic result because its true geometry was modelled.

Summarizing the previous thoughts, the FVM based simulations without multiphase transition or any particle-based approach and with porous medium simplification the mask just a volumetric part which dissipates and slows down the flow depending by the pressure and volumetric flow rate of the cough. With this method, we can represent where the flow is able to go, and we are not able to simulate the filtering process of the face mask.

Our first simulation was a base study for comparison where the AC was off. In this case, the total volume of the mannequin's sneeze or cough was 5 litres and it is shown without a mask in Figure 13 and with a mask in Figure 14. In the following figures, the mass fraction of water is represented in the flow field. For the 50% humidity, the mass fraction of the water in the air is 0.0072422341 for 20.05°C, the 100% is 0.0145506907 for 38.3°C. In our figures, for representation, we chose the rendered volume limits to 0.007275 and 0.00735, and the colour chart limits to 0.0072 and 0.00775.

In this case, we were able to observe the sneeze spreading in time, while with a half-splitted isosurface plot we were able to see the internal flow of the sneeze.

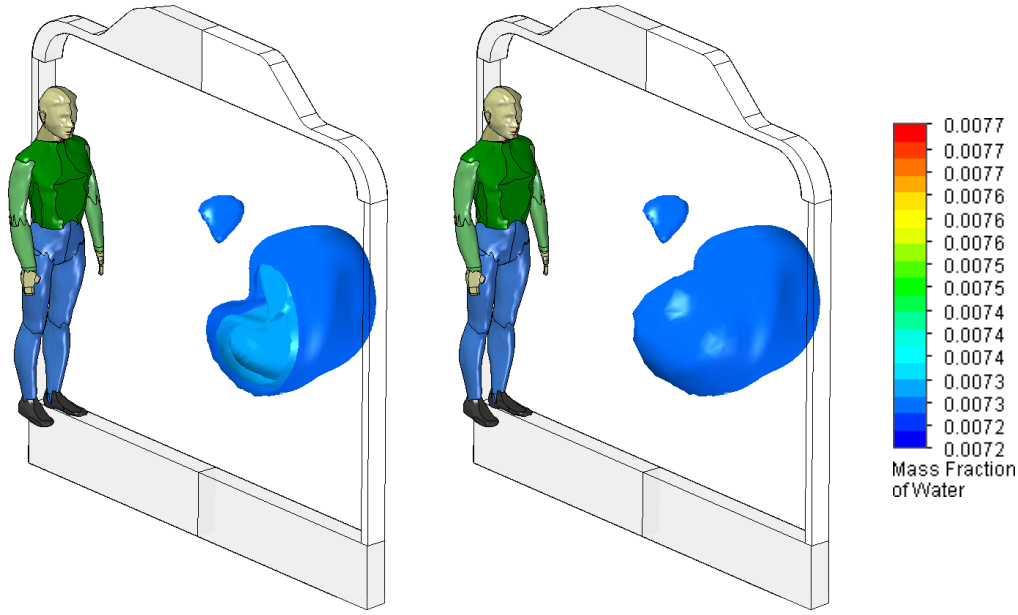


Figure 13. Sneeze spreading without AC and face mask after the sneezing with 5 seconds (the internal flow of sneeze showed in half-splitted plot and the whole in uncut)

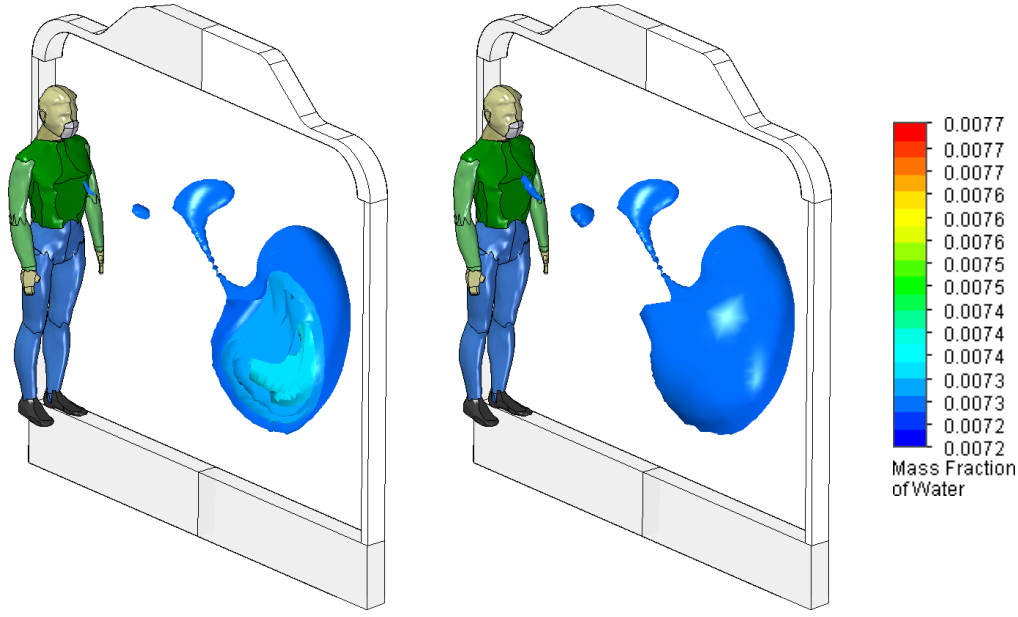


Figure 14. Sneeze spreading without AC and with face mask after the sneezing with 5 seconds (the internal flow of sneeze showed in half-splitted plot and the whole in uncut)

Comparing the results with and without a face mask, we observed on the case where the mannequin has no mask, the coughing cloud remain together as a *C* shaped wet cloud with a smaller bubble detachment. In the case where the mannequin has a mask, the *C* shape changed to an "italic" *O* shape with a tail, which is connected with the detached bubble.

The next simulation was running with AC, where the total volume of cough was 2, 4, and 5 litres. The result of the expiratory event is shown in the following figures (Figure 15, Figure 16, and Figure 17) with and without mask after 5 seconds of the cough or sneeze started.

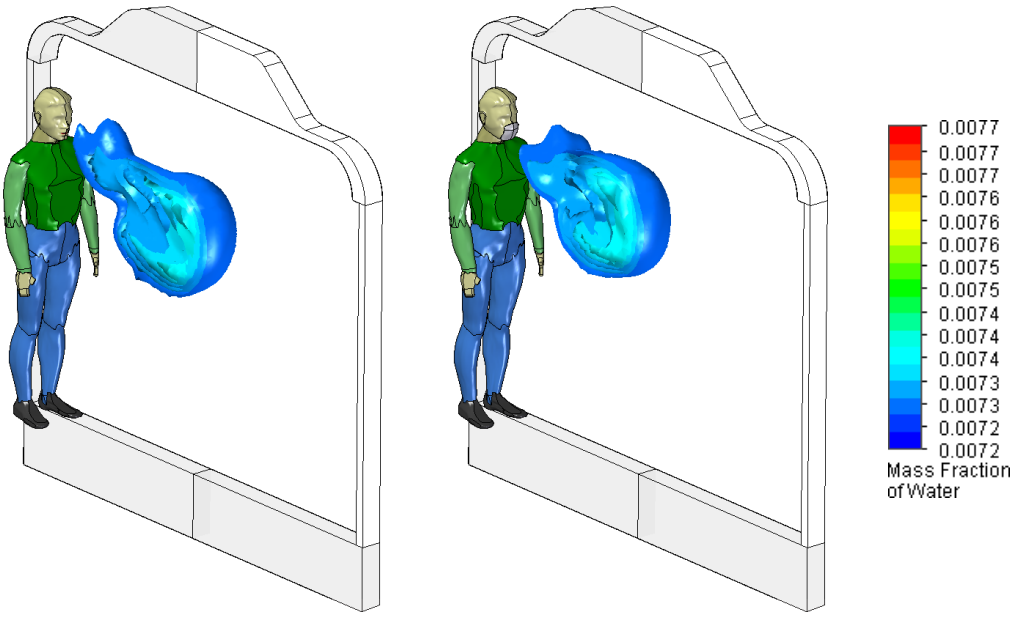


Figure 15. 2 litres of sneeze spreading with AC and without and with face mask after the sneezing started with 5 seconds (the sneeze was cut in the half for better representation for the internal flows)

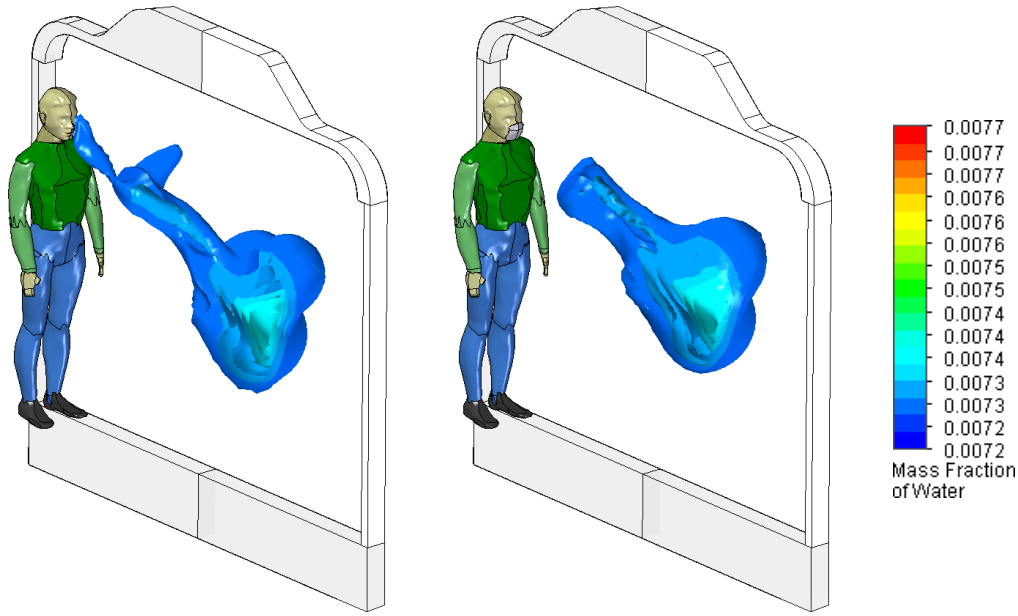


Figure 16. 4 litres of sneeze spreading with AC and without and with face mask after the sneezing started with 5 seconds (the sneeze was cut in the half for better representation for the internal flows)

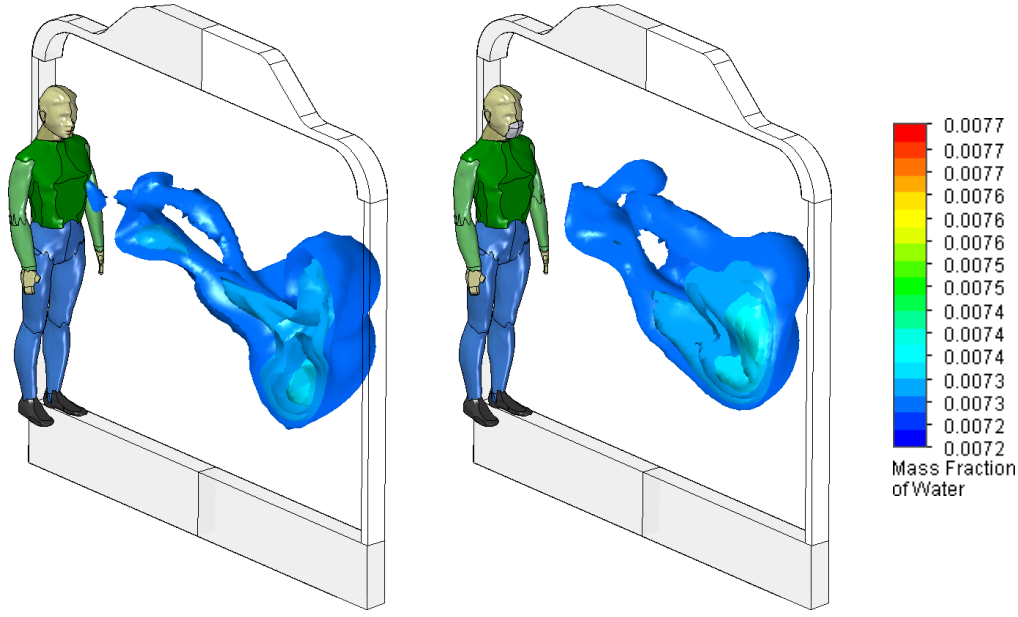


Figure 17. 5 litres of sneeze spreading with AC and without and with face mask after the sneezing started with 5 seconds (the sneeze cut in the half for better representation for the internal flows)

In this result, we were able to see a mushroom cloud shape, due to the ACs which has driven the sneezing forward and prevented its spread along the length of the subway. Other hands, we found in a small volume (2 litres) the sneeze shape remains spherical after 5 seconds of the sneeze started and it remains in front of the mannequin. In these cases, we found the puff clouds are longer and narrowed without a mask, because the cough enters into the computational domain without any slowing effect, therefore it has more kinetic energy and it can spread farther. In Figure 18, 0.75 seconds after the cough was ended the remaining cough can see near the mannequin face, without a mask, a small amount of water vapour remaining, while with a mask a larger amount of water vapour gets out of the mask.

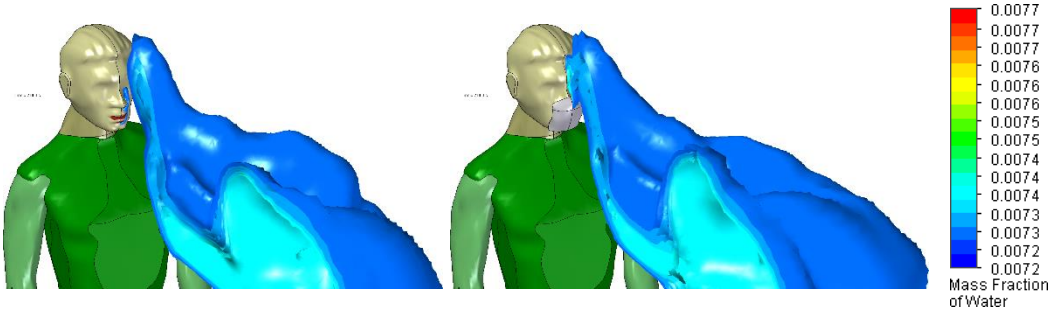


Figure 18. Sneeze spreading after the sneeze ended with 0.75 seconds without and with a mask

In the following figures the sneeze spreading shown with opened windows without and with a face mask.

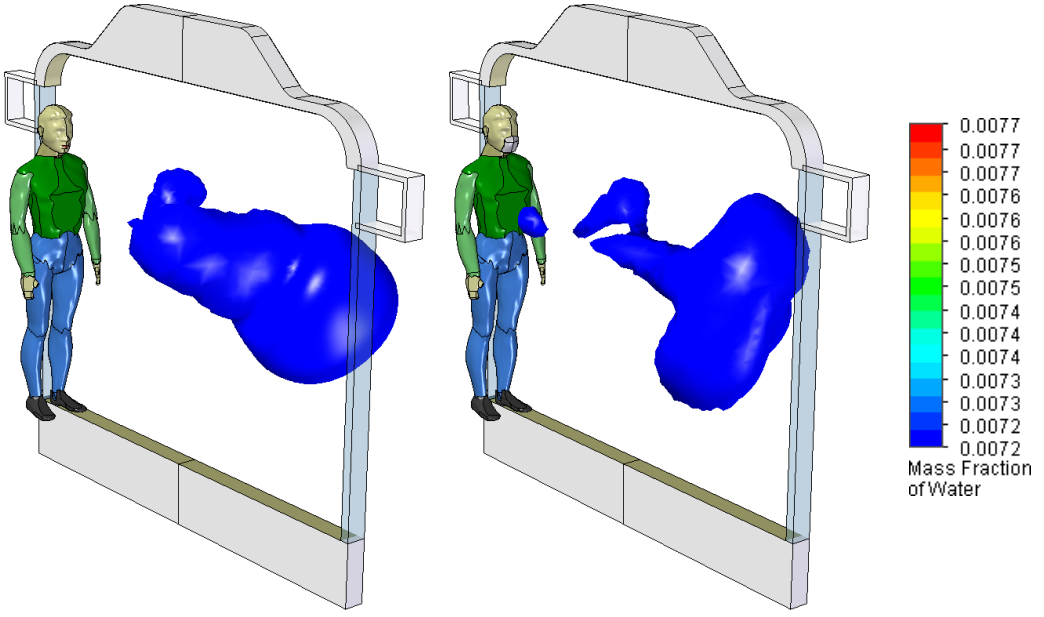


Figure 19. 5 litres of sneeze spreading with opened windows without and with face mask after the sneezing started with 5 seconds (isometric view)

In the previous figure the "usual" angle with the half splitted view does not represent well the sneeze, and it could be deceptive because the sneeze is highly unsymmetric. For better visualization, the sneeze is shown from two back views in the next two figures.

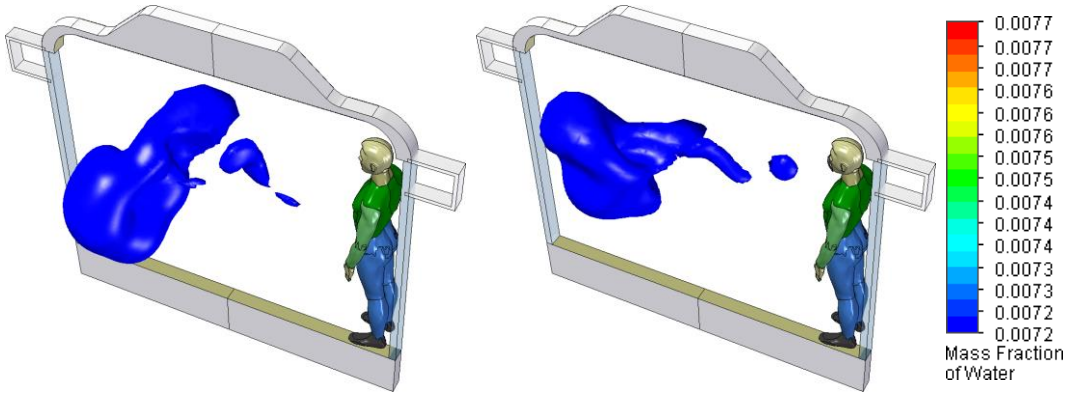


Figure 20. 5 litres of sneeze spreading with opened windows without and with a face mask after the sneezing started with 5 seconds (back view 1.)

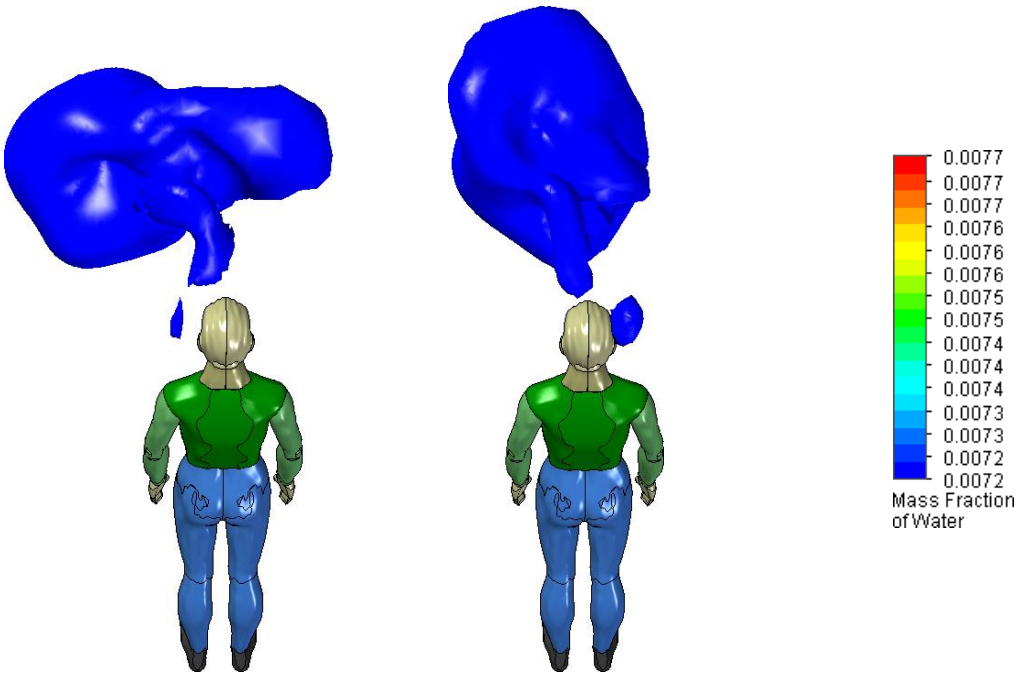


Figure 21. 5 litres of sneeze spreading with opened windows without and with a face mask after the sneezing started with 5 seconds (back view 2.)

In the case of open windows, the spatial extent of sneezing was greater to the sides than in the other cases. In these studies, the sneezing spread laterally, but its effect was much smaller than we expected. For better representation of this volume, the cough/sneeze with the travellers and with the subway car interior shown from front view in Figure 22 and Figure 23.

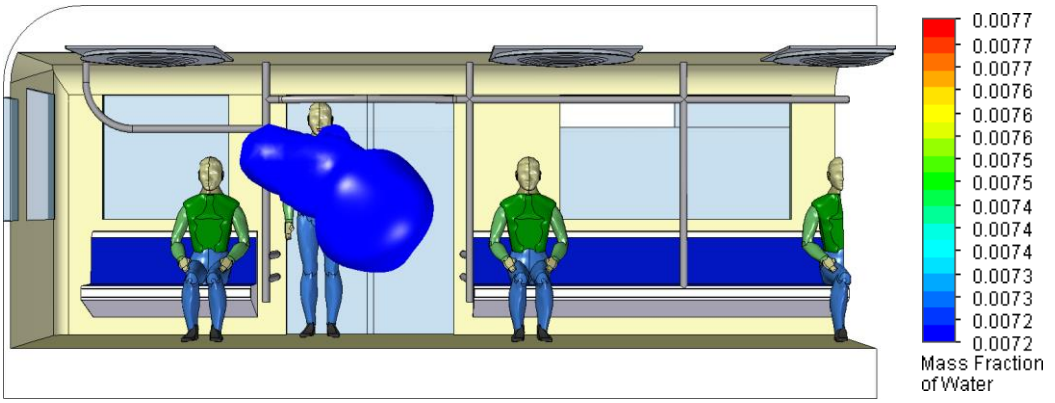


Figure 22. 5 litres of sneeze spreading with opened windows without a face mask after the sneezing started with 5 seconds (front view)

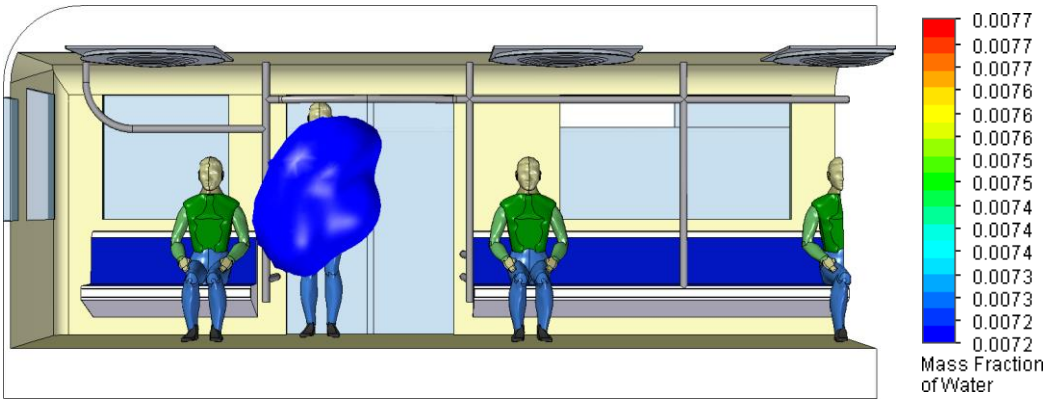


Figure 23. 5 litres of sneeze spreading with opened windows with a face mask after the sneezing started with 5 seconds (front view)

The following figures (Figure 24 and Figure 25) shown the cough/sneeze with streamlines.

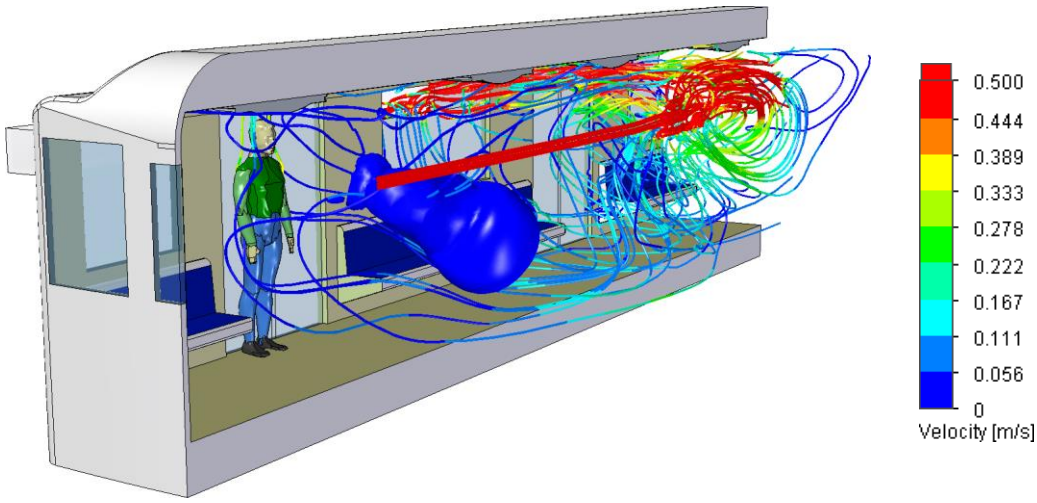


Figure 24. 5 litres of sneeze spreading with opened windows without a face mask after the sneezing started with 5 seconds (isometric view, with streamlines)

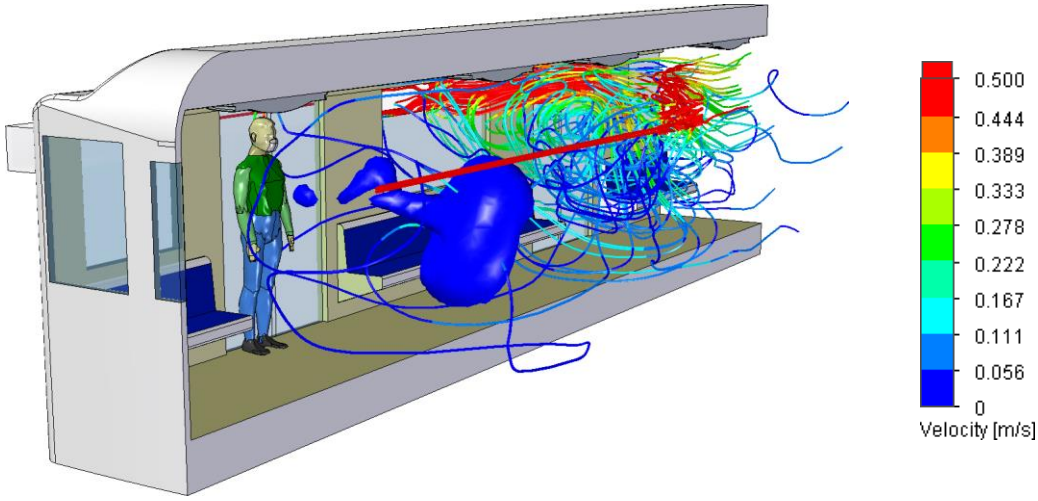


Figure 25. 5 litres of sneeze spreading with opened windows with a face mask after the sneezing started with 5 seconds (isometric view, with streamlines)

For the previous cases, the following figures (from Figure 26 to Figure 31) are showing the velocity fields.

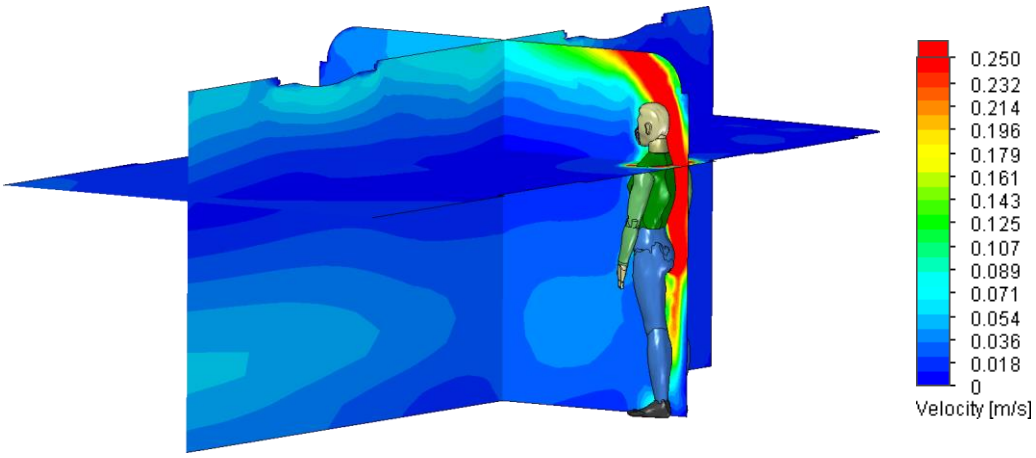


Figure 26. Velocity filed without AC (section views)

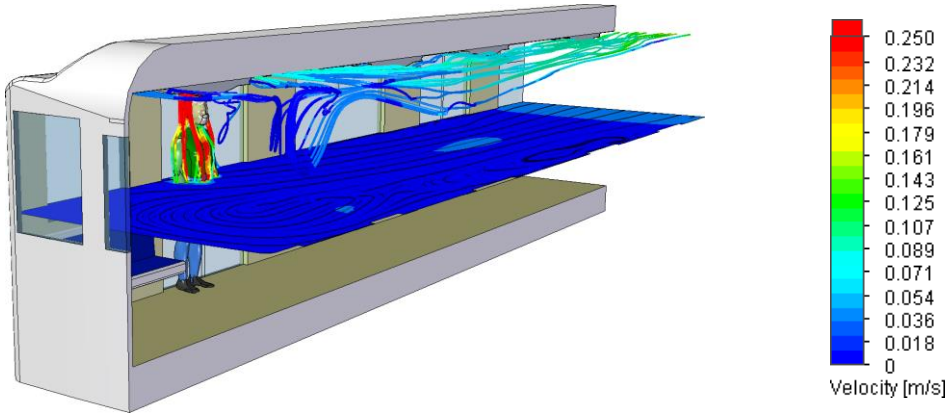


Figure 27. Velocity filed without AC (isometric view, streamlined from the mannequin)

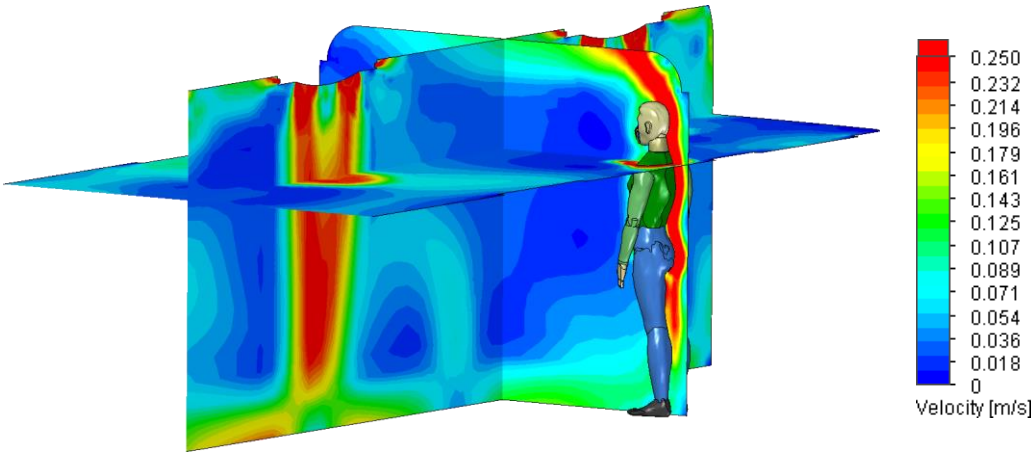


Figure 28. Velocity filed with AC (section views)

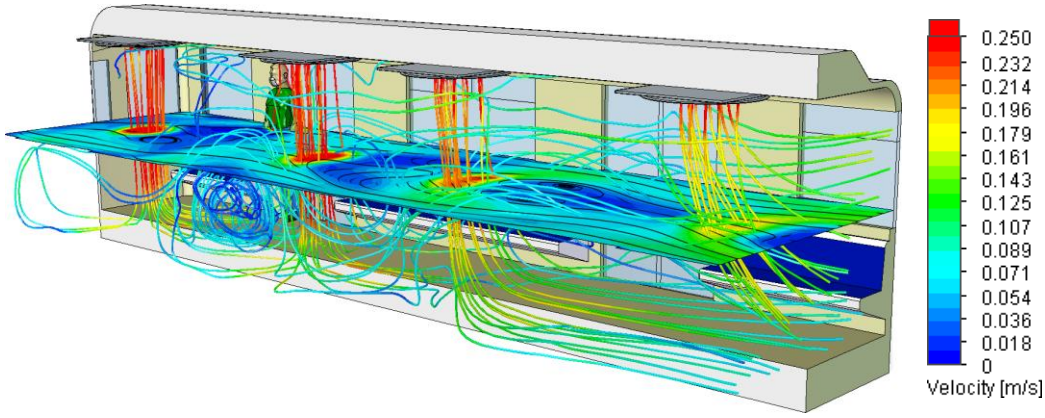


Figure 29. Velocity filed with AC (isometric view, streamlined from the ACs)

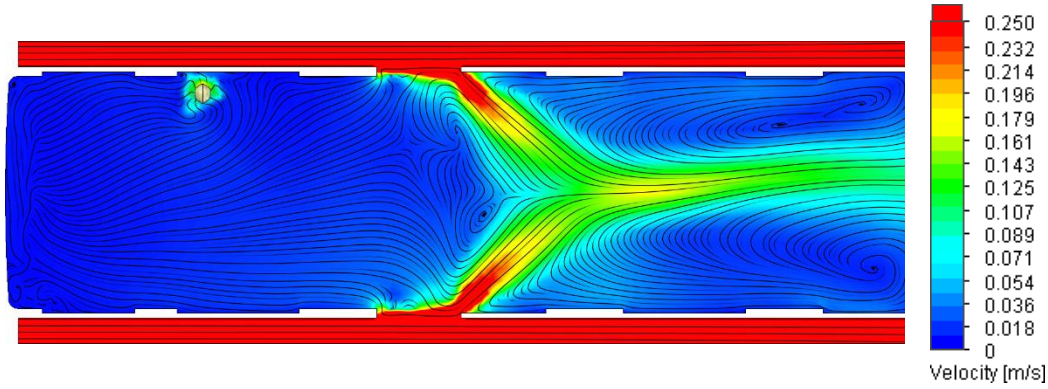


Figure 30. Velocity filed with opened windows (section view)

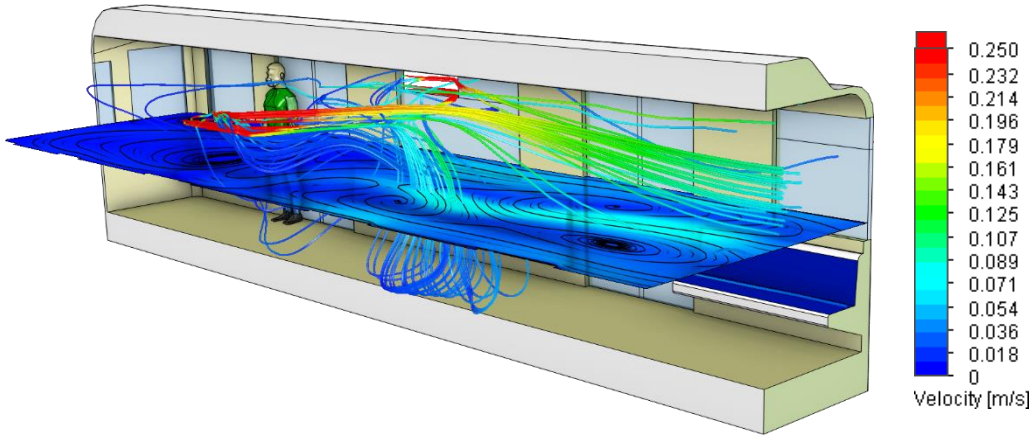


Figure 31. Velocity filed with opened windows (isometric view, streamlined from the "left" window)

In Figure 26 and Figure 27, where the AC was off and the windows were closed, we can see an almost non-moving, stationary air. In this case, the flow velocities were non zero, near the mannequin due to his body temperature and it was driven approx. a 0.075 m

s^{-1} airspeed near the ceiling and a 0.035 - 0.05 m s^{-1} airspeed at knee height in the middle of the seat next to the mannequin. In Figure 28 and Figure 29, we can see the same body temperature-driven flow near the mannequin, like in Figure 26 and Figure 27, and we can see the AC driven flow regions under the air conditioner devices. In Figure 30 and Figure 31, we can see the velocity filed at the window and the hip heights and the streamlines in the whole domain (for better and easier visualization just from one window), in this case, the air mixes and the air from the metro train's front is sucked forward.
Based on the results, the followings can be stated:

1. Using an FVM based CFD software can determine the sneezed or coughed air distribution in the computational domain.
2. With closed windows and without AC, the sneezed or coughed air shape is deformed spherical bubble.
3. With closed windows and with AC the sneezed or coughed air shape is a bubble with a cylindrical tail.
4. With opened windows and without AC the coughed air shape was different in the analysed two cases.
5. With closed windows the sneezed/coughed air typically spreading forward.
6. With opened windows the sneeze/cough spread mostly forward and a little bit laterally by the venturi force, but its effect was much smaller than we expected.
7. The AC's current baffle plates open outwards (see Figure 32/a and Figure 32/b), which mixes the air. If the AC's flow was blowing down straight or narrowed (see Figure 32/c), it could create different regions separated by "air walls", due to the sneeze cannot spread or it would be less likely to spread longitudinally on the metro. The negative effect of this modification is the draft effect, which would decrease the comfort of travellers.
8. The study without AC shows that the air can be stuck around the ceiling. This case with time, the airborne particle due to the buoyancy force can lift and it can remain until an airflow move it to the travelling space [33], therefore the fast and efficient air change is recommended.
9. With closed windows, we were not able to observe the estimated sneeze route (see Figure 8).

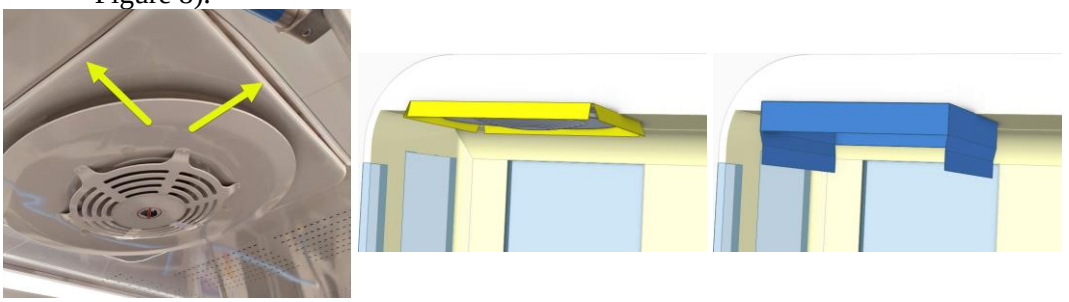


Figure 32. AC's baffle plates. a, Current transparent plastic baffle; b, Current transparent plastic baffle (coloured to yellow for better representation in Solid Edge CAD system); c, Recommended AC reducer (coloured to blue for better representation in Solid Edge CAD system)

For decreasing the probability of infection, according to the WHO [34], the hygiene is important, therefore the following are recommended for the use of public transportation:

- Maintain at least 1-meter social distance.
- Properly wear a mask (it should cover your chin, mouth, and nose).
- Due to the available quantity, use a fabric mask (preferably with multiple layers), if you are in a particular risk group use a medical/surgical mask, or if you are a health worker use a respiratory mask.
- Avoid the closed, crowded places and close contact.
- Regularly and thoroughly clean your hand.
- Avoid touching surfaces which were not cleaned and disinfected, e.g. handrails or ticket machines in the subway.
- Avoid touching your eyes, nose, and mouth.

SUMMARY

On a pandemic situation, a sneeze or cough can be frightening, and it can cause panic. In this paper, we examined multiple respiratory events with computational fluid dynamic software based on the finite volume method. For determining the sneeze/cough spreading direction we were running the simulations for 5 seconds after the event. With our results, we determined the spreading directions and established some conclusions.

Based on our results we recommend using public transportation with social distancing and with a face mask with the recommendations of the WHO and the other health organization. In one of our case, where the AC was on shown the sneeze spreading almost straight forward, and the sneeze/cough was spreading through the opposite door (approx. 2.5 metres) in 5 seconds (see Figure 17). In this condition, if we are facing with the sneeze or cough a face mask can filter the sneezed air as well and with the social distance, the contact with large particles can be avoided.

Using our results, the spread of sneezing/coughing is visualized in the examined subway car and with these illustrations, the anxiety can be reduced, and the passengers' sense of security can be increased.

ACKNOWLEDGEMENT

SUPPORTED BY THE ÚNKP-20-3 NEW NATIONAL EXCELLENCE PROGRAM OF THE MINISTRY FOR INNOVATION AND TECHNOLOGY FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND.

REFERENCES

[1] The Global Economic Outlook During the COVID-19 Pandemic: A Changed World. The World Bank. https://www.worldbank.org/en/news/feature/2020/06/08/the-global-economic-outlook-during-the-covid-19-pandemic-a-changed-world (accessed Oct. 30, 2020).

[2] J. Besenyő and M. Kármán, "COVID-19 pandemic on the African continent," (in Hungarian: A COVID-19 pandémia az afrikai kontinensen), *Safety and Security Sciences Review*, vol. 2, no. 2., pp. 39-56, Jun. 2020, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/57

[3] Cs. Kollár and Á. Zakar, "Social Engineering and Manipulation Techniques and Methods," (in Hungarian: A social engineering és a manipulációs technikák és módszerek – kutatási jelentés), *Safety and Security Sciences Review*, vol. 2, no. 3., pp. 31-46, Sept. 2020, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/70

[4] "Pandemic." Wikipedia. https://en.wikipedia.org/wiki/Pandemic (2020.10.20.)

[5] D. Bernoulli, "Testing a new analysis of smallpox mortality and the benefits of inoculation to prevent it," (in French: Essai d'une nouvelle analyse de la mortalité causée par la petite verole et des avantages de l'inoculation pour la prevenir), Mémoires de mathématiques et de physique, Académie royale des sciences, pp. 1-45, 1760, http://gallica.bnf.fr/ark:/12148/bpt6k3558n/f220.image.r=daniel%20bernoulli

[6] W. O. Kermack, A. G. McKendrick, "Contributions to the mathematical theory of epidemics—I," Bulletin of Mathematical Biology, vol. 53, pp. 33–55, 1991, doi: 10.1007/BF02464423

[7] W. O. Kermack, A. G. McKendrick, "Contributions to the mathematical theory of epidemics—II," The problem of endemicity. Bulletin of Mathematical Biology, vol. 53, pp. 57–87, 1991, doi: 10.1007/BF02464424

[8] W. O. Kermack, A. G. McKendrick, "Contributions to the mathematical theory of epidemics—III," Further studies of the problem of endemicity. Bulletin of Mathematical Biology, vol. 53, pp. 89–118, 1991, doi: 10.1007/BF02464425

[9] F. Brauer, P. van den Driessche, J. Wu, "Compartmental Models in Epidemiology," in *Mathematical Epidemiology*, Lecture Notes in Mathematics, vol. 1945, Springer, Berlin, Heidelberg, pp. 19-79, 2008, doi: 10.1007/978-3-540-78911-6_2

[10] "Prevention.", (in Hungarian: Megelőzés), koronavirus.gov.hu. https://koronavirus.gov.hu/megelozes (accessed Oct. 26, 2020).

[11] S. Radcliffe. "Staying 6 Feet Apart Often Isn't Enough During COVID-19 Pandemic." Healthline.com. https://www.healthline.com/health-news/staying-6-feet-apart-often-isnt-enough-during-covid-19-pandemic#New-model-of-physical-distancing (accessed Sept. 22, 2020).

[12] "Coronavirus disease (COVID-19) advice for the public." WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public (accessed Oct. 26, 2020).

[13] "Transmission of SARS-CoV-2: implications for infection prevention precautions," WHO. https://www.who.int/news-room/commentaries/detail/transmission-of-sars-cov-2-implications-for-infection-prevention-precautions (accessed Oct. 26, 2020).

[14] W. F. "Wells, On airborne infection. Study II. Droplets and droplet nuclei," *American Journal of Epidemiology*, vol. 20, no. 3, pp. 611–618, 1934, https://doi.org/10.1093/oxfordjournals.aje.a118097 (accessed Oct. 10, 2020).

[15] L. Bourouiba, E. Dehandschoewercker and J. W. M. Bush, "Violent expiratory events: on coughing and sneezing," *Journal of Fluid Mechanics*, vol. 745, pp. 537-563, April 2014, doi: 10.1017/jfm.2014.88

[16] B. R. Morton, G. I. Taylor and J. S. Turner, "Turbulent gravitational convection from maintained and instantaneous sources," *Proceedings of the Royal Society A*, vol. 234, pp. 1–23, January 1956, doi: 10.1098/rspa.1956.0011

[17] G. R. Hunt, T. S. van den Bremer, "Classical plume theory: 1937–2010 and beyond," *IMA Journal of Applied Mathematics*, vol. 76, no. 3, pp. 424–448, June 2011, doi: 10.1093/imamat/hxq056

[18] J. P. Duguid, "The size and the duration of air-carriage of respiratory droplets and droplet-nuclei," *The Journal of Hygiene*, vol. 44, no. 6, pp. 471–479, Sept. 1946. doi: 10.1017/s0022172400019288

[19] Y. Wang and L. Bourouiba, "Drop impact on small surfaces: thickness and velocity profiles of the expanding sheet in the air," *Journal of Fluid Mechanics*, vol. 814, pp. 510-534, March 2017, doi: 10.1017/jfm.2017.18P

[20] Y. Wang and L. Bourouiba, "Unsteady sheet fragmentation: droplet sizes and speeds" *Journal of Fluid Mechanics*, vol. 848, pp. 946-967, August 2018, doi: 10.1017/jfm.2018.359

[21] "Testing Shows Type of Cloth Used in Homemade Masks Makes a Difference, Doctors Say." Wake Forest Baptist Medical Center https://newsroom.wakehealth.edu/News-Releases/2020/04/Testing-Shows-Type-of-Cloth-Used-in-Homemade-Masks-Makes-a-Difference (accessed Oct. 31, 2020).

[22] P. Bahl, S. Bhattacharjee, C. de Silva, *et al*., "Face coverings and mask to minimise droplet dispersion and aerosolisation: a video case study," *Thorax*, vol. 75, pp. 1024-1025, 2020, doi: 10.1136/thoraxjnl-2020-215748

[23] S. Bhattacharjee, P. Bahl, A. A. Chughtai, *et al.* "Last- resort strategies during mask shortages: optimal design features of cloth masks and decontamination of disposable masks during the COVID-19 pandemic," *BMJ Open Respiratory Research,* vol. 7, pp. 1-10, 2020; doi: 10.1136/bmjresp-2020-000698

[24] E. P. Fischer, M. C. Fischer, D. Grass *et al.* "Low-cost measurement of facemask efficacy for filtering expelled droplets during speech," *Science Advances*, vol. 6, no. 36, pp. 1-5, Sep 2020, doi: 10.1126/sciadv.abd3083

[25] "Respirator." Wikipedia, https://en.wikipedia.org/wiki/Respirator (accessed Oct. 31, 2020).

[26] "Shortage of personal protective equipment endangering health workers worldwide." WHO. https://www.who.int/news/item/03-03-2020-shortage-of-personal-protective-equipment-endangering-health-workers-worldwide (accessed Oct. 31, 2020).

[27] M. Abkarian and H. A. Stone, "Stretching and break-up of saliva filaments during speech: A route for pathogen aerosolization and its potential mitigation," *Physical Review Fluids*, vol. 5, pp. 102301-1 102301-10, October 2020, doi: 10.1103/PhysRevFluids.5.102301

[28] J. W. Tang, T. J. Liebner, B. A. Craven, and G. S. Settles, "A schlieren optical study of the human cough with and without wearing masks for aerosol infection control," *Journal of the Royal Society Interface*, vol. 6, pp. S727-S736, December 2009, doi: 10.1098/rsif.2009.0295.focus

[29] "Comparison of the four metro lines." Metro4, http://www.metro4.hu/en/how-does-it-work/comparison-of-the-four-metro-lines (accessed Nov. 01, 2020).

[30] "Air and Climate Technology." (in Hungarian: Lég- és Klímatechnika), Magyar Épületgépészeti Koordinációs Szövetség, http://www.megksz.hu/epuletgepeszet/legtechnika/ (accessed Sept. 11, 2020).

[31] "Lung volumes." Wikipedia. https://en.wikipedia.org/wiki/Lung_volumes (accessed Sept. 10, 2020).
[32] "Density of air." Wikipedia. https://en.wikipedia.org/wiki/Density_of_air#Humid_air (accessed Sept. 10, 2020)
[33] R. K. Bhagat, M. S. D. Wykes, S. B. Dalziel and P. F. Linden, "Effects of ventilation on the indoor spread of COVID-19," *Journal of Fluid Mechanics*, vol. 903, pp. F1-1 - F1-18, Nov. 2020, doi: 10.1017/jfm.2020.720
[34] "Coronavirus disease (COVID-19) advice for the public." WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public (accessed Nov. 13, 2020)

APPRENDIX

Our CAD model available here: https://grabcad.com/library/m3-metro-train-renovated-1

REVIEW OF SOFTWARE QUALITY RELATED ISO STANDARDS

A SZOFTVERMINŐSÉGGEL KAPCSOLATOS ISO SZABVÁNYOK ÁTTEKINTÉSE

NYÁRI Norbert[1] – KERTI András[2]

Abstract

The present study aims to provide an overview of the current state of standardization efforts regarding software quality. Starting with the general characteristics of ISO standards, taking into account both their good and less good properties, briefly covering standardization organizations other than ISO. Starting from a brief, historical recall of the relevant basic concepts of quality and software quality, it outlines the key elements of the ISO / IEC 25000 family of standards, emphasizing the beneficial effects on IT security of using the family of standards, with a brief description of related additional standards. It illustrates the effective applicability of this family of standards with real-life examples from different parts of the world, taking into account Hungary's involvement and position on the subject.

Keywords

software quality, quality management, standards theory, information security, software development

Absztrakt

Jelen tanulmány egy áttekintő képet kíván szolgáltatni a szoftverminőséget érintő szabványosítási törekvések jelenlegi állásáról. Kezdve az ISO szabványok általános jellemzőitől, egyaránt számba véve azok jó és kevésbé jó tulajdonságait, röviden kitérve az ISO-tól különböző szabványosító szervezetekre is. A minőség és a szoftverminőség releváns alapfogalmainak rövid, történeti jellegű felidézésétől elindulva nagy vonalakban ismerteti az ISO/IEC 25000 szabványcsalád leglényegesebb elemeit, hangsúlyozva a szabványcsalád alkalmazásának kedvező hatását az informatikai biztonságra, a kapcsolódó további szabványok rövid ismertetésével. Való életből, a világ különböző részeiről származó példákkal illusztrálja az említett szabványcsalád hatékony alkalmazhatóságát, figyelembe véve Magyarország érintettségét és helyzetét a témában.

Kulcsszavak

szoftverminőség, minőségmenedzsment, szabványelmélet, információbiztonság, szoftverfejlesztés

[1] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kerti.andras@uni-obuda.hu | ORCID: 0000-0003-2149-5500 | associate professor, Faculty of Military Science and Officer Training of the University of Public Service | egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvéd-tisztkép-ző Kar

INTRODUCTION

Software is everywhere, it's in our computers, our cars, our watches, our washing machines, even in today's lawn mowers. Faulty software can cause many harms, in some cases, people's lives can depend on software quality, so it must be taken seriously. The quality of software in industrial applications or even in everyday life is vital for both developers and customers. Several standardization efforts aim to provide frameworks for evaluating software from the perspective of quality, but unfortunately, I they are not widespread enough. Software quality deficiencies can cause many issues, including security related problems. For example, I believe that usability problems can easily encourage users to deviate from the intended use of software systems. The topic has a strong relation with risk assessment, I plan to address this aspect in another article.

This study aims to do multiple things. I would like to give a review about software quality related de jure standards and also popularize them (knowing the disadvantages as well). I think that software quality standards should be used more widely in the industry.

ISO STANDARDS IN GENERAL

Let's start with a delicate topic, standards in general. The goals of standardization are well known, giving a unified approach on performing various activities, to put it simple, standards are showing the best way of doing things. [1] This is a goal with which one can easily identify, however not all features of standards are clearly positive, in the following I would like to highlight some difficulties as well. There are many standardization bodies around the world like ISO, ECMA, NIST etc., but mainly I shall focus on ISO in this article.

First of all, ISO standards cost money. It is only natural though, considering the lot of experience and work needed for creating a well-defined, usable standard. Secondly, ISO standards are famous for limited accessibility. David Travis also states that ISO standards are hard to access and expensive. [2] I can only confirm this from my personal experience. As an individual researcher, I have very few options to access ISO standards. First thing to check: university libraries, based on their catalogues, they do to not tend to hold copies of standards.

However, the Hungarian Standards Institution (Magyar Szabványügyi Testület, MSzT) has a reading room which provides international standards for reading purposes, but only those that have been published in Hungary. The service has a fee, but it is free for students. (On a side note: it is closed due to the current pandemic situation.) The institution has an online reading room as well, it is available as a yearly subscription, but there is no option for universities to have institutional access whatsoever. Furthermore, the students discount is valid only for the real reading room. [3]

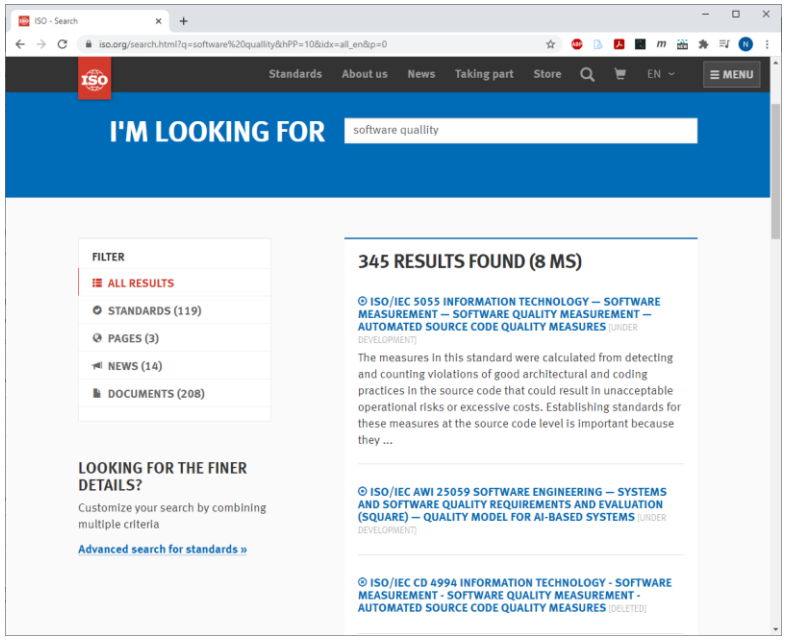
The price of standards only makes the situation worse; consider the ISO 9241 standard, a multipart standard covering ergonomics of human-computer interaction. It consists of more than twenty parts, buying all of them would cost at least a thousand euros. I have stopped counting at the fifth part of the standard. [2] [4] Obviously not all users need all parts of a standard, so the expenses can be fine-tuned.

I think that each and every standard, and family of standards should have a freely accessible, ISO-published, detailed guide that is available free of charge. It would make a lot easier for those interested in standards to find the most appropriate ones for their needs.

In connection with the price of standards emerges the problem of withdrawn standards. Let's consider ISO/IEC 9241-151 "Ergonomics of human-system interaction — Part 151: Guidance on World Wide Web user interfaces". It was first published in May 2008, and approximately 10 years later withdrawn, with no successor standard designated on the official site. After few internet searches I have found ISO/IEC/IEEE 23026:2015 "Systems and software engineering — Engineering and management of websites for systems, software, and services information", which based on its abstract covers more or less the ISO/IEC 9241-151, but I cannot state it with full conviction, because I do not own the new standard. I think that owners of soon to be withdrawn standards should be notified about the upcoming withdrawal, and should be offered alternatives to buy on a discount price.

Another "bad example" is the following standard: ISO/IEC/IEEE 12207-2:2020 Systems and software engineering — Software life cycle processes — Part 2: Relation and mapping between ISO/IEC/IEEE 12207:2017 and ISO/IEC 12207:2008. It costs approximately 180 EUR. [5] If a business wants to maintain compliance to ISO/IEC 12207, it has to pay for mapping tables between the withdrawn and newly published standards. I think that this kind of information should be a part of the aforementioned free-of-charge guide.

There are however some initiatives for making ISO standards more accessible in the form of review books, informational portals and such. These documents can really help businesses and individuals navigate in the world of standards. Again, the ISO 9241; without guidance it can be hard to determine, which part of the standard is relevant to a business. Although the table of contents is accessible for most of the standards on the official ISO website as a preview, it provides far too little information to make a well-informed decision.



1. Figure ISO search

One more note on the accessibility of standards, the official ISO website is less straightforward to a new inquirer. The search gives an overwhelming amount of information

if one does not know exactly, what he/she is looking for. I typed in 'software quality' in the ISO web shop search bar, the result is 345 elements of standards, news, web pages and documents mixed up in one list. On the first page there were 10 results, half of them was irrelevant because it was either deleted or under development. And there were 20 more pages to review.

The other method is to browse the catalogue by ICS, or TC. ICS stands for 'International Classification for Standards' and TC means 'Technical Committee'. Searching for 'ICS' on the ISO website leads the inquirer to the download screen of latest version of the ICS documentation and similarly a search for 'TC' gives information about the standard developing technical committees of ISO.

Speaking of Technical Committees, according to ISO official website ISO member bodies, like the aforementioned Hungarian Standards Institution (Magyar Szabványügyi Testület, MSzT) can choose if they want to participate to a particular TC and the level of involvement. The membership in a TC can be of two types: observing (O) or participating (P). O-members can observe the standards that are being developed, offering comments and advice. While P-members actively participate by voting on the standard at various stages of its development. [5]

In the 2004 study, Who Develops ISO Standards? A Survey of Participation in ISO's International Standards Development Processes stated that historically speaking, ISO standards have been dominated by industrialized nations, especially Western European countries. And there was no significant improvement in participations of less-developed regions despite ISO acknowledging the problem of under-representation of less-developed regions. The study also stated that the contribution of less developed countries matters less even if they are P-members of a TC, furthermore developed nations tend to send far more delegates to meetings and to hold more leadership positions within TCs. [6]

I haven't found a similar, more up-to-date study, but I have checked the official ISO website regarding the Hungarian participation in developing standards. MSzT is a participating member of 104 TC's and observing member of 419 TC's furthermore, it's a P-member of ISO/CASCO (Committee on conformity assessment) PDC and O-member of two other PDC's. PDC stands for Policy Development Committee. [5] In my humble opinion, I consider it very important that Hungary participates in so many TCs, thus providing an opportunity to influence the development of international standards.

The two following membership is relevant to this study: MSzT is P-member of the ISO/TC 176 Quality management and quality assurance TC and O-member of the ISO/IEC JTC 1 Information technology TC. [5]

On a side note: I do not know if the official ISO website is certified based on any ISO standards, but personally I would find it appealing if it were. ISO could easily set a good example by certifying its own website based on the relevant ISO/IEC standards, such as ISO/IEC/IEEE 23026:2015 and/or ISO/IEC 250xx standards.

Furthermore, the application of standards is optional in many cases. On one hand, this can be considered as an advantage, because small businesses do not have pay for the standards and the certification process, because no organization enforces the use of standards in any way (they are not like laws). On the other hand, not using a standard may deprive businesses of applying good practices, in some cases reduces their chances of winning tenders.

There are however standardization bodies other than ISO, like W3C (World Wide Web Consortium), ECMA (European association for standardising information and communication systems) etc. I would like to stress out that many of important standards, or in other words recommendations with great impact on the world are freely available like the W3C XML recommendation (Extensible Markup Language (XML) 1.0 (Fifth Edition)), or the ECMA-262 ECMAScript® 2020 language specification which is the basis of the very popular JavaScript programming language.

The software industry has taken significant steps towards open-source software in the recent years, with several large companies opening the source code for their very important products, e.g., the Microsoft .NET programming platform. I believe that a similar approach to standards would greatly contribute to the widespread use of standards.

SOFTWARE QUALITY

Next, I shall give a brief overview of the concepts of quality and software quality in particular. According to the Cambridge English Dictionary the word quality has three main meanings: 'how good or bad something is', 'a high standard', 'a characteristic or feature of someone or something'. [7]

In his 1984 paper Garvin synthetized the various interpretations of quality into 5 definitions. The *transcendent definition* mainly represents a philosophical position, which on its own proved to be less pragmatic in the past years. [8] [9]

The *product-based definition* views quality as an exactly measurable variable, so quality is an objective characteristic stemming from the features of the product. [8] [9]

The *manufacturing-based (or process-based) definition* simply states that quality is nothing more than compliance with requirements. [8] [9]

The *user-based definition* is subjective, because it views quality in terms of suitability for use, practically speaking, the best product is the one that is best suited to accomplish the goal. [8] [9]

Finally, the *value-based definition* states that a good quality product fulfils requirements in a cost-effective way, to put it simple, it is suitable for the task and in the same time preferably inexpensive. [8] [9]

Basically, two approaches, the process based and product based, have taken root in the industry, complemented by certain aspects of the other perspectives. [9]

ISO 9001:2015 standard uses a process-based approach helping its users creating, and maintaining processes that ensure the quality of the product or service in question. It defines quality as the following: 'degree to which a set of inherent characteristics of an object fulfils requirements '. [10] So, basically, as Crosby also stated in 1979, quality means meeting the specification. [11]

This definition however needs further clarification based on the aforementioned standard. An "object" can be anything perceivable or conceivable, given that software is object in this terminology.

A "requirement" is 'need or expectation that is stated, generally implied or obligatory'. Requirements can be of many types e.g., customer, statutory, regulatory. Requirements can be fulfilled or neglected, these two states were named by the authors of the standard "conformity" and "nonconformity". [10]

The traditional definition of quality cannot be interpreted directly for software though for many reasons. Firstly, software quality has different meanings for different participants in the software development process. A good software for developers has a readable, maintainable source code etc. A good software for operators is easy to install, has a straightforward configuration, secure enough, etc. A good software for end-users is suitable for the task, fast, has a straightforward UI etc. Secondly, the other aspect arises from the former, for a software to be called good, functional compliance is not enough by far.

This is why the definition of requirement needs further refinement in terms of software. Ian Sommerville basically distinguishes between two types of requirements: *functional* and *nonfunctional*. Sommerville also mentions a third category called *domain requirements.* [12]

Functional requirements describe in detail how the software system should work. Non-functional requirements are another dimension of software expectation because they do not directly relate to the functionality of the system, but rather describe the resulting properties of the system or impose constraints on them. [12]

In my opinion, non-functional requirements can also be interpreted as requirements for meeting functional requirements, as they set expectations for functionalities in terms of speed, size, usability, robustness, and portability (e.g., an application is suitable for performing a certain task, but is it fast enough while doing it? is it secure enough while doing it? etc.). Conformance to regulations and standards is also a nonfunctional requirement. [12]

Domain requirements stem from the industry environment in which the software is used, and can be classified into the former two categories. [12]

Back to the standards, at first ISO 9000 has not supported software development processes specifically, so the ISO 9000-3 was published to fulfill the needs of the software industry. In 2004 the first version of ISO/IEC 90003 superseded the aforementioned standard, giving guidelines on applying the latest ISO 9000 in software development. [9] [13]

There are also other approaches to ensure the quality of software development processes like CMM (Capability Maturity Model), CMMI (Capability Maturity Model Integration), ISO/IEC 33001:2015, among others, but they are out of the scope of this study.

In contrary, the now obsolete yet noteworthy ISO/IEC 9126 and its successor, the ISO/IEC 25010:2011 keeps software as a product in focus. The quality model defined in the former serves as a solid base for the ISO/IEC 25010.

Although the two interpretations of quality (process-based and product-based) mentioned above are fundamentally different, they go hand in hand in many cases. The process-based ISO 90003 recommends that the ISO/IEC 25010 should be used to define the quality attributes of the software produced with the ISO 9000 conformant software development processes. [13]

The ISO/IEC 25000 family of standards, also known as SQuaRE (System and Software Quality Requirements and Evaluation), provides a framework for the evaluation of software product quality having five divisions: Quality Management (2500x), Quality Model (2501x), Quality Measurement (2502x), Quality Requirements (2503x) and Quality Evaluation (2504x). [14] [15]The standards included in the series are shown in the table below.

ISO number	Name

ISO/IEC 25000 family	Systems and software engineering - Systems and software quality requirements and evaluation (SQUARE)
Quality Management Division	
ISO/IEC 25000:2014	Guide to SQUARE
ISO/IEC 25001:2014	Planning and Management
Quality Model Division	
ISO/IEC 25010:2011	System and software quality models
ISO/IEC 25012:2008	Data Quality model
Quality Measurement Division	
ISO/IEC 25020:2015	Measurement reference model and guide
ISO/IEC 25021:2015	Quality measure elements
ISO/IEC 25022:2015	Measurement of quality in use
ISO/IEC 25023:2015	Measurement of system and software product quality
ISO/IEC 25024:2015	Measurement of data quality
Quality Requirements Division	
ISO/IEC 25030:2015	Quality requirements
Quality Evaluation Divison	
ISO/IEC 25040:2011	Evaluation reference model and guide
ISO/IEC 25041:2012	Evaluation guide for developers, acquirers and independent evaluators
ISO/IEC 25042:2015	Evaluation modules
ISO/IEC 25045:2015	Evaluation module for recoverability

1. Table ISO/IEC 25000 family

The two standards (Guide to SQuaRE and Planning and management) in the Quality Management division define all common models, terms and definitions referred by all other standards from the series. [15]

The ISO/IEC 25010 standard from the Quality Model division defines quality requirements for software development products in eight areas (functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, portability). [14] Note that seven main categories of eight are related to non-functional requirements, which also confirms that software quality depends on functional conformity only to a relatively small extent.

The quality models in ISO/IEC 25010:2011 can be used in the following product development activities: identifying software requirements; validating requirements; identifying software design objectives; identifying software testing objectives; as part of quality assurance in establishing quality management criteria; identifying user acceptance criteria for a software product; in developing quality characteristics. According to its recommendation, ISO/IEC 25010: 2011 should be used either in conjunction with other members of the SQuaRE family of standards or in addition to ISO/IEC/IEEE 12207:2017 and/or ISO/IEC/IEEE 15288. [16] [17] The assessment of the requirements can also be used in the implementation phase to test the products delivered by the system vendor. [18] In my understanding the quality profile of software product should be determined in cooperation by the developers and users in the earliest phase as possible, in order to ensure that quality means the same for every stakeholder in the development process.

Also from Quality Model division, the ISO/IEC 25012 - Data Quality model: defines a general data quality model for structured data retained within computer systems. It focuses on the quality of the data as part of a computer system and defines quality characteristics. [14]

ISO/IEC 12207:2017 System and software engineering – Software lifecycle processes also provides processes that can be employed for defining, controlling, and improving software life cycle processes within an organization or a project. ISO/IEC/IEEE 15288:2015 System and software engineering – System life cycle processes, according to the official ISO website, establishes a common framework of process descriptions for describing the life cycle of systems created by humans from an engineering viewpoint. The previous two standards share a common terminology. Thus, the choice of whether to apply the former standard for the software life cycle processes, or the latter depends on the system-of-interest. Processes in both documents differ in activities and tasks to perform software engineering or systems engineering, respectively. [5]

The standards in the Quality Measurement division provide a software a reference model for measuring software product quality, mathematical definitions of quality measures, and guidance for their application. [14]

The Quality Requirements division this division helps specifying quality requirements. These quality requirements can be used in the process of quality requirements, elicitation for a software product to be developed or as inputs for an evaluation process. The requirements definition process is mapped to technical processes defined in the aforementioned ISO/IEC 15288. [15] [14]

The Quality Evaluation standards form the ISO/IEC 25000 family requirements, recommendations and guidelines for software product evaluation. [14]

ISO/IEC 14598-6:2001 is also a relevant standard to the Quality Evaluation division, reviewed and confirmed in 2008. According to the official ISO website, this standard defines the structure and content of the documentation to be used to describe an Evaluation Model. Evaluation modules are intended to be used within the context of the ISO/IEC 9126 and the ISO/IEC 14598 multipart standards. [5]

I have found this standard somewhat outdated, since the ISO/IEC 9126 is withdrawn and replaced by ISO/IEC 25010, and the ISO/IEC 14598 no more published parts other than this one. [5] However, I assume, that the concepts in this standard can be mapped to ISO/IEC 25010, since it is the official successor of ISO/IEC 9126. However, ISO/IEC 25040 states, that SQuaRE replaces the ISO/IEC 9126 series and the ISO/IEC 14598 series. [15]

REAL WORLD APPLICATIONS OF ISO/IEC 25000

One of the drawbacks of ISO standards, as I mentioned in the previous chapter, is the voluntary application. The use of software quality related standards can be motivated from the customer side though. The Spanish public administration includes among the requirements the conformance to ISO/IEC 25000 in the software related requests for proposals (RFP). In the 2020 digital hospital model specification of San Carlos Clinical Hospital the Servicio Madrileño de Salud (Madrid Health Service) included the ISO 25000 certification among its criteria, having the ISO/IEC 25000 certification provide 7 points out of the 40 points assigned to the technical conditions. [19] [20] This example can be set in parallel with Nigel Bevan's opinion in his article on Usability Standards. Bevan states that standards have the greatest impact incorporated into regulations and contracts. [4]

More examples can be found in Spain: CGM CompuGroup Medical obtained an ISO/IEC 25000 certificate for Functional Suitability for their decision support software. The

AENOR (Spanish Association for Standardisation and Certification) and AQC Lab evaluates and certifies software products in Spain in the Functional Suitability and Maintainability area of SQUARE. [14]

Based on the Spanish example public administrations of other countries should consider incorporating the requirement of ISO 25000 conformance and certification in request for proposals which includes software development activity.

According to the official website of the EU project SmartOpenData, it aims to make environmental and geospatial data concerning rural and protected areas more readily available and re-usable, better linked with data without direct geospatial reference so different distributed data sources could be easily combined together. The projects evaluation plan heavily uses SQUARE. [21]

In the 2019 article Examples of practical use of ISO/IEC 25000 it is stated that in Italy the ISO/IEC 25000 family was primarily applied by companies where the attending experts had participated in the TC developing the standard. Other companies with very large databases also applied the standard in order to guarantee consistency between multiple systems. Finally similarly to the example of the Spanish public administration, the application of ISO/IEC 25000 series is required or recommended in the public procurement of IT products. [22]

In the paper Measuring Public Value UX based on ISO/IEC 25010 Quality Attributes the authors measured the user experience of a job-seeking website called JobsMalaysia managed by Malaysian government. The authors performed the testing in an accredited Software Testing facility in Malaysia. The facility was MS ISO/IEC 17025: 2005 certified in software testing including usability and user experience. The usability characteristics were measured against ISO/IEC 25010:2011. The authors state that measuring usability based on the quality characteristics defined in the former standard seemed to be the most optimal method. [23]

In Hungary the National Accreditation Authority (Nemzeti Akkreditáló Hatóság, NAH) is entitled to conduct accreditation procedures. Having checked nah.gov.hu, I found that there is no organization in Hungary accredited for certifying software products based on the ISO/IEC 25010 standard. There are however many laboratories which are certified to operate based on MSZ EN ISO/IEC 17025:2018. Most of them are eligible to conduct certification processes in terms of software and IT systems, based on ISO/IEC 18045:2008, which is practically speaking an evaluation guide to ISO/IEC 15408 (Common Criteria). [24] Such a prevalence of Common Criteria is not surprising considering that the Hungarian Administrative IT Committee (Közigazgatási Informatikai Bizottság, KIB) published recommendations related to IT security based on Common Criteria. [25]

HOW CAN SOFTWARE QUALITY SERVE INFORMATION SECURITY?

In the following, I would like to emphasize that efforts spent on enhancing software quality can contribute to improvement of information security. No wonder that the ISO/IEC 27000 family of standards is very popular nowadays, in the Information Age. Basically, the standard provides guidelines to implement an ISMS (Information Security Management System). The level of security in a system depends on many things though e.g., education and safety awareness of users, IT governance policies, applied security solutions in the system etc. Such system would probably contain various software implementations. I believe

that the quality of the applied software in Electronic Information Systems can highly contribute to increasing the overall security of any system.

Software quality has eight high-level characteristics according to the ISO/IEC 25010 standard, each of them is composed of a set of related subcharacteristics as it can be seen on the diagram below. [9] Obviously Funcitional Suitability is vital for a software, but I think tha deficiencies of other kind can cause even security problems. Usability deficiencies can easily encourage users to deviate from the intended use of the software system, bypassing even the security solutions of it.

I think that in software-intensive systems the ISO/IEC 25000 family should be heavily used, possibly in the early stages of software development in order to define the proper characteristics that guarantee the adequate level of security in the system. In this aspect security, reliability, usability and usability characteristics are key to achieve the expected level of security.

2. Figure Characteristics of software quality based on ISO/IEC 25010

SUMMARY

I shall summarize my findings as follows. First of all, making ISO standards more easily accessible would greatly contribute to the wider application of standards. ISO should provide detailed guides to their standards free of charge. It would also be highly advisable to provide institutional read-only access for universities to standards for academic purposes. Even making specific standards open-source should be considered.

There are many relevant ISO standards in the topic, it takes a bit of an effort to get familiar with all of them. There also should be ISO-published documents about the relationships between standard families.

Using standards in contracts help spreading of ISO standards. Either governmental or commercial customers should incorporate conformance to ISO/IEC 25000 into their software related contracts (either COTS, or personalized development).

Unfortunately, there is no organization right now in Hungary, which can evaluate and certify software based on ISO/IEC 25010. Furthermore, as far as I know the ISO/IEC 25000 family have not been published in Hungarian. MSzT being an O-member of the ISO/IEC JTC 1 Information technology TC, which is in charge of developing the standard family is great news though, but it would be even better if it could achieve P-member status.

Last but not least, applying the security, reliability and usability characteristics of ISO/IEC 25010 on software in complex IT systems can improve the overall security.

RESOURCES

[1] ISO, "Benefits of standards," [Online]. Available: https://www.iso.org/benefits-of-standards.html. [Accessed 22 03 2021].

[2] D. Travis, Bluffers' Guide to ISO 9241, Userfocus ltd., 2014.

[3] Magyar Szabványügyi Testület, "Magyar Szabványügyi Testület," [Online]. Available: https://prod.mszt.hu/hu-hu/. [Accessed 22 03 2021].

[4] N. Bevan, "International Standards for Usability Should Be More Widely Used," Journal of Usability Studies, vol. 4, no. 3, pp. 106-113, 2009.

[5] ISO, "iso.org," ISO, [Online]. Available: www.iso.org. [Accessed 05 04 2021].

[6] M. Morikawa and J. Morrison, "Who Develops ISO Standards? A Survey of Participation in ISO's International Standards Development Processes," Pacific Institute for Studies in Development, Environment, and Security, 2004.

[7] Cambridge Dictionary, "Cambridge Dictionary," [Online]. Available: https://dictionary.cambridge.org/dictionary/english/. [Accessed 23 03 2021].

[8] D. A. Garvin, "What doees 'product quality' really mean?," MIT Sloan Management Review, Fall, vol. 26, pp. 25-43, 1984.

[9] K. Balla, Minőségmenedzsment a szoftverfejlesztésben, Budapest: Panem Könyvkiadó, 2007.

[10] ISO, ISO 9000:2015 Quality management systems — Fundamentals and vocabulary, ISO, 2015.

[11] P. B. Crosby, Quality is free, New York: McGraw-Hill, 1979.

[12] I. Sommerville, Software engineering 8th edition, Addison Wesley, 2006.

[13] ISO, ISO/IEC/IEEE 90003:2018 Software engineering — Guidelines for the application of ISO 9001:2015 to computer software, ISO, 2018.

[14] iso25000.com, "iso25000.com," iso25000.com, [Online]. Available: https://iso25000.com/. [Accessed 10 04 2021].

[15] ISO, ISO/IEC 25040:2011, ISO, 2011.

[16] C. Sikné Lányi and J. Schanda, Számítógépes ergonómia, Pannon Egyetem, 2014.

[17] L. Izsó and M. Antalovits, Bevezetés az információ-ergonómiába, Budapest: BME, 2000.

[18] KIFÜ, Informatikai fejlesztések termékminőségbiztosítási tevékenységei – módszertani leírás, Budapest: KIFÜ, 2014.

[19] iso25000.com, "Spanish public administration values the quality of the software product with ISO/IEC 25000 on their RFPs," iso25000.com, [Online]. Available: https://iso25000.com/index.php/en/news/192-spanish-public-administration-values-the-quality-of-the-software-product-with-iso-iec-25000-on-their-rfps. [Accessed 23 03 2021].

[20] Servicio Madrileño de Salud, PLIEGO DE CLÁUSULAS ADMINISTRATIVAS PARTICULARES QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DE "IMPLANTACIÓN DEL MODELO DE HOSPITAL DIGITAL EN EL HOSPITAL CLÍNICO SAN CARLOS" A ADJUDICAR POR PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS., 2020.

[21] SmartOpenData, "SmartOpenData," SmartOpenData, [Online]. Available: http://www.smartopendata.eu/. [Accessed 10 04 2021].

[22] N. Domenico and A. Trenta, "Examples of practical use of ISO/IEC 25000," IWESQ 2019: 1st International Workshop on Experience with SQuaRE series and their Future Direction, pp. 9-10, 2019.
[23] Ashok Sivaji et al., "Measuring Public Value UX based on ISO/IEC 25010 Quality Attributes Case Study on e-Government," INTERNATIONAL CONFERENCE ON USER SCIENCE & ENGINEERING 2014 (i-USEr 2014), 2014.
[24] NAH, "NAH," NAH, [Online]. Available: https://www.nah.gov.hu/. [Accessed 10 04 2021].
[25] KIB, A KIB 25. számú ajánlása: 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió, Budapest: KIB, 2008.
[26] S. Goericke, The Future of Software Quality Assurance, Cham, Switzerland: Springer Nature Switzerland AG, 2020.
[27] K. Balla, "A szoftveripar sajátosságai," in Róth, András (szerk.), A minőségfejlesztés új útjai: A minőségügyi szakemberek gyakorlati szerepe az információs társadalomban., Budapest, Verlag Dashöfer Szakkiadó Kft, 2008, pp. 6.8.1-6.8.64.

HIGH RELIABILITY, UNIAXIAL PHOTOVOLTAIC VOLTAGE SOURCE

NAGY MEGBÍZHATÓSÁGÚ, EGY TENGELY MENTÉN FORGATHATÓ FOTOVOLTAIKUS FESZÜLTSÉGFORRÁS

BESZÉDES Bertalan[1] - GYÖRÖK György[2]

Abstract

The aim of this study, which processes domestic and foreign sources, is to present the development possibilities of photovoltaic, off-grid equipment that can be used successfully in industrial and civil areas, requiring high reliability in terms of energy security. After introducing the topic, I will write about the possibility of increasing the availability of the power source, and then I will describe an efficiently usable construction. In a separate subchapter I deal with the energy demand of the technical equipment, the possibility of energy storage and the monitorability of the equipment. To conclude my study, I discuss the end-user parameterization of application-dependent modes.

Keywords

fotovoltaikus, szigetüzemű, egytengelyű forgatás, rendelkezésre állás, megbízhatóság, modularitás

Absztrakt

Hazai és külföldi forrásokat feldolgozó tanulmány célja, hogy a nagy megbízhatóságot igénylő, ipari és polgári területeken eredményesen használható, fotovoltaikusan táplált, szigetüzemű berendezések fejlesztési lehetőségeit mutassa be, az energiabiztonság szempontjából. A téma bevezetését követően a tápellátás rendelkezésre állásának növelési lehetőségéről írunk, majd ismertetünk egy hatékonyan alkalmazható konstrukciót. Külön alfejezet foglalkozik a műszaki berendezések energiaigényével, az energia tárolás lehetőségével és a berendezés monitorozhatóságával. A tanulmány zárásaként az alkalmazási területtől függő működési módok végfelhasználó általi paraméterezhetőségéről esik szó.

Kulcsszavak

photovoltaic, off-grid, uniaxial rotation, availability, reliability, modularity

[1] beszedes.bertalan@uni-obuda.hu | ORCID: 0000-0002-9350-1802 | assistant professor, Óbuda University Alba Regia Technical Faculty | egyetemi tanársegéd, Óbudai Egyetem Alba Regia Műszaki Kar

[2] gyorok.gyorgy@uni-obuda.hu | ORCID: 0000-0003-3668-7855 | professor, Óbuda University Alba Regia Technical Faculty egyetemi tanár, Óbudai Egyetem Alba Regia Műszaki Kar

BEVEZETÉS

A napenergia elektromos árammá történő átalakítása lehetővé teszi, hogy a hálózati villamos energiától függetlenül is legyen lehetőség a villamos energia megtermelésére a felhasználás helyén. A technológia alkalmazása nagyban elősegíti az olyan objektumok villamos energiával történő ellátását, melyek elhelyezkedésükből adódóan nem csatlakoztathatnak a villamos hálózatra. A felhasználás jellemző területei a természetvédelmi területek, vadgazdálkodási területek, nagy kiterjedésű mezőgazdasági területek, nagy területű állattartó vagy állattenyésztő területek, ipari csővezetékek nyomvonalai, infrastruktúrától távol elhelyezkedő vízügyi erőforrások, stb. Az ilyen jellegű területek és vagyon tárgyainak védelme, valamint azok működőképességének detektálása különösen fontos, - kiemelt jelentőségűek a kritikus infrastruktúrákhoz sorolt szektorok.

A jelenlegi energetikai rendszernek nem feltétele a centralizált hálózat. A szakemberek nagy mennyiségű erőforrás felhasználásával, fejlesztik a megújuló energiaforrásokat. A fejlesztések eredményeként már polgári célra is elérhetőek olyan napenergiát hasznosító megoldások, amelyek képesek épületek vagy berendezések villamos tápellátásának biztosítására. Jelen kutatás a nagyobb teljesítményű ipari napelemes rendszerekre, illetve a koncentrált napenergia hasznosításra nem tér ki.

SZIGETÜZEMŰ NAPELEMES RENDSZEREK

A napenergiát felhasználó, villamos energiát előállító rendszerek csoportosíthatóak aszerint, hogy képesek-e a villamos hálózatra visszatáplálni. A szigetüzemű tápellátást biztosító rendszerek, a villamos hálózattól függetlenül látják el feladatukat, a kutatás alkalmazási területéből adódóan az önálló működésre is képes rendszereket vizsgálom. Az előállított villamos energia szempontjából léteznek egyenáramot, illetve váltakozó áramot előállító sziget üzemben működő, napenergiát hasznosító rendszerek. A napelemek, az akkumulátor töltő, a DC/DC konverter és az inverter jelentős mértékben meghatározza a rendszer teljesítményét, hatásfokát és egyéb üzemi paramé-tereit [1].

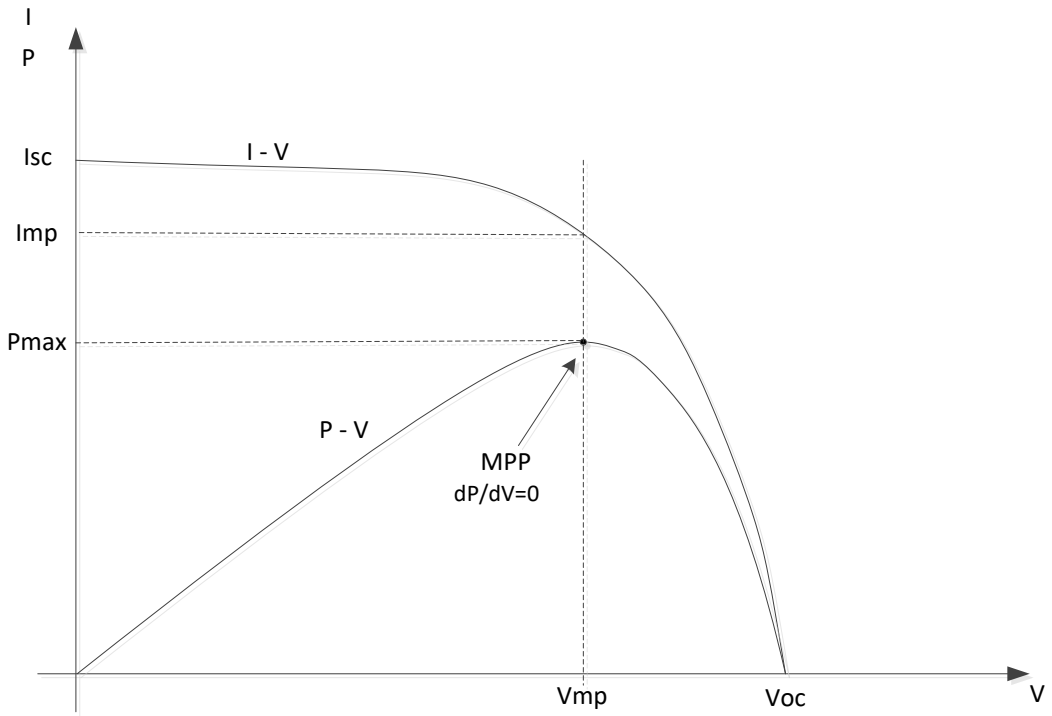
A rendszer a napelemek segítségével megtermelt energiát az akkumulátorokban, mint töltés tárolására képes egységekben raktározza el. Az energiaforrásból érkező- vagy az akkumulátorban eltárolt energiát a tápellátó rendszerre csatlakoztatott berendezés fogja felhasználni.

Az akkumulátor töltésére alkalmazott áramkör feladata illeszteni a napelem paneleket az akkumulátorhoz. Ez esetben szükséges figyelembe venni a napelem terhelésének optimalizálását, valamint az akkumulátor típusához illeszkedő töltési módokat. A különböző technológiákkal gyártott akkumulátorok különböző töltési diagramokkal rendelkeznek, ezeknek be nem tartása a rend-szerelem élettartamának nagy mértékű csökkenését eredményezhetik.

A terhelés meghajtására hivatott áramkör feladata illeszteni az akkumulátor feszültségét a terhelés bemeneti feszültségigényéhez. Egyenáramú meghajtás esetében egy DC/DC konverter, váltakozó feszültségű kimenet esetében egy inverter alkalmazása szükséges. Szigetüzemű tápellátás és inverteres kimeneti fokozat esetében, a hálózati 50Hz-es frekvencia és az inverter kimeneti frekvenciájának szinkronizálása nem szükséges. Az inverter kimeneti feszültségének jelalakja esetében erőteljesen ajánlott a tisztán szinuszos jelalak, a meghajtott terhelés hosszabb élettartama érdekében.

FOTOVOLTAIKUS CELLÁK ÉS NAPELEM PANELEK ALKALMAZÁSA

A tápellátó rendszer számára a napelem panelek biztosítják az energiaellátást. A napelem panelek kimenete a megvilágítottságtól (napszaktól, évszaktól, felhőzöttség-, illetve szennyezettség mértékétől) függően széles határok között változhat. A bemenő kör célja, a költséghatékony kiépítés jegyében, a napelemek legjobb hatásfokkal történő kihasználása, ehhez a napelemeket illeszteni kell az azokat terhelő fokozathoz. A legnagyobb hatásfok eléréséhez, a napelem táblák teljesítmény illesztése szükséges. Az akkumulátor töltő elektronika feladata a napelem táblák munkapontjának beállítása, ehhez az MPPT3 töltési algoritmust alkalmazza (1. Ábra). Az akkumulátor töltő elektronikának képesnek kell lennie a beérkező széles határok között változó feszültség és áram értékek mérésére és kezelésére.



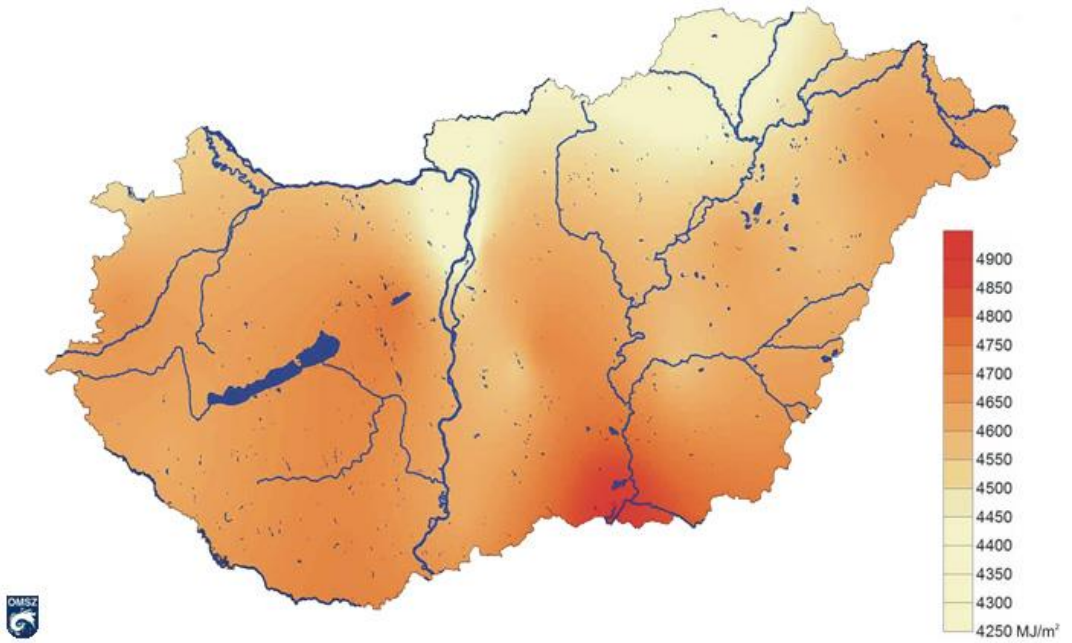
1. Ábra: Fotovoltaikus cellák karakterisztikája

NAPELEMEK ELHELYEZÉSE

Magyarország területe jó közelítéssel 90 000 km2. Az ország több mint fele 200 méternél alacsonyabban fekszik, valamint a 400 méternél magasabb területek mennyisége kevesebb mint 2%. A fotovoltaikus panelek megfelelő tájolása lényeges a kinyerhető energia mennyisége szempontjából. A legnagyobb éves besugárzás az ország déli területeit jel-

[3] MPPT - Max Power Point Tracking - maximális munkapont követés

lemzi (2. Ábra), ahol átlagosan meghaladja az évi 4500 MJ/m2-t. Derült időben a fölfelszínre beérkező energia mennyisége jó közelítéssel 1000 W/m2 (a déli órákban), ami a felhősödés mértékétől függően lecsökkenhet 50-100 W/m2-re is.



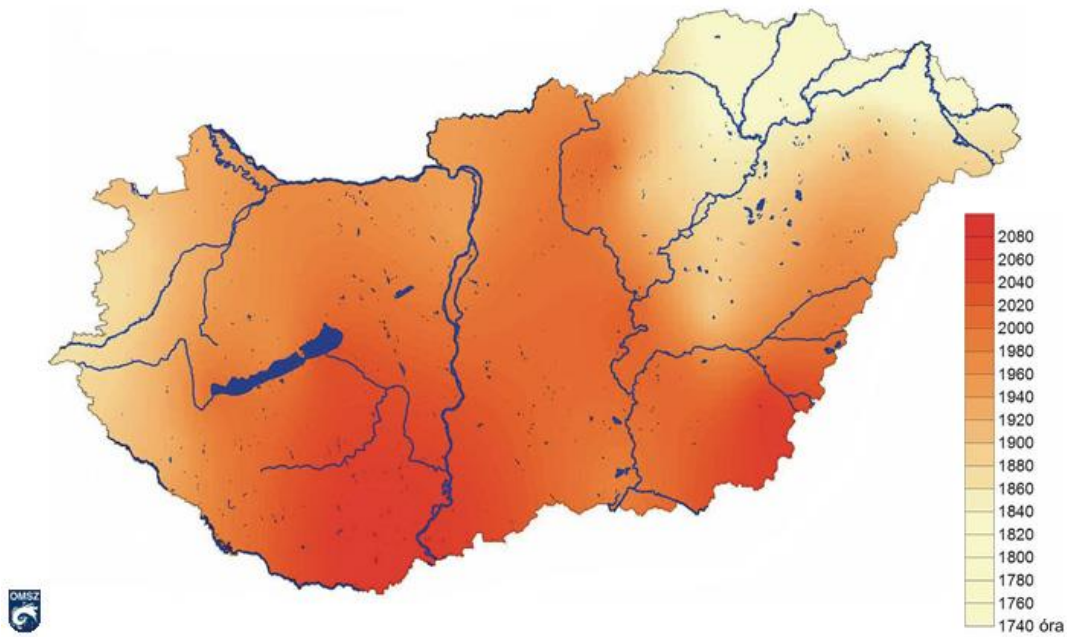
2. Ábra: Éves átlagos napenergia besugárzás mértéke 2000 és 2009 között (forrás:https://www.met.hu/eghajlat/magyarorszag_eghajlata/altalanos_eghajlati_jellemzes/sugarzas/images/abra1.jpg)

A besugárzott napenergia mennyiségét nagy mértékben befolyásolja a domborzat és a felhőzet. A legmagasabb napsütéses órák száma (2000 h/év) a déli országrész területein található (3. Ábra). Az Országos Meteorológiai Szolgálat adatai alapján, az országrészek közötti eltérés hozzávetőlegesen 10%. Megjegyzendő, hogy télen a magasan fekvő területek közelítőleg 1,5-ször több napsugárzáshoz jutnak, mint az alacsony területek. Az alacsony területeket gyakran borító ködből a magasabb hegyek kiemelkednek, nyáron viszont csapadékosabbak az említett területek.

Magyarország az északi szélesség 45°45’ és a 48°35’ között helyezkedik el - nagyjából az Északi-sark és az egyenlítő között félúton – a szoláris éghajlati felosztás szerint a mérsékelt övben. A legnagyobb mértékű napenergia felfogásához a Nap sugarainak és a napelem táblának merőleges elhelyezkedése esetén van lehetőség, ebben az esetben a legalacsonyabb mértékű a visszatükröződés is.

Az előbbiekből adódóan, a napelemek dőlésszögének beállítása megközelítőleg 45°-os szögben javasolt felhelyezni, a forgató mechanizmus középállásában déli irányban - ebben az esetben biztosítható az optimális éves energiatermelés. A javasolt dőlésszög csak egy iránymutatás a teljes évre vonatkozó beállításhoz, mivel a nyári és téli időszakban eltérő a Nap pályájának magassága. Ez nyári időszakban, délben a közel vízszintes helyzetet jelenti, téli időszakban viszont ez lenne a legkedvezőtlenebb pozíció. A vízszinteshez képest,

nyáron célszerű lenne 36°-ra (19° és 42° közötti besugárzási szöghöz tartozó köztes beállítás) télen pedig 59°-ra (42° és 66° közötti besugárzási szöghöz tartozó köztes beállítás) beállítani a napelem panelek dőlésszögét. A 45°-os dőlésszög másik fontos momentuma, hogy a táblákra rakódott hó csak akkor tud távozni, ha a lejtés megfelelő, ennek okán nem javasolt a 40°-nál kisebb szögben történő elhelyezés.



3. Ábra: Éves átlagos napsütéses órák száma 1971 és 2000 között (forrás: https://www.met.hu/eghajlat/magyarorszag_eghajlata/altalanos_eghajlati_jellemzes/sugarzas/images/abra3.jpg)

Jelen kutatásba ismertetett megoldás törekszik a költségek és a rendszer hatásfokának optimalizálására is, valamint a robosztus mechanikai kivitel megvalósítására, ezért csak a tengelyirányú forgató mechanikát alkalmazza.

A berendezés elhelyezését tekintve talajra helyezve az aljnövényzet és az esetleges fák koronája miatt nem lenne megfelelő a besugárzást, ezért javasolt kiemelni, valamint az esetleges kamerarendszernek is megfelelőbb, ha a magasságból figyelheti meg a terepet. Fás, erdős területen a megfelelő árbócmagasság a 10-15m lenne.

A hatásfok maximumára, a kiválasztott napelem gyártási technológiája is hatással van. A kristályos szilícium napelem egy a kereskedelmi forgalomban kapható megfizethető áru napelem technológia, az egyik legmagasabb hatásfokkal rendelkezik (20-24%). [3]

TELJESÍTMÉNYIGÉNY MEGHATÁROZÁSA

A kutatást támogató modellben, a környezet monitorozó rendszer, a video felvevő rendszerrel, a vezeték nélküli kapcsolattal, és az éjszakai infravörös fényt kibocsájtó LED-el, 24 órára vetítve, átlagosan 20W teljesítményigénnyel rendelkezik. Ez 24 óra leforgása alatt 480 Wh-nyi energia-mennyiséget jelent. 12V-os akkumulátorokat és rendszerfeszültséget alkalmazva ez 40Ah-nyi töltésmennyiség. Az alkalmazott akkumulátor technológia, a

környezeti hőmérséklet, és a várható gyengén napsütéses órák száma függvényében további korrekciók szükségesek.

Akkumulátorok esetében a belőlük kinyerhető töltésmennyiség megállapításakor, a maximális töltési és a minimális kisütési feszültség különbségének figyelembevételével is számolni kell. Javasolt az ipari alkalmazásra gyártott, kötött elektrolitú (zselés - gel), szeleppel ellátott, savas, zárt ólomakkumulátorok beépítése. A minőségi típusok a névleges feszültségük 20%-ára is károsodás nélkül kisüthetőek. A technológiát alkalmazva a feszültséglépcső 9,6V lehet, ami legalább 50Ah-s akkumulátor kapacitást jelent. [2]

30 év meteorológiai adatait figyelembe véve, magyarországi a nyári hónapokban nagyjából 4-szer több a napsütéses órák száma, mint a téli hónapokban. A téli -10°C-os környezeti hőmérséklet mellett az említett akkumulátor kapacitása nagyjából a 65%-ra esik vissza. Az említett üzemi körülmények a legridegebb alkalmazási környezetet feltételezik. A rendelkezésre állás biztosításának igénye függvényében, az akkumulátor kapacitásának megnövelésének mértéke meghatározható – ez mindenképpen a költségek növekedését vonja maga után.

REDUNDÁNS NAPELEM PANEL FIZIKAI KIÉPÍTÉSÉNEK LEHETŐSÉGE

A rendszer egyik kulcsfontosságú eleme maga a fotovoltikus komponens, a napelem. Ennek optimális elektronikus illesztéséről, mint releváns mérnöki problémáról már esett szó. A napelem működéséből adódó hibák kiküszöbölése a célzott feladat, a hatásfok növelésének egyik módja a Nap pályájának követése. [4] Sok cikk tárgyalta a napelem optimális helyzetét, két tengelyen követve a Nap pályáját. [5]

A kísérleti modell az irodalom alapján épül fel. A gyakorlatból vett probléma a napelemek szenynyezése és károsodása, ezáltal a termelt energia csökkentése. A felhasználói tapasztalatok alapján ezek a szennyeződések lehetnek; szennyezett eső (por tartalommal), homokvihar (szél által szállított por), ipari szennyezés, mezőgazdasági tevékenységből származó szennyeződés, biológiai szennyezés (rovarok, madarak, állatok), stb.

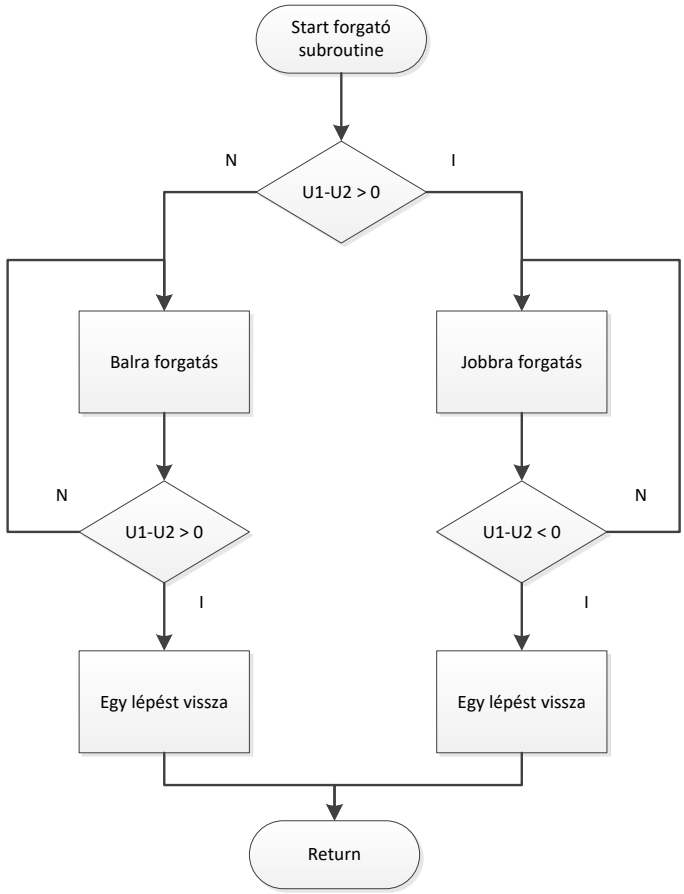
A sérülés visszafordíthatatlan állapot, amelyet bármilyen mechanikai behatás kiválthat, például jégeső, emberi beavatkozás (dobás, lövés). A szennyeződést ütemezett vagy szükséges karban-tartási művelettel lehet eltávolítani. A mechanikai sérüléseket csak cserével lehet orvosolni.

A felhasználó számára fontos értesülni a teljesítményromlásról, és a megbízható működés érdekében fontos valamilyen redundáns rendszer kifejlesztése.

A 7. Ábra látható elrendezés egy duplikált egytengelyű napelemet ábrázol. A vezérelt tengely kettős funkcióval rendelkezik; a napelem az aktív és a korábban inaktív napelemet jelentős 180 fokos forgással helyettesíti, ha a teljesítmény jelentősen csökken. A tartalék napelem valószínű-leg nagyobb hatékonysággal fog működni, mint amit piszkosnak vagy sérültnek nyilvánított a rendszer. Az inaktívvá vált napelemet a karbantartás során tisztítják vagy kicserélik.

Egy tengely vezérlésével mikrokontroller segítségével történő vezérlésével lehetőségünk van meghatározni annak optimális helyzetét a Nap aktuális helyzetéhez viszonyítva, folyamatosan alkalmazkodva a változáshoz. [6] A Nap helyzetének érzékelése történhet többek között elektrooptikai szenzorok segítségével [7], vagy a napelemből kinyerhető maximális teljesítmény megállapításával [8]. Az említett érzékelési megoldások alkalmazása nagy beállítási pontosságot tesz lehetővé jó időjárási körülmények között. A szenzorjelek

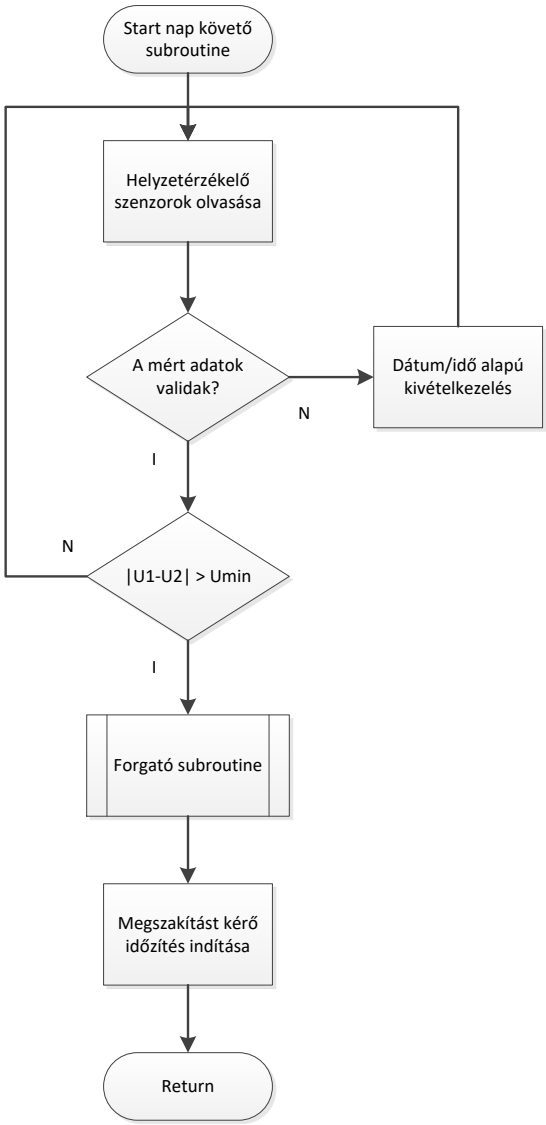
feldolgozása történhet analóg komponensek (tranzisztorok, műveleti erősítők) [10] vagy analógdigitál átalakító segítségével [11]. A 4. Ábra szerinti algoritmusa vázolja az optoelektronikai elemek kimeneti jeleit feldolgozó szoftveres megvalósítást. Egy hibrid alkalmazás tovább növeli a megbízhatóságot.



4. Ábra: Napelem panel forgató algoritmus

U1 és U2 a két digitalizált szenzorkimenet, a kisebb érték irányába fog a napelem panel fordulni. A túlzott elfordulás érzékelése után a napelem panel egy egységet visszalép, és ezzel a pontossággal megelégedve a rendszer kilép a forgató algoritmusból.

Felhős időjárási körülmények között a szórt fény forrásának költséghatékony megállapítása a koordináta és dátum/idő adatok alapján lehetséges. [9] Az alkalmazott mikrokontroller (vagy az azt kiegészítő memória) képes tárolni a kronológiai adatokat, a felbontás növelése a tárolt adatokat felhasználó interpoláció segítségével lehetséges. Három bemeneti szögérték segítségével már szoftveres többségi -, középérték szavazó vagy egyéb átlagoló algoritmus is megvalósítható (5. Ábra). [12], [13], [14]

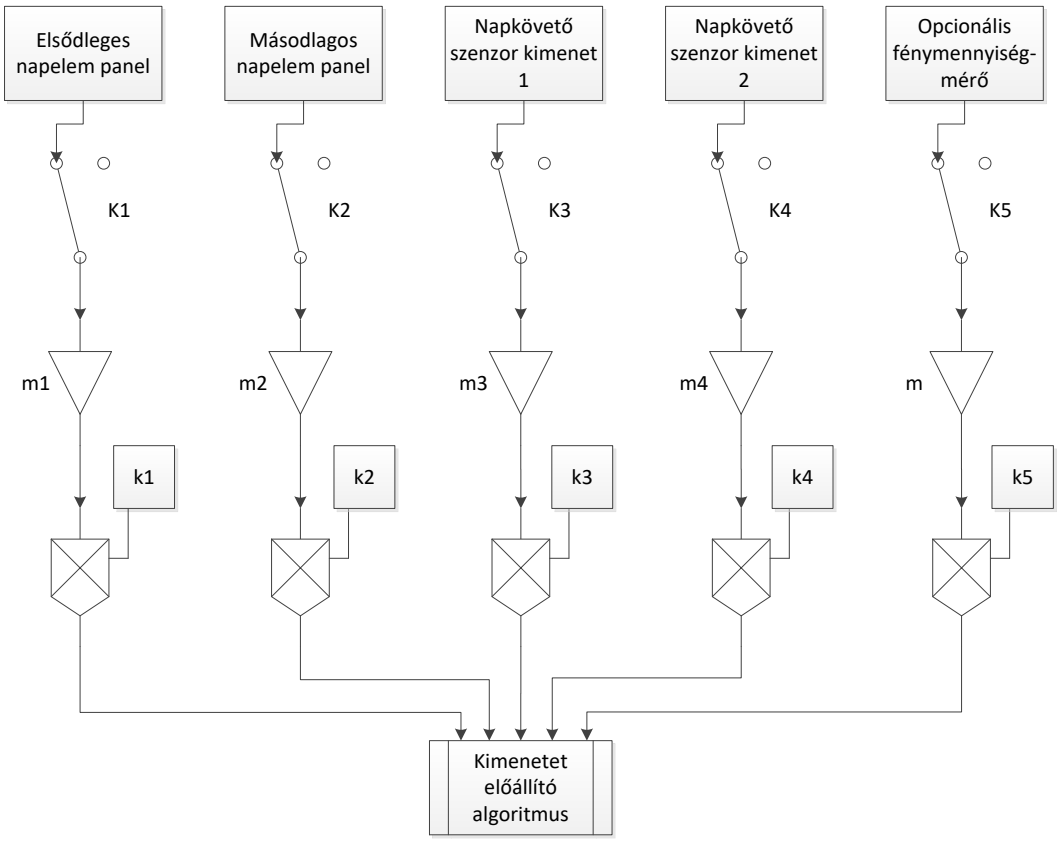


5. Ábra: Nap követő algoritmus

Az elsődleges napelem panel, a tartalék napelem panel és a nap mozgását detektáló érzékelők kimeneteinek súlyozott, valamint normált értékei felhasználhatóak a beérkező fénymennyiség megállapítására. [15] A beérkező fénymennyiség ismeretében kalkulálható az elsődleges napelem elvárt kimeneti teljesítménye (adott terhelés mellett), amennyiben ettől eltérő eredményt mér a rendszer a napelem panel hatásfokromlását detektálhatja.

Opcionálisan – mint redundáns érzékelő – a besugárzást érzékelő félvezető is elhelyezhető a napelem mellett, amely katasztrofális meghibásodás esetén nagy segítség lehet a rendszerállapot meghatározásában, a beérkező fénymennyiség mérésében, illetve a napelem

panelek jóságának megállapításában. Szintén alkalmazhatóak a szoftveres többségi -, középérték szavazó vagy egyéb átlagoló algoritmusok (6. Ábra).



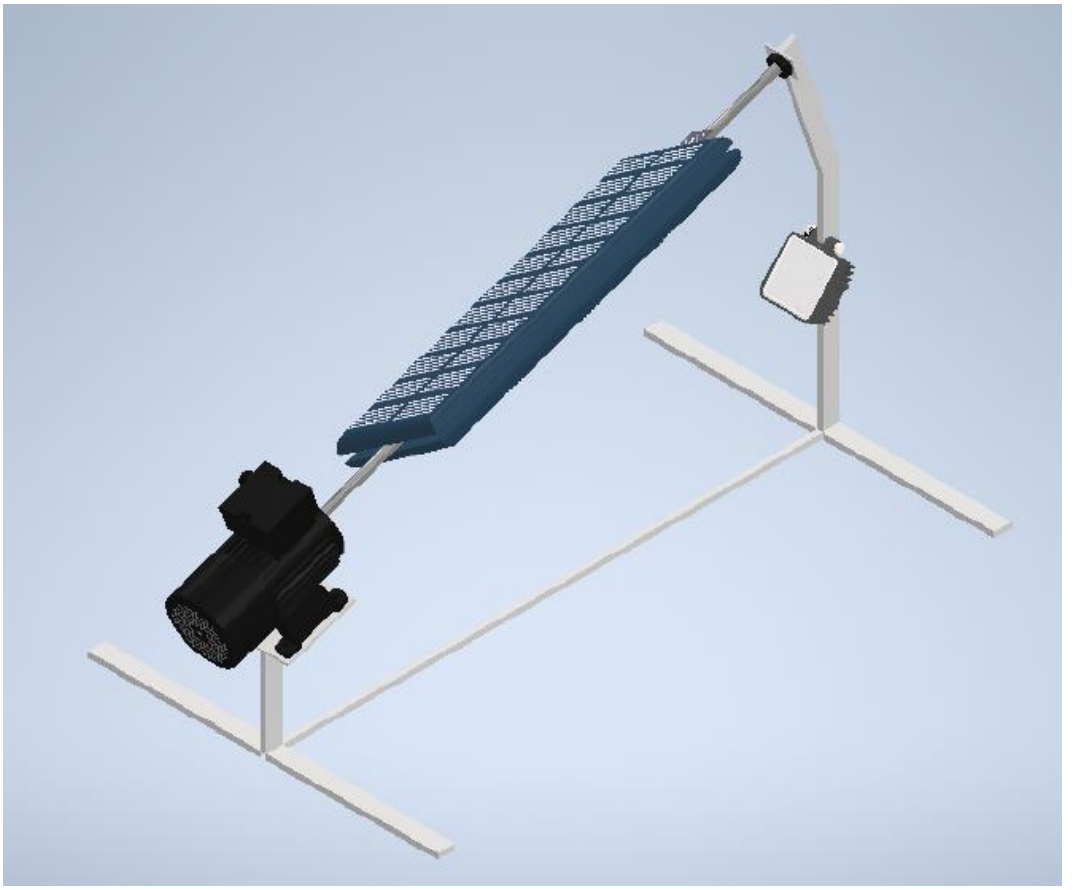
6. Ábra: Szoftveres fénymennyiség mérő algoritmus működési vázlata

A Kn kapcsolókat a vezérlő rendszer inaktiválja amennyiben a bemenő jelet egy másik szoftver-komponens megbízhatatlannak jelöli meg. Az mn erősítők a bemenő jelek súlyozását látják el, a kn konstansok a szorzó áramkörök segítségével a bemenő jeleket normálják.

A fizikai forgást megvalósító működtető egység általában egy villanymotor (jellemzően DC motor), amely a napelemeket magában foglaló mechanizmust egy áttételen keresztül, – opcionálisan egy szöghajtással – illetve egy tengelykapcsoló segítségével forgatja.

Különösen fontos egy napelem-pótlási stratégia kidolgozása. Az aktív elem önmagával való összehasonlítása nem eredményezhet megoldást. Opcióként felmerül, ha több hasonló napelem van a rendszerben, azok összehasonlíthatóak egymással. Ha csak egy duplikált napelem van a javasolt elrendezésben, akkor annak állapotáról a tartalék napelemmel történő összevetése adhat információt. A 7. Ábra szerinti konstrukcióban a még nem használt (azaz hibátlan) tartalék nap-elem, a szórt fény vagy mesterséges megvilágítás segítség-

ével nyújt használható mérési adatokat. Az alacsony mérnökóra segítségével implementálható kiértékelés egy empirikus úton megállapított look-up-table interpolációjával könnyedén elvégezhető.



7. Ábra: Egytengelyes forgási mechanizmussal rendelkező redundáns napelem panel izometrikus ábrája

ÖSSZEFOGLALÁS

Tanulmányom legfontosabb eredményének azt tartom, hogy a bemutatott konstrukció alapján a szigetüzemű napelemmel táplált berendezések tápellátásának megbízhatósága nagy mértékben növelhető. Az önellenőrzést lehetővé tevő hardverelemek, illetve a hozzájuk társuló vezérlő rutinok felhasználásával a berendezés képes alkalmazkodni a környezeti változásokhoz, valamint képes a működési idejét meghosszabbítani az esetleges meghibásodások esetén. Az egytengelyes forgási mechanizmussal rendelkező duplikált napelem panel további robusztusságot ad a rendszernek. A szerző meggyőződése, hogy a műszaki berendezések kiegészítése a vázolt rendszerelemmel, releváns piaci, gazdasági és környezeti hatással rendelkezik.

FELHASZNÁLT FORRÁSOK

[1] O. Serlin. 1984. „*Fault-Tolerant Systems in Commercial Applications"*. Computer 17, 8. August 1984. 19–30. pp. DOI:10.1109/MC.1984.1659214

[2] FIAMM Energy Technology. „*SMG Battery Range*". https://www.fiamm.com/fileadmin//user_upload/SMGS_FOLDER_EMEA_ENG.pdf (letöltve: 2020.10.09.)

[3] Boes EC, Maish AB. „*Advances in concentrator technology*". In: Proceedings of 19th IEEE Photovoltaic Specialists Conference, 1987. p. 985–91

[4] Gay CF, Yerkes JW, Wilson JH. „*Performance advantages of two-axis tracking for large flat-plate photovoltaic energy system"*. In: Proceedings of 16th IEEE Photovoltaic Specialists Conference, 1982. p. 1368–71

[5] P. Roth, A. Georgiev, H. Boudinov. „*Cheap two axis sun following device*". Energy Conversion and Management. Volume 46, Issues 7–8. 2005. pp. 1179-1192. ISSN 0196-8904. https://doi.org/10.1016/j.enconman.2004.06.015.

[6] İbrahim Sefa, Mehmet Demirtas, İlhami Çolak. „*Application of one-axis sun tracking system"*. Energy Conversion and Management. Volume 50, Issue 11. 2009. Pages 2709-2718. ISSN 0196-8904. https://doi.org/10.1016/j.enconman.2009.06.018.

[7] B.P. Edwards. „*Computer based sun following system*". Solar Energy, 21 (6) (1978), pp. 491-498

[8] Maish AB. „*A self-aligning photovoltaic array tracking controller"*. In: Proceedings of the 20th IEEE Photovoltaic Specialists Conference, 1988

[9] Jerin Kuriakose Tharamuttam, Andrew Keong Ng. „*Design and Development of an Automatic Solar Tracker. Energy Procedia"*. Volume 143. 2017. pp. 629-634. ISSN 1876-6102. https://doi.org/10.1016/j.egypro.2017.12.738.

[10] S.S.N. Rumala. „*A shadow method for automatic tracking"*. Solar Energy, 37 (3) (1986). pp. 245-247

[11] V. Poulek, M. Libra. „*New solar tracker"*. Solar Energy Materials and Solar Cells. Volume 51, Issue 2. 1998. Pages 113-120. ISSN 0927-0248. https://doi.org/10.1016/S0927-0248(97)00276-6.

[12] A. Szűts, „*Developing a Complex Decision-Making Framework for Evaluating the Energy-Efficiency of Residential Property Investments"*. ACTA POLYTECHNICA HUNGARICA 12 : 6 pp. 231-248. , 18 p. (2015)

[13] A. Szűts, I. Krómer: „*Estimating Hungarian Household Energy Consumption Using Artificial Neural Networks*", Acta Polytechnica Hungarica, Vol. 11, No. 4,pp. 155-168,2014

[14] A. Szűts, I. Krómer: „*Developing a Fuzzy Analytic Hierarchy Process for Choosing the Energetically Optimal Solution at the Early Design Phase of a Building"*, Acta Polytechnica Hungarica, Vol. 12, No. 3, pp. 25-39, 2015

[15] G. Györök, „*Programozható analóg áramkörök mikrovezérlő környezetben"*, vol. 1. Székesfehérvár: Óbudai Egyetem, 2013.

CONNECTION BETWEEN CALL CENTERS AND SENSE OF SECURITY DURING THE COVID-19 EPIDEMIC

A TELEFONKÖZPONTOK ÉS A BIZTONSÁGÉRZETÜNK ÖSSZEFÜGGÉSEI A COVID-19 JÁRVÁNY IDEJÉN

HAJDU Beáta[1]

Abstract

I find it important to highlight the validity of my research area, the relevance of this article, and the value of it regarding the field of security science. Call centers and telephone switchboards are in the focus of my study. We do not have to go back too far in time to see that operating telephone switchboards became fundamental in terms of our security. The relevance of this topic was verified when the COVID-19 epidemic started. The reason for this is one of first measures implemented by the countries that were affected by the pandemic: telephone centers were set up on national, regional or county level. The set up of these centers was essential for every country: it was used for reporting and different authorities were directed with the help of telephone switchboards, which are also a proper mean for people in terms of getting information. One way of protection against the epidemic is social distancing and avoiding personal meetings, which was greatly assured by telephone switchboards set up in a methodic and goal oriented way.

Keywords

telephone switchboard, security awareness, human resourses, COVID-19

Absztrakt

Fontosnak tartom, hogy rávilágítsak a kutatási területem létjogosultságára, és ezen cikk relevanciájára, illetve a biztonságtudományi területen belüli értékére. A kutatásom a call centereket, telefonközpontokat helyezi origóba. Az időben nem kell messzire menni, hogy láthatóvá váljon a telefonközpontok működtetése a biztonságunk egyik alapköve lett. A COVID 19-es világjárvány megjelenésével bizonyított a téma mivolta, hisz a pandémia által érintett országokban mi volt az első intézkedések egyike? - felállítottak országosan, vagy régiónként, megyénként telefonos központokat. Minden ország számára fontos volt a központok kialakítása, ezen csatornát használhatták a bejelentések eszközlésére, illetve a különböző hatóságokat is telefonközpontok segítségével navigálták, továbbá alkalmas az állampolgárok tájékozódására. A járvánnyal szembeni egyik védekezési lehetőség a távolságtartás és a találkozók kerülése, ezen védekezési lehetőség biztosítását nagyban segítette a módszeresen és feladatorientáltan létrehozott telefonközpontok működése.

Kulcsszavak

telefonközpont, biztonságtudatosság, humán erőforrás, COVID-19

[1] hajdu.bea31@gmail.com | ORCID: 0000-0002-2195-1505 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A 2020-as évben a hivatásos életben folyó kontrolláltsággal összefüggésben megjelent cikkemben egy speciális objektumban, kritikus infrastruktúrában szolgálatot teljesítő telefonközpontos, humánerőforrás precizitást igénylő tevékenységéről írtam. Vizsgáltam azt a felvetést, miszerint a szóban forgó objektumok telefonközpontjaiban dolgozó kollégákat a folyamatos kontrolláltság nemhogy zavarja, hanem a biztonságérzetüket nagymértékben javítja. Egy bevetés irányítási központban dolgozó humán erőforrásnak minden egyes hívást komolyan kell vennie. [1] Mindez azt jelenti, hogy döntéselméleti szempontból minden új döntési helyzet információhiányos állapotnak számít. Ilyen helyzetben pedig nem lehet a jó döntés feltételeinek maradéktalanul megfelelni. A feltárt témakör kapcsán a biztonság, vagy a biztonságtudatosság fogalmi körét alapjaiban és részleteiben feltárni lehetetlennek bizonyult, mert mindenki mást gondol, más metódusban értelmezi. Azonban egy biztos, hogy a biztonság csak akkor létező teória, ha mellé párosítjuk a veszély, vagy a fenyegetés kollokációt. [2; 4-6.o.]

Logikus párhuzamnak gondolom - és ezen teória által folytathatom a Biztonságtudományi Szemlében megjelent írásom rendszerszemléletét, jelen esetben más aspektusban vizsgálva - hogy a pandémiával szembeni küzdelem érdekében létrehozott telefonközpontokat speciális objektumoknak, vagy akár kritikus infrastruktúráknak tekintsem, hisz olyan nemzeti és országos, illetve lakosság számára nélkülözhetetlen feladatokat látnak el, hogy a fogalomkört lefedetnek lehet tekinteni.

Természetesen egy-egy infrastruktúrának nem minden eleme tekinthető kritikusnak, még abban az esetben sem, ha kritikus infrastruktúráról beszélünk. Ezért szükség lehet azonosítani és meghatározni azokat az elemeket, amelyek a legkritikusabbak, azaz amelyek támadásával, és amelyek kiesésével, részleges, időleges, vagy teljes működésképtelenségével a legjelentősebb mértékben okozhatók komoly humán (emberi élet), vagy anyagi (gazdasági) kár. Az infrastruktúrák méretének és összetettségének mérése lehetőséget teremthet beazonosítani ezeket a kritikus elemeket. A kritikus infrastruktúrák meghatározása során a rendszerek priorálása is komoly segítséget nyújthat. A feltártak alapján egyértelmű, a kritikus infrastruktúrák tanulmányozása is meglehetősen nehéz és bonyolult feladat úgy, mint az objektumok, a speciális objektumok precíz számbavétele, mert ami kritikus egy objektum, vagy egy szervezet számára, az nem biztos, hogy kritikus az állam számára is. Ráadásul, a pontos meghatározás egy kockázatelemzést feltételez, amivel végképp nem rendelkezik a szóban forgó objektumok mindegyike.[3] Megjegyzésként muszáj említést tenni arról a témában való jártasság bizonyítása érdekében, még akkor is, ha nem is képzi a cikk tematikájának origós tézisét, hogy egyértelmű; „*a kritikus infrastruktúrák védelme és működésének fenntartása, nemzetbiztonsági szempontból minden kormányzat alapvető és létfontosságú feladata*". [4] „*Míg az infrastruktúra fogalma kellő körültekintés árán kielégítő pontossággal meghatározható, a kritikusság ismérvei sokrétűek, szerteágazóak, tudomány- és iparáganként változnak. Egy infrastruktúra tehát nagyon sok szempontból lehet kritikus, kritikussá minősítéséhez viszont az is elég, ha csak egyetlen egy kritérium szerint az. A kritikus infrastruktúra fogalmának meghatározása ennek megfelelően nem egységes."* [5]

A KORONAVÍRUS ÉS A TELEFONKÖZPONTOK KAPCSOLATA

A COVID-19 járvány idején a média permanensen hangoztatta/hangoztatja, illetve az egészségügyi rendszerben tapasztalható, hogy a betegellátásban dolgozók nagymértékben túlterhelhetek, erejükön felül dolgoznak és küzdenek nap, mint nap, hogy emberéleteket mentsenek. A szóban forgó orvosi és szakellátói humánerő team munkáját háttértámogató rendszerek segítik, többek közt pl. a kórházak, a mentők telefonközpontjaiban dolgozók. Ezen telefonközpontok alkalmazottai is óriási leterheltség mellett végzik feladatukat, hisz a pandémia első sorban az egészségügyben dolgozókat érintette a legmélyebben. Persze főhajtás mellett említést érdemel, minden olyan tevékenységet folytató „egység" melynek a járvány terjedésének megakadályozása érdekében, zárva kellett lennie, és mit tettek ezen egységek? – ők is, általában telefonos (és informatikai) rendszerüket bővítették, hisz az érdeklődés irányukban sem csökkent; pl.: oktatási intézmények, művelődési intézmények.

A kutatásom nagy részét a motivációs elméletek és a biztonságtudatos viselkedés, valamint a biztonságtudományi terület összefüggéseinek vizsgálata tette ki. Fontosnak tartom jelen helyzetben a COVID-19 és a telefonközpontok humánerőforrásainak motivációs lehetőségeinek korrelációját vizsgálni. Az analízis azért is releváns, hisz az államok, a kormányok, a munkáltatók minden anyagi forrást a védekezésre fordítottak, így érdekes lehet és jövőbe mutató, hogy a legalapvetőbb – plusz anyagi eszköz biztosítása nélkül, milyen motivációs eszköz alkalmazható a telefonközpontok humánerőforrásaival szemben a biztonságtudatos és erőn felüli munkavégzés érdekében.

A cikkben egy olyan téma kidolgozását találhatjuk melynek célja, hogy választ kapjunk arra, miként tudják a gyakorlatban a vezetők javítani a munkavállalói elkötelezettséget és a munkahelyi légkört és valóban része - e, a vállalati sikereknek a vezető iránti lojalitás. Több tanulmányt értelmezve, majd annak meritumát jelen cikk origójára helyezve arra a következtetésre jutottam, hogy a pandémia idején az emóció fontossága nélkülözhetetlen egy vezetőnek a kellő motiváció eléréséhez a beosztottakkal szemben.

A cikk tézise: egy jó vezető az emocionális eszköztárával motiválhatja kellő mértékben a munkavállalót plusz anyagi elismerés nélkül a COVID-19 járvány ideje alatt a biztonságtudatosság megléte mellett. Az emóció fontossága megkérdőjelezhetetlen a vezető életében, vagyis az érzelmileg intelligens vezetői tevékenység sikere, vagy kudarca nagyban befolyásolja a biztonságérzetét, biztonságtudatosságát mind a humán erőforrásnak, mind a vele kapcsolatba kerülő állampolgárnak.

MOTIVÁCIÓS ESZKÖZTÁR INTERPRETÁLÁSA

Tartalomelméletek

A motivációs elméleteket alapvetően két csoportra oszthatjuk, úgymint tartalomelméletek és folyamatelméletek. Valamennyi tartalomelmélet különböző nézőpontból közelít a motivációkhoz, egyik elmélet sem tekinthető olyan biztos alapnak, melyet a vezetők egyértelműen „használhatónak" tarthatnának, vagy éppen értelmezhetnék a motivációt. A tartalomelméletek azokat az egyénre jellemző motívumokat foglalják össze, amelyek cselekvésre serkentenek bennünket. Tehát alapvetően a tartalomelmélet azt tárja fel, hogy mit akarnak, mire van szükségük a munkavállalóknak, és ezért a vezetőnek milyen eszközöket szükséges alkalmazni motiválásuk érdekében. Az egyes modellek nem konkrét

vezetői ajánlások, amelyeket közvetlenül alkalmazhatunk egyik vagy másik kollégánkra. Egy – egy adott vezetői helyzetben mindig konkrét elemzést kell végezni. Egy cég, egy call center életében a sikerességet mérhetjük gazdasági mutatókkal, pénzügyi erőforrásokkal, az innováció iránti elkötelezettséggel, a versenyképességgel, a humán erőforrás gazdagságával, illetve az intenzifikált szervezetfejlesztéssel, továbbá a biztonságtudatos viselkedés produktív megjelenésével. [6; 7]

A tartalomelméleteket már volt szerencsém sorra venni és vizsgálni témámat érintően 2018-ban és 2019-ben megjelent cikkeimben. Cél volt, hogy választ kapjak, miként is tudják a gyakorlatban a vezetők tartósan fenntartani a motivációt, az érdeklődést azon munka iránt, melyet a kiégés és a fluktuáció jellemez. A szóban forgó szenzitív körülmény nehezítette, hogy a biztonságtudatosság is a munkavállalók primer és szignifikáns jellemzője legyen. A vizsgálat során arra a következtetésre jutottam, hogy a megfelelő hozzáállás a belső motiváció és a biztonságtudatos viselkedés együttes megléte szükséges a kölcsönös együttműködéshez egy cég/egy telefonközpont zökkenőmentes életéhez. Az egyes motivációs modellek nem konkrét vezetői ajánlások, amelyeket közvetlenül alkalmazhatunk egyik vagy másik kollégánkra, hisz abban az esetben, ha egy kritikus infrastruktúra call centeri alkalmazottairól beszélünk sokban más, szigorúbb elbírálás alá esnek, mint egy kereskedelmi tevékenységet végző cég telefonközpontjában. Egy – egy adott vezetői helyzetben mindig konkrét elemzést kell végezni. [8; 9]

Folyamatelméletek

„*A folyamatelméletek inkább modelljellegűek, elvonatkoztatnak a cselekvés céljától, a munka tartalmától, és a motiváció keletkezésének folyamatát, irányát, erősségét elemzik. Ebben az esetben a motiváció a munkatársak cselekvésének megfelelő irányítását, terelését jelenti*". [10] E hatás-törvény két lényeges fogalma a *feltétel* és a *következmény*. Következmény lehet bármi, amit a munkavállaló szeretne elnyerni: pénz, jutalom, dicséret, státusz, kihívó feladat, vagy bármi, ami a motivációinak megfelel. azonban hangsúllyal érdemes még egyszer rámutatni arra, hogy a folyamatelméletek alkalmazására csak akkor kerülhet sor, ha pontos képünk, vagy okkal jónak tartott feltételezésünk van a munkavállaló motivációinak tartalmára. [11]

A motiváció folyamatelméleteinek alapja a tanulásról szóló elméletekhez nyúl vissza. A megerősítésen alapuló tanulási elmélet azt mutatja be, miként viselkedjünk úgy, hogy számunkra kedvező jutalmakat kapjunk, illetve elkerüljük a számunkra kedvezőtlen büntetést. Az egyéni célokat, törekvéseket megértő és jó szervezeti teljesítményre törekvő vezetőknek éppen erre a magatartásra van szüksége, a sikeres viselkedésformákat meg kell erősíteniük, fenn kell tartaniuk.

Szekunder források feltárása az érzelmi intelligenciáról

Az előzőekben megismert elméletek valószínűleg nem célravezető motivációs eszközök egy olyan helyzetben, ahol a napi munkaidő sokszor megduplázódik, ahol minden nap szembesülni kell a halálozási adatokkal, mert az is egy mérőszám. Az ember egy olyan speciális objektum diszpécserközpontjában, ahol az egészségügyi rendszer háttértámogatását végzik nem csak testileg és fizikálisan leterhelt, hanem szellemileg és nagy mértékben lelkileg is elfárad, azonban a biztonságtudatosságuk tovább fokozódik. Tehát ebben a nehéz néha kilátástalannak tűnő időkben kell az objektum munkavállalóit motiválni, hogy még legyen erejük, tartsanak ki és ugyanolyan precízen végezzék munkájukat,

mint a „békeidőkben". Elméletem szerint a szóban forgó szakterület humán erőforrását emocionális tulajdonság nélkül nemhogy motiválni, de vezetni sem lehet. A kutatott területem nagyon érzékeny és a mai világban még nem teljesen elfogadott témát boncolgat. A hipotézis érdekesnek és bátor gondolatnak vélhető, de a következő cikkek segítségével, rávilágítok a fontosságára illetve, hogy a feltevés nem mellőzhető kérdés egy telefonközpont, mint munkahely, pandémia alatti biztonságtudatos életében:

- *„Csaknem mindenkinek vannak tapasztalatai elviselhetetlen munkahelyi feletteseként, akik nehezen tolerálható vagy éppen zűrzavaros személyiségek voltak, s irányításuk alatt kín volt dolgozni. Lehetséges ez még akkor is, ha szakismereteik nem hagytak kívánnivalót maguk után. Az ilyen vezető elől előbb-utóbb megszöknek a beosztottak, vagy megpróbálják megkeseríteni az életét, ami mindenképpen a munka rovására megy. A jó irányítónak nem elég a szakterületen felkészültnek lennie, a sikerhez jól szocializált személyiségre, fejlett érzelmi intelligenciára is szükség van. Szinte magától adódik a következtetés, hogy a sikeres főnöki, vezetői működést is meghatározza az érzelmi intelligencia, illetve az, hogy az ezzel kapcsolatos ismereteket a főnöki pozícióban levők jól hasznosíthatják."* [12]
- *„Minden sikert csak emberekkel való kapcsolatokon keresztül tudunk elérni. Az emberi kapcsolatok irányítását, annak képességét pedig nem az IQ, hanem az EQ – az érzelmi intelligencia – határozza meg. Hogyan ad visszajelzést a beosztottjának egy „igazi főnök"? Durván, érzéketlenül, a másik fél érzelmeire való odafigyelés nélkül. Nem is serkenti így a másik embert hosszú távon magasabb teljesítményre. Valószínű, hogy tudattalan célja az, hogy könnyítsen saját magán, és nem az, hogy a beosztottat segítse jobban teljesíteni. Miért nem tud egy vezető magasabb teljesítményt kihozni az embereiből? Mert nem veszi figyelembe az egyes embereinek belső tulajdonságait, a személyiségüket, és az általános, illetve pillanatnyi érzelmi állapotukat. Egyre több ember felismeri, hogy a sikerhez vezetővé kell válni. Először a saját életünk vezetőjévé, majd – ha még magasabb szintű sikerre vágyunk, akkor – mások vezetőjévé. Az érzelmileg intelligens emberek – a jó vezetők – gyorsan és azonnal olvasnak a beszélgető partnerük mimikájából, és a másik fél érzelmi állapotához igazítják a mondanivalójukat."* [13]

A cikkeket a figyelem felkeltése érdekében, nem a mai „írásokból" merítettem, ezzel is azt hangsúlyozva, hogy jó pár éve szó esik arról, hogy igenis fontos az emóció, de lehet, hogy ezen szellemiségnek csak a koronavírus - járvány adott táptalajt. Az érzelmi intelligencia a gyakorlati életben jelentkező felhasználása rohamosan terjed, egyre nagyobb hangsúlyt kap az a megállapítás, hogy a társas érintkezés terén - emberi kapcsolatokban, a vezetői tevékenységben – szükséges eszköz. Önmagunk, mások, csoportok érzelmeinek kezelésére, irányítására használhatjuk. Tehát, kulcskérdésnek tekinthető a sikerhez vezető úton az érzelmi intelligencia fejlettsége. Nehéz feladat egy vezető számára eldönteni milyen is a helyes viselkedés, hogy célt érjen el a dicsérettel, vagy a megrovással, találja meg a közlési mód arany középútját. Az érzelmi intelligencia, mint kompetencia tanulható és fejleszthető, elsajátítására a speciális objektumok, kritikus infrastruktúrák vezetőinek, energiát kellene biztosítaniuk.

Goleman több tanulmányában rávilágít az érzelmi kompetencia területére; tehát egy vezető kezében a humán erőforrásra vetítve kiváló az egyéni teljesítmények fokozására és ez által a szervezetek eredményességét is döntően befolyásolja. A szakértelmet, vagyis a szakmaiságot a kiinduló helyzet zérójának véli, melyek szükségesek ugyan a munkavégzéshez, de a siker nem tőlük függ. Az előzőeken túl fontos azon készség, hogy menyire tudunk saját magunkkal és másokkal bánni. Magyarázatába a kompetenciának kizárólag érzelmi vonatkozásai maradnak, a kognitív tudást a szakmai ismereteket figyelmen kívül hagyja. Az érzelmi kompetencia – az író felfogásában – az érzelmi intelligenciára épülő olyan személyiségvonás, amely kiemelkedő munkavégzéshez vezet. [14]

AZ ÉRZELMI INTELLIGENCIA TERÜLETEI ÉS KOMPETENCIÁI

Fentebb olvashattuk, hogy releváns az emóció egy vezető eszköztárában, de miből is áll, milyen területei vannak, miből meríthet a kellő motiváció elérése érdekében?

Az érzelmi intelligenciának négy alapterülete van:

- az én-tudatosság
- az önszabályozás
- a társas készség
- a kapcsolatok irányításának képessége, és ezeken belül megannyi kompetencia található.

Mindegyik képesség nagyon fontos, de egyedi méretben járulnak hozzá, hogy a vezetők rezonánsabbá és hatékonyabbá váljanak a telefonközpontok humánerő forrásának irányításában. Az igazsághoz azonban az is hozzátartozik, hogy egy vezető sem, még a legkiválóbbak sem rendelkeznek az előbb felsorolt készségek mindegyikével még „béke-időben" sem, nemhogy egy vészhelyzeti, halálozásokkal teli korban. Alább részletezem a négy alapterületet annak érdekében, hogy világosabban láthassuk, hogy néhány kicsi lépés is elegendő lenne a harmonikusabb és motiváltabb légkör megteremtéséhez úgy, hogy a biztonságtudatosság és a biztonságérzet zavartalanul a munkaadó és a munkavállaló strukturális kompetenciái közzé tartozzanak.

Én – tudatosság

Az én-tudatosság különböző összetevőkből áll, az egyik ilyen fontos rész az érzelmi tudatosság, vagyis az érzelmi tudatossággal rendelkező vezetők tudatában vannak annak, hogy érzelmeik hatnak a viselkedésükre és teljesítményükre. Döntéseikben megmutatkozik az általuk képviselt értékrend, az érzelmi tudatosságuk következtében pedig őszinte, nyílt és megbízható embereknek ismerjük őket.

Az én-tudatosság másik lényeges eleme a pontos önértékelés képessége. A valós önértékeléssel rendelkező vezetők ismerik erősségeiket és hiányosságaikat, a kritikákat és bírálatokat építő jelleggel hasznosítják munkájuk során. A valós önértékelésnek köszönhetően a vezető átlátja a különböző helyzetek veszélyeit és tudja, hogy mikor kell segítséget kérnie és a lépést meg is teszi, „nem dugja a fejét a homokba". Mindezeken túl meglátja azokat a területeket melyekben fejlesztenie kell vezetői képességeit.

Harmadik alkotóelemként említhetjük az önbizalmat. Aki ismeri önmagát az képes felmérni „erőit" és képes meglátni azokat a szituációkat melyekben az adottságai jól kapacitáltathatók, illetve kihívásnak tekinti az általa is nehéznek vélt feladatokat.

Önszabályozás

Az önszabályozás is, hasonlóan az én-tudatossághoz különböző faktorokból tevődik össze.

Az önszabályozás egyik fontos pilléreként lehet említeni az érzelmi kontrollra való képességet. Az önkontrollal rendelkező vezető az egyik leghatékonyabb, hiszen a nehéz helyzetekben sem veszíti el a „fejét". Voltaképpen az önkontroll segít a vezetőnek, a káros indulatokat és érzelmeket háttérbe szorítani.

A rugalmasság képessége is nagyban befolyásoló erejű lehet és az önszabályozás ezen területe akár kifizetődőnek is nevezhető. Hiszen a rugalmas vezetők sokféle elvárásnak meg tudnak felelni és könnyen alkalmazkodnak az új elvárásokhoz, valamint a változások ideje alatt is feltalálják magukat.

A sikervágy is az egyik kelléke az önszabályozási képességnek, ugyanis aki tudatában van a sikervágyának az a vezető igényes önmagával szemben, ezért egyre jobb teljesítményre törekszik, és erre ösztönzi a beosztottjait is.

Az optimizmus a derűlátás is lényeges a jó vezető életében és munkásságában. Az ilyen beállítottsággal rendelkező vezető nem riad vissza a kihívásoktól, az akadályoktól, mert azokban is a lehetőségeket látja. Az optimisták mindig a dolgok jó oldalát tartják szem előtt és nem fecsérelnek energiát a negatívumokra.

Társas készség

A társas készség a szociális kompetenciák egyike.

A tárgyalt készségnek kötelezően említendő részegysége az empátia, mert az empátiával rendelkező vezetők átérzik és megértik mások véleményét és érzelmeit. Az empátia teszi a vezetőket képessé arra, hogy megtalálják a hangot azokkal a beosztottakkal is, akik más értékrenddel rendelkeznek vagy más beállítottságúak, mint ők. Azok a vezetők, akik rendelkeznek ezzel a szociális kompetenciával nélkülözhetetlen tagjai a cég életének.

A kliensközpontúság is a társas készségek egyike, egy vető szerepet betöltő ember életében, mert ezzel a kompetenciával képes felismerni és kielégíteni a megrendelők vagy ügyfelek szükségleteit és igényeit.

Kapcsolatirányító képesség

A kapcsolatirányító képesség szintén a szociális kompetenciák egyike. Az előbbiekben már tapasztaltak alapján, ez a képesség is több alkalmazási területet foglal magába.

Az ösztönző erő olyan terület, melynek hiányában nem képzelhető el magasabb teljesítmény. Segítségével a vezető rezonanciát teremt, példát mutat, így a közös cél felé motiválja a humán erőforrást.

A meggyőzőerő az a részegység, mely egy irányító kezében a siker kulcsa lehet, hiszen ennek az erőnek köszönhetően képes elfogadtatni céljait és szempontjait másokkal, így a cél elérése már közös lehet a csoporttal és nem egyéni harc.

A katalizáló képesség ugyanúgy elengedhetetlen a sikerhez vezető úton, mivel a vezető feladata, hogy új irányvonalakat határozzon meg és változásokat kezdeményezzen, ha szükséges. Viszont az irányvonalakat és változásokat nemcsak meghatározni kell, hanem a vezetőre hárul ezen feladatok végrehajtása és majdani betartatása is.

A konfliktuskezelő képesség nélkülözhetetlen egy munkahelyen, a vezető ennek hiányában sikert sohasem érhet el. Ugyanis a konfliktushelyzeteket jól kezelő felettesek-

nek van a legnagyobb esélye arra, hogy mindenkit meg tudjanak nyerni az együttműködés érdekében. Az ellentéteket és a visszás helyzeteket, képességük révén könnyen elsimítják, így a „társaságot" csapattá tudják kovácsolni.

A csapatmunkára és együttműködésre való képességgel kötelező bővíteni egy igazi vezető repertoárját, mivel azok a vezetők, akik egyben jó csapatjátékosok azoknak van lehetőségük egy barátságos és összetartó munkacsoportot kialakítaniuk. Jellemükből fakadóan időt szánnak kapcsolataik megszilárdítására és elmélyítésére, példát tudnak mutatni tapintatból, tisztelettudásból és együttműködésből. Ez által, mint követendő „minta" fognak a csapat élén tevékenykedni és így, együtt elérhetik a kitűzött célokat.

A kapcsolatépítés lényegét, ha valaki átlátja, igazán sikeres ember lehet. Ezen eszköz használatával a kapcsolati háló kiszélesítése, majdan a kapcsolatok ápolása és fenntartása hozzájárulhat a pozitív végkimenetelhez, vagyis céljaink eléréséhez.[15]

KONKLÚZIÓ

Úgy gondolom a téma relevanciája a XXI. században sajnos bizonyított, az egyes telefonközpontok és az ott dolgozó humánerőforrás nem csak a saját, de mindenki biztonságtudatosságát, biztonságérzetét növelő „eszközök". A cikk tézise, akár konklúzióként is értelmezhető egy jó vezető az emocionális eszköztárával motiválhatja kellő mértékben a munkavállalót plusz anyagi elismerés nélkül a COVID-19 járvány ideje alatt a biztonságtudatosság megléte mellett. Az emóció fontossága megkérdőjelezhetetlen a vezető életében, vagyis az érzelmileg intelligens vezetői tevékenység sikere, vagy kudarca nagyban befolyásolja a biztonságérzetét, biztonságtudatosságát mind a humán erőforrásnak, mind a vele kapcsolatba kerülő állampolgárnak.

Felfoghatatlan, hogy a mai generációnak meg kellett tapasztalnia ezt a borzalmas vírust és a terjedésének megakadályozása érdekében hozott intézkedéseket, azonban jó néhány tapasztalat jövőbemutató értéket képvisel. A kutatók és a hivatalok feladata lesz, hogy kiértékelje, statisztikai kimutatásokat készítsen a tapasztalatok halmazából.

Ezen cikkel bebizonyítottam; ilyen vészes időkben nagy felelősség hárul a telefonközpontok, call centerek, diszpécser szolgálatok vezetőire annak érdekében, hogy a munkavállaló bírja/kibírja az eddig nem tapasztalt terheket, bizonyítottnak gondolom azon véleményemet, hogy az autoriter vezetési stílusa nem megfelelő, vagyis ajánlott lenne eme vezetési stílust mellőzni.

Javaslatként megfogalmazható, hogy a későbbiekben építkezzünk a COVID-19-es járvány idején kiépített emberi kapcsolatokra, értékeljük azok mivoltát és továbbra is használjuk az emocionális eszköztárunkat.

FELHASZNÁLT FORRÁSOK

[1] HAJDU Beáta: Speciális objektumok speciális területe, avagy az objektumok telefonközpontjai; Biztonságtudományi Szemle, 2020. II. évf. 1.szám, 39-48, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/49/44 (letöltve: 2021. május 15.), ISSN 2676-9042

[2] BEREK Lajos – BEREK Tamás – BEREK László: Személy- és vagyonbiztonság; Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar kiadványa, Budapest, 2016., ISBN 978-615-5460-94-4, 4-100.
[3] BUKOVICS István – VAVRIK Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés; Hadmérnök, 2006. december, ISSN 1788- 1919 http://zrinyi.zmne.hu/hadmernok/archivum/2006/3/2006_3_bukovics.html (letöltve: 2018. december 9.)
[4] HAIG Zsolt: Az információs társadalmat fenyegető információlapú veszélyforrások; Hadtudomány, 2007/3., ISSN: 1215-4121, 37-56. http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/2201/hadtud_2007_3_haig.pdf?sequence=1&isAllowed=y (letöltve: 2019. május 22.)
[5] PRÉCSÉNYI Zoltán – SOLYMOSI József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé; Hadmérnök, 2007. március, ISSN 1788- 1919, http://www.hadmernok.hu/archivum/2007/1/2007_1_precsenyi.html (letöltve: 2018. december 9.)
[6] VARGA János – CCISZÁRIK – Kocsir Á.: 2015: Versenyképességi átrendeződés Közép-Kelet Európában, fókuszpontban a V4 országok, Kárpát-medencei versenyképesség - 6. Báthory – Brassai Konferencia Kötete, Óbudai Egyetem, 2015. május 27.-28., 316.-335. pp., ISBN: 978-615-5460-38-5
[7] VARGA J. – CSISZÁRIK - Kocsir Á.: 2016: A szervezetek versenyképességének alapjai: stratégiai menedzsment a hazai vállalkozásoknál, Vállalkozásfejlesztés a XXI. században VI. – Tanulmánykötet, Óbudai Egyetem, Keleti Károly Gazdasági Kar, 433-458. pp., ISBN: 978-615- 5460-78-4
[8] HAJDU Beáta: Egy sikeres cég mérföldkövei és a biztonságtudatos viselkedés kohéziói, 2018., In: Monika Gubanova (szerk.), Nyitra: Slovak University of Agriculture in Nitra, pp. 153-159., ISBN:978-80-552-1839 -7
[9] HAJDU Beáta: Motivációs eszközök alkalmazásának lehetőségei egy call centeren belül a biztonságtudatos szervezet ernyője alatt, 2019., In: Monika Gubanova (szerk.), Nyitra: Slovak University of Agriculture in Nitra, pp. 58- 67., ISBN 978-80-552-2018-5
[10] BAKACSI Gyula, 2015, A szervezeti magatartás alapjai, Semmelweis Kiadó, Budapest, ISBN: 978-963-331-313-8
[11] KELKO Tamás: Mi motiválja valójában a munkavállalókat? 2017., https://www.kelko.hu/mi-motivalja-valojaban-a-munkavallalokat/ (letöltve: 2021. május 15.)
[12] http://munkaugyilevelek.hu/1999/05/a-vezetoi-erzelmi-intelligencia A vezetői érzelmi intelligencia. – Az empátia nélkülözhetetlen. A Munkaadó Lapja. 1999. május 15. 17. szám (letöltve: 2021. május 15.)
[13] BOÉR Tamás: Érzelmi intelligencia – kulcs a sikerhez. Pozitív Gondolkodás Magazin. 2012. áprilisi szám. pp. 34-35.
[14] Daniel GOLEMAN: Social intelligence, New York, Kiadó: Bantam Dell, 2007., ISBN: 978-0-553-38449-9
[15] Velibor Bobo KOVAC: Basic motivation and human behaviour, London, Kiadó: Palgrave Macmillan, 2016., ISBN: 1137470550

MEDIA REPRESENTATION OF THE HUMAN-ROBOT (HUMAN-MACHINE)

AZ EMBER-ROBOT (EMBER-GÉP) MÉDIAREPREZENTÁCIÓJA

KISS Csaba[1]

Abstract

Tool making makes a person's life easier. Over the years, our tools became more and more complex until they were able to imitate human activity, ie they grew into robots. In the publication, I map the relationship between fantasy and reality from the perspective of robots according to a qualitative research form in chronological order. Reality is nothing but the development of science that precedes and follows the world of fantasy that appears in films. Because of the sea of robot-related films that have already appeared, the publication does not aim to analyze all robot-related films, only successful films selected by the author. The analysis is carried out along the computer that appears spectacularly in the films, ie artificial intelligence, communication, the ability of robots, the use of robots, and scientific discoveries. Movies always want to entertain and science wants to get to know our world and make our lives easier. Through the films I have analyzed, I intend to examine the interplay between fiction and science.

Keywords

robot, science, android, interaction

Absztrakt

Az eszközkészítés megkönnyíti az ember életét. Az eszközeink az évek múlásával egyre összetettebbek lettek, mígnem képesek az emberi tevékenységet utánozni, azaz robotokká nőtték ki magukat. A publikációban időrendi sorrendben feltérképezem kvalitatív kutatási forma szerint a robotok szemszögéből a fantázia és valóság kapcsolatát. A valóság nem más, mint a tudomány fejlődése, ami hol megelőzi, hol követi a filmekben megjelenő fantázia világát. A már eddig is megjelenő tengernyi robotokkal kapcsolatos filmek miatt a publikációnak nem célja minden robotokkal kapcsolatos filmet elemezni csak a szerző által kiválasztott közönségsikeres filmeket. Az elemzés a filmekben is látványosan megjelenő számítógép, azaz mesterséges intelligencia, kommunikáció, robotok képessége, robotok felhasználása, tudományos felfedezések mentén történik. A filmek mindig is szórakoztatni akarnak a tudomány pedig megismerni világunkat és megkönnyíteni életünket. Az általam elemzett filmek révén meg kívánom vizsgálni a fikció és a tudomány egymásra hatását.

Kulcsszavak

robot, tudomány, android, interakció

[1] publikacio.kisscsaba@gmail.com |orcid: 0000-0002-7265-8704 | chief officer, Hungarian Armed Forces Reserve and Support Command | főtiszt, Magyar Honvédség Tartalékképző és Támogató Parancsnokság

BEVEZETÉS (INTRODUCTION)

Az ember fantáziáját mindig is izgatta az hogyan lehetne az életét megkönnyítő eszközöket kitalálni. Minden korban voltak feltalálók, akik az eszközkészítés művészetét egyre magasabb szintre tudták emelni. Ezek az eszközök az évek múlásával mindig bonyolultabbak, míg az eredményük egyre látványosabb lett (pl.: önállóan működő szövőszék). Az önmagától mozgó tárgyaknak a megnevezése automaton (automata) volt. Az ügyes emberi feltalálók az ókorban és a középkorban még nem mesterséges intelligenciát [1], hanem olyan szerkezeteket találtak fel, amelyek általában az intelligenciával kapcsolatos tevékenységeket végeztek. A működés egyszerű a szerkezeti elemeik megfelelő sorrendben és időben meghatározott mozgásokat végeznek, és így végül lehetségessé vált olyan mozgások utánzása, amely élőlényekkel kapcsolatos tevékenységeket modellez, mint például az emberét.

ELMÉLETI ALAPVETÉS

Az eszközkészítés alapvető mozgatórugója a képzelőerő. A képzelőerő vagy fantázia, ami nem más, mint az elme új gondolatokat teremtő képessége addig még nem létező fogalmakat, elképzeléseket hoz létre. Ezek az új gondolatok tették lehetővé többek között a kibernetika megszületését is. A kibernetika pedig a mesterséges intelligencia megjelenését segítette elő [6]. A mesterséges intelligencia természetesen a katonai robotoknál is megjelenik, mint például 'Hercules', 'Drone', 'Battlefield Extraction-Assist Robot (BEAR)', 'BigDog', 'Atlas' [15]. A mesterséges intelligencia léptékei a testen viselhető okoseszközöktől az intelligens földig mindegyike megtalálhatóak a filmekben [14]. Ugyancsak megtalálhatóak a mesterséges intelligencia, mint az emberek és aktivitásaik érzékelésétől a társadalmi kontextusban tanulni az emberektőlig [12]. A filmekben a robotok önállósági fokát egy tízes skála mentén lehet értelmezni, ahol az egyes a 'Nem nyújt semmilyen segítséget mindent az ember csinál', a tízes pedig 'Maga dönt el mindent, automatikusan működik, figyelmen kívül hagyva az embert' [14]. A robotokat számos szempont szerint lehet osztályozni az egyik leg elfogadottabb a Libin és Libin felosztás [11], ahol az ipari robottól a társasági robotig foglalták rendszerbe a robotokat. Ezek mindegyike visszaköszön a filmekben. A szeretet is megjelenik a filmbéli robotoknál. A szeretet minden változata az 'Anyai szeretettől' a 'Kedves szomszéd'-ig [10]. A filmben terápiás robotok is megjelennek, amik a jövőben az ember bizalmasai lehetnek [9]. A filmekben, azaz a fantázia világában a robot már képes átvenni az ember helyét szerepét képes helyettesíteni őt. Ezzel szemben a valóságban csak idő kérdése az ember feletti általános mesterséges intelligencia megalkotása, ami a korábbi technológiáknál sokkal nagyobb mértékben fogja átalakítani az életünket [8]. „A közeljövőben gyökeresen megváltoznak mindennapjaink, akárcsak az egészségügy, az igazságszolgáltatás, a hadászat és jogrendszer, a magántulajdon és a munkahelyek megszűnésével pedig a gazdaságban ma érvényesülő elvek is értelmüket vesztik." [8]. Napjainkban, ahogy a számítógépek tárkapacitása, illetve számítási sebessége növekszik, a kérdés az lett, mire és milyen módon tegyük alkalmassá a számítógépet. A mesterséges intelligencia fejlődése olyan problémák megoldási eljárásaira keresi a választ, amelyeknek a kezelésére pillanatnyilag még nem léteznek begyakorlott módszerek [7]. Az intelligens robotok megszületése azonban a vártnál sokkal lassúbb folyamat. Számos rendkívül bonyolult probléma merül fel, többek között a tudatosság és a környezet hatásainak kérdése [5]. A mesterséges

intelligencia képes érzékelni környezetét, feldolgozza amit észlelt, problémákat old meg, és konkrét cél elérése érdekében tervezi meg lépéseit [4]. A technika fejlődése egyre inkább közelebb hozza az emberiséget a mesterséges intelligencia megteremtéséhez. A kérdés ősi: „mi célból akarjuk mi, emberek az értelem mesterséges változatát létrehozni?"[3]. A filmek fantázia világa természetesen választ ad a kérdésre hisz a filmekben nincs mit veszíteni, viszont a tudomány ezzel szemben, azaz az emberiség ezzel szemben sokat kockáztat [2]. A kockázat következménye pedig igen befolyásoló lehet az emberi életre akár csak a globális felmelegedés vagy egy világjárvány.

KUTATÁSMÓDSZERTAN

A képekben való gondolkodás képessége egyidős az emberiséggel. A képek hangulatot érzést közvetítenek, amit kihasznál a filmipar különösképpen a reklámkészítők. A filmek vizsgálatakor csak részben követtem a vizuális történetmesélés elemzés elvét. A filmekben megjelenő robot vagy mesterséges intelligencia és a kor tudománya közötti kapcsolatot kerestem. Hipotézisem, hogy a legmodernebb technikai megoldások megjelennek a filmekben, illetve a filmekben bemutatott fiktív technikák többsége idővel megjelenik a valóságban. Ilyen szemszögből a film története nem befolyásoló tényező sokkal inkább az ember és robot közötti interakció. Ma már biztosan állíthatjuk, hogy a mesterséges intelligencia létrehozása és fejlesztése elkerülhetetlen. A kérdés az, hogy mennyire engedjük szabadon működni vagy ellenőrzés alatt tartani. A Sheridan-skála pontosan meghatározza a működési önállósági fokokat. Hipotézisem, hogy a filmekben megjelenő MI fejlettségi foka beazonosítható a Sheridan-skála szerint és a fejlettségi fokának magasabb szintre kerülése nyomon követhető a filmekben [16].

AZ ELSŐ LÉPÉSEK (THE FIRST STEPS)

Robot születik

A cseh feltaláló Karel Čapek RUR (Rossum Universal Robots) nevezetű játéka népszerűsítette 1921-ben egy szintetikus anyagból készült ember-szerű gépet a „robot"-ot. (A „robot" szó a cseh nyelvben „robota", melynek értelmezése: szolgaságban tartani.)
1927-ben Fritz Lang filmjében láthatták az első robotot a nézők, amely filmvásznon szerepelt Metropolisban. Ez a robot „gép-ember", a gynoid humanoid robot, másnéven „paródia", „Futura", „Robotrix" vagy a „Maria megszemélyesítőjeként" volt ismert.
S innentől kezdve csak az ember fantáziája szabott határt a robotok filmen történő fejlődésének az emberrel való együttműködésének és mivel az ember szeret borzongani a robot emberrel szembeni küzdelme is megjelent a filmeken. A filmtársaságok hamar ráéreztek ennek az új robot jelenség bevételre gyakorolt hatására. A mai napig a tudományos-fantasztikus filmek kategóriájában több mint 200 alkotás született [17].
A tudomány 1927-ben az elektroncsövek és a lyukkártyák világát éli [18], ami előrevetíti az akkor ismert világ változását. 1936-ban megjelenik az első programozható elektromechanikus számológép [18], amit még elektroncsövek építenek fel, de már látható a tranzisztor megjelenése (1947) [18], ami nemsokára kiváltja az elektroncsöveket.

Mesterséges Intelligencia születik (MI)

A nap, mikor megállt a Föld (1951) A film érdekessége, hogy szerepel benne egy Gort névre hallgató kétméteres robot, ami lézerfegyverével védi a főhősünk űrhajóját. A

lézerfegyver megjelenése a filmben azért izgalmas, mert az első lézert az amerikai Theodore Harold Maiman fejlesztette ki 1960-ban [18] a film elkészülte után.

Tiltott bolygó (1956) Egy robot Robby, ami készségesen segíti a hőseinket egy távoli bolygón az Altaira 4-en. A robot mesterséges intelligenciája sokoldalúvá teszi őt és az embert támogató kisegítő fellépése sok szimpatizánst szerzett a 2257-ben játszódó filmnek. A film érdekessége még, hogy a zenéjét csak elektronikus eszközökkel hozták létre.

A tudomány begyorsít 1957-ben megjelenik az első műhold a Föld körül a szovjet Szputnyik-1. 1958-tól a tranzisztor alkalmazásával a csöves technikákat leváltja egy gyorsabb megbízhatóbb és olcsóbb technika [18]. Megjelennek a tranzisztoros rádiók, amik hordozható kivitelűek és az autókba is beépítik. A számítógépek fejlődése eddig még nem látott gyorsaságot érnek el, ami a felhasználásuknak a területét is hirtelen kitágítja. 1960-ban a hadseregben megjelenik egy igény, számítógépes hálózat kiépítésére. 1961 az első ember a világűrben Jurij Alekszejevics Gagarin. A számítógép területén 1964-ben megjelenik a BASIC program nyelv és a grafikus monitor [18]. 1966-ban José Silva megalkotja a később az egész világon a legelterjedtebb személyiségfejlesztő módszert az Agykontrollt, azaz az agy hatalma a test felett, amit több film is átvett alapmotívumként. 1969-ben megrendezik az első Mesterséges Intelligencia (MI) [4] konferenciát és ember lép a Holdra.

Személyi számítógép születik

1971-ben megjelenik az első személyi számítógép, ami az embereket a filmekben látott robotvilág felé repíti, s ekkor már úgy érzik ez a változás nem megfordítható. Gépen keresztüli kommunikációra 1972-ben megszületett az első e-mail-program. 1973-ban létrejön az első mobiltelefon hívás egy hordozható készülék segítségével [18].

Feltámad a vadnyugat (1973). Időutazás, ahol a nyaralni vágyókat a kornak megfelelő jelmezbe öltöztetett androidok fogadják. Az androidok minden igényét kielégítik az időutazóknak, mígnem a karbantartók észreveszik, hogy egyre több a meghibásodás a robotok körül. Az androidok, amik képesek akár szeretni is, önálló életre kelnek. Az androidok ellenőrzését és programozását a kornak megfelelő szintű számítógépeken végzik.

Mikroprocesszor születik

1974-ben az elektronikai alkatrészek méreteinek csökkentése nem áll meg, megjelenik a mikroprocesszor és velük együtt a nagy mennyiségben eladható otthoni számítógépek [18]. Megjelennek a számítógépes játékok és azok programozói, akik tudásukat különböző tanfolyamokon és könyvekben tanítják. A programozás elérhetővé válik mindenki számára, ekkor jelenik meg először az „internet" kifejezés egy TCP (Transmission control protocol) tanulmányban. 1981-ben megjelenik az első hordozható számítógép [18]. A mobiltelefonok is fejlődnek létrejön az 1G generáció automatikus celluláris hálózat.

Szárnyas fejvadász (1982) Ez a film is a jövőbe repít minket a helyszín Los-Angeles, ahol a megszökött replikánsok, azaz ember kinézetű androidok próbálják bebizonyítani, hogy ők is emberek nekik is vannak érzelmeik.

Virtuális valóság születik

1983-tól elérhetővé válnak a kézi rádiótelefonok és a rádiótelefon-hálózatok gomba módra szaporodnak a világon [18]. Megjelenik a virtuális valóság Myron Krueger által Artficial Reality programjában, aminek a lényege egy számítógéphez csatlakoztatott kamera,

amely továbbítja a gépnek az ember képét, ami azt belekeveri a programba. A virtuális valóság elengedhetetlen eszköz lett a későbbi filmek és játékok megalkotásánál és oktatásban is, hisz először a vadászpilóták képzésére használják majd 1986-ban.

Terminátor - A halálosztó (1984) Az öntudatára ébredt Skynet számítógépes rendszer kiírtja az emberiséget, azaz a film bemutatja a küzdelmet ember és gép között az ember és a mesterséges intelligencia között. Mivel az ember mégis nyerésre áll ebben a küzdelemben a Skynet visszaküld a múltba egy androidot, hogy végezzen ki egy húsvér embert, azaz már nem tabu a robotnak ember ellen fordulnia.

A ROBOTVILÁG (THE ROBOT WORLD)

Robot a műtőben

1985-ben az Amerikai Egyesült Államokban először használtak robotot egy idegsebészeti beavatkozásnál. Ez a siker több filmben visszaköszön, mint a robot, ami az embert diagnosztizálja, műti, gyógyítja vagy életben tartja. 1986-ban a Szovjetúnió elkezdi építeni a MIR űrállomást, ami a Föld körül keringő tudományos kutatásoknak helyt adó űrkomplekszum.

A bolygó neve: Halál (1986) Bár sokak számára izgalmas film a történet és látványvilága miatt, de a robotok és mesterséges intelligencia szempontjából újat nem hozott. A gép kiszolgálja az embert az idegen lénnyel szembeni harcában.

Robot és a törvény

A nyolcvanas évek végére az optikai kábelek segítségével a különböző országokban telepített szuperszámítógépeket összekötik. Kialakul egy globális az egész földet átfogó hálózat, aminek a növekedése az újabb számítógépközpontok becsatolásával a mai napig tart. 1988-ban a számítógépeken megjelenik a 3 dimenziós grafikus feldolgozás és az első hálózaton keresztül terjedő féregvírus [19]. Londonban a PROBOT nevű robot sebészeti beavatkozást végez emberen. 1989-ben megjelenik a Laptop s 1991-ben kidolgozzák a szoftverek multimédiás alkalmazhatóságát. A számítógépes játékokban megjelennek a sikeres filmek főhősei s ez fordítva is igaz.

Robotzsaru (1987) Alex Murphy egy rendőr holttestét sikerül a kor legújabb technológiájával újra életre kelteni, azaz robotzsarut készíteni. Mint robotnak végre kell hajtania az ember utasításait betartva az érvényes törvényeket, de a gépben feléled az ember is. Hol a határ az ember és gép között? Mikor gép és mikor ember? Ezeket a határokat feszegeti a végig izgalmas és fordulatos film.

Robotosodás

A számítógépekben megjelenik a párhuzamos működésű mikroprocesszor, ami egy egyre kisebb méretű mikrochipben működik. A méret csökkenésnek fizikai határa van, amit valahogy ki kell kerülni. Az optika sikeres alkalmazása gép–gép közötti kommunikációra felvetette a gépen belüli alkalmazhatóságának megvizsgálását. 1991-től az optikai, sőt a kvantumszámítógépek megalkotása a cél[19] . A méret csökkenésének az lett az egyik kézzel fogható következménye, hogy a mindennapi eszközeinkben is megjelentek a mikrochippek úgy, mint televízió, rádió, mosógép, hűtőszekrény. A mikroprocesszort elkezdtük mindenhova beépíteni, a játékokba, az autókba, a lakásunkba, sőt az orvosi eszközökbe, egyszóval a környezetünkbe, és szép lassan testközelbe kerülnek azok a találmányok, amiket a filmek fantáziavilága bemutatott.

Terminátor 2. - Az ítélet napja (1991) Ebben a filmben jelenik meg a robot-robot elleni harc körítve a Terminátor 1. -ben megismert történet folytatásaként. A film érdekessége, hogy megjelenik az intelligens fém és a gyermek, aki képes megtanulni, majd irányítani a mesterséges intelligenciával felruházott kiborgot.

Páncélba zárt szellem (1995) Egy kiborg rendőrnő, akinek az egyetlen emberi része az agya egy speciális rendőri egységet vezet, ami kizárólag kiborgokból áll. Az első csoportos kiborg együttműködés. A kiborg rendőrnő képes bármelyik ember emlékeibe belépni és manipulálni azt.

Robot barátság

1996-ban megszületik a világ első klónozott emlőse Dolly, a birka. 1998-ban lipcsei Szívközpontban végrehajtják az első szívkikerülésére szolgáló robotos operációt, majd 1999-ben Kanadában végrehajtják az első lüktető szíven történő sebészeti robottal végzett műtétet. 1998-ban megkezdődik a Nemzetközi Űrállomás építése, az ISS (International Space Station). A mikrochip beépítése a mobiltelefonba annak drasztikus méretbeli csökkenését hozta magával, amivel olcsóbbá és tömegcikké alakult. Nem csak beszéd átvitelére, hanem szöveg átvitelére is képes lett.

Szuper haver (1999) A történet egy kilencéves kisfiú és az űrből érkezett robot körül forog. A kettejük közötti barátság kialakulása gyerek gép közötti interakciók érzelmet csalnak a nézők szívébe. A robot elfogadja a gyermek irányítását s a városba érkező ügynök elöl egy roncstelepen talál menedéket.

Robot önállósodás

A. I. Mesterséges értelem (2001) A film a jövőben játszódik, mikor az embereket a mesterséges intelligenciával ellátott gépek teszik boldoggá. A legújabb fejlesztésű androidok már érzelmet is kapnak, ami felvet egy alapkérdést a robotokkal szemben. Lehetnek-e az androidok szabadok, önálló akarattal vagy csakis az embertől függhetnek?

Én, a robot (2004) A film egy klasszikus témát dolgoz fel: képesek-e az emberformájú robotok átvenni a hatalmat a földön? A nyomozást egy robotfóbiában szenvedő detektív végzi, aki a filmben egy magasabb intelligenciával felruházott robotokkal szemben nyomoz, amik képesek csoportban együttműködni.

2005-ben megjelennek az okostelefonok s ezzel gyökeresen megváltozik az életünk. A sikeres telefonos alkalmazások még inkább ember közelebbivé tette a készüléket azaz szorosabban emberhez kötötte. 2006-ban Olaszországban az első emberi beavatkozás nélküli robot automata operációja sikerrel végződik. A rendszert (da Vinci sebészeti/operációs rendszer) 800 kórházban használják s 2006 végére már több mint 48.000 operációt végeznek vele [20].

Robotok (2005) Ez a film tökéletes példája a gyerekek figyelmének a lekötésére. A robotok emberi érzelemmel vannak felruházva s a film végén a jó elnyeri jutalmát s a rossz pedig a büntetését. A gyerekek fantáziáját megmozgatja a film s a film nézése után sokan közülük robotokat kezdenek építeni s robottá akarnak válni. A film észrevétlen csempészi a gyerek fantázia világába a robot világát.

Robot és ember

A NASA 2011 és 2014 között alkalmazott egy láb nélküli humanoidot, ami segítette az asztronauták munkáját a neve pedig Robonaut volt. 2019-ben egy különleges rakomány indult a Nemzetközi Űrállomásra (ISS) egy humanoid robot Skybot F-850 az ISS első orosz

robotja. A robot képes automata üzemmódban dolgozni, de távolból is irányítható továbbá képes az emberek számára készített eszközök felismerésére és használatára.

Vasököl (2011) A Vasököl névre hallgató robot egy bokszoló robot, ami mesterséges intelligenciájával és erős felépítésével egymás után aratja a győzelmeket a ringben természetesen robotok ellen. Ez harc robot robot ellen az ember alkotta törvényen alapuló s régen csak az ember által végzett sport területén a bokszban.

A robot és Frank (2012) Az öregkort nem lehet elkerülni az egyedüllét megviseli az időseket úgy mint a folyton változó környezet. A robot lehet a megoldás az állandó egyedüllét megtörésére. A film bemutat egy robotot, ami képes egy idősebb ember társaként élni kiszolgálni azt azaz helyettesíteni az emberi társat jóban rosszban.

Tűzgyűrű (2013) Ebben a filmben ember és gép eggyé válik. A robot testében két ember kap helyet, akik képesek egymásra kapcsolódni s így irányítják a géptestet.

Hős6os (2014) Egy gyermek s a robotja egy csapatot alkotnak s szembeszállnak a gonosszal.

Chappie (2015) Chappie egy robot, ami mint egy gyerek tanulnia kell s mindent amit tud saját tapasztalatai útján szerzi meg. A nulláról építi fel a tudását emberi segítséggel emberi tanítással legyen az jó vagy rossz.

Robot vagy ember

Bosszúállók: Ultron kora (2015) Harc a mesterséges intelligencia ellen, amit az ember alkotott a saját védelmére. Legyőzhető-e a magunk alkotta szörny, ami arra a következtetésre jut, hogy csak akkor lesz béke a földön, ha nem lesz több ember?

Ex Machina (2015) A film érzékien mutatja be a tudatára ébredt mesterséges intelligencia küzdését az ember szerű érzéseivel. A kérdés klasszikus: átváltozhat-e emberré a robot? Ha átváltozhat mikor és hogyan vesszük észre?

Páncélba zárt szellem (2017) Egy fontos filozófiai kérdés amit a film feszeget: Képes-e az általunk teremtett mesterséges intelligencia eltitkolni előttünk, hogy nem mi irányítjuk?

2020-ban Sir Nick Carter, az Egyesült Királyság hadseregének tábornoka adott interjút a Sky News-nak, amiben elmondta, hogy az évtized végére a hadseregük negyede robotokból áll majd [13].

ÖSSZEFOGLALÁS (SUMMARY)

Természetesen lehetne folytatni a sort mindenkinek vannak kedvenc filmjei és kedvenc robotjai. Ezek a filmek előkészítik azt a kort, amikor mindenkinek lesz egy személyi robotja úgy, mint most egy személyi számítógépe. Az ember képes a saját érzelmeit kivetíteni, átruházni tárgyakra, élőlényekre ez történik a robotok esetében is. A filmek bemutatják a robotokra kivetített érzelmeinket, félelmeinket, vágyainkat beágyazva a tudományos eredményeink, fantáziánk és az emberiséget érdeklő filozófiai kérdések közé. A filmek gyakran megelőzik a korukat, olyan technikai újításokat mutatnak be, amiket a kor embere még nem tudott használni. A fantázia játéka vagy mindennek van tudományos alapja? Nagyon szoros a kapcsolat tudomány és fantázia között ez a kapcsolat inspirálja az újabbnál újabb ötleteket. Megállapíthatjuk a tudomány és filmek fantázia világával kapcsolatban, hogy a tudomány táplálja a fantáziát és a fantázia táplálja a tudományt.

FELHASZNÁLT FORRÁSOK

[1] Futó Iván: Mesterséges intelligencia 1999, Könyvkiadó: AULA KIADÓ Kft

[2] Pokol Béla: A mesterséges intelligencia társadalma 2018, Könyvkiadó: KAIROSZ Könyvkiadó Kft.

[3] Lábos Elemér: Természetes és mesterséges értelem 1979, Könyvkiadó: Magvető

[4] Alison Cawsey: Mesterséges intelligencia 2002, Könyvkiadó: Panem Könyvkiadó

[5] Henry Brighton – Howard Selina: Mesterséges intelligencia másképp 2004, Könyvkiadó: Edge 2000 KFT

[6] Jenny Raggett – William Bains: Mesterséges intelligencia A-Z 1994, Könyvkiadó: Akadémiai Kiadó

[7] Yoshiaki Shirai – Jun-inchi Tsujii: Mesterséges intelligencia alapelvek, alkalmazások 1987, Könyvkiadó: Novotrade Rt

[8] Max Tegmark: Élet 3.0 2018,Könyvkiadó: HVG Könyvek

[9] Kollár, Csaba ; Ványa, László Szerethetők-e a robotok?: Az ember-robot interakció humán oldalának empirikus aspektusa HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 27 : 1-2 pp. 163-177. , 15 p. (2017)

[10] Kollár, Csaba: Szerethetők-e a robotok: Az ember-robot interakció humán oldalának teoretikus aspektusa HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 26 : különszám pp. 142-154. , 13 p. (2016)

[11] Kollár, Csaba: A mesterséges intelligencia kapcsolata a humán biztonsággal NEMZETBIZTONSÁGI SZEMLE (ONLINE) VI. évf. : 1. szám pp. 5-23. , 19 p. (2018)

[12] Kollár, Csaba:A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, (2019) pp. 47-61., 15 p.

[13] Deborah Haynes: Risk of new world war is real, head of UK armed forces warns [Online] Available: https://news.sky.com/story/risk-of-new-world-war-is-real-head-of uk-armed-forces-warns-12126389 [Hozzáférés dátuma: 3. március 2021.]

[14] Kollár, Csaba: A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2. Budapest, Magyarország: Óbudai Egyetem, Biztonságtudományi Doktori Iskola, (2019) pp. 62-70., 9 p.

[15] Kollár Csaba: A katona-robot interakció fejlődési irányai a következő évtizedekben [Online] Available: https://www.slideshare.net/drkollarcsaba/drkollarcsaba-katonarobotinterakcio [Hozzáférés dátuma: 2. március 2021.]

[16] Steven Jay Schneider: 101 sci-fi film amit látnod kell, mielőtt meghalsz, Gabo Könyvkiadó, Budapest, 2009

[17] Robotok a filmekben [Online] Available: https://www.robotvilag.hu/film [Hozzáférés dátuma: 9.március 2021.]

[18] Műszaki Lexikon I-IV, Könyvkiadó: Akadémiai, 1984 Budapest

[19] Marx György: A Marslakók Érkezése - Magyar Tudósok, akik nyugaton alakították a 20. század történelmét Akadémia Kiadó, Budapest 2000

[20] Lenyelhető robotok a gyógyításban [Online] Available: http://medicalonline.hu/informatika/cikk/lenyelheto_robotok_a_gyogyitasban [Hozzáférés dátuma: 5. március 2021.]

THEORETICAL PROTECTION CAPABILITIES OF THE POLICE OFFICIER, THE ARMED SECURITY GUARD AND THE SECURITY GUARD

A RENDŐR, A FEGYVERES BIZTONSÁGI ŐR ÉS A SZEMÉLY- ÉS VAGYONŐR ELMÉLETI VÉDELMI KÉPESSÉGEI

BORUZS Hunor [1]

Abstract

A comparison-based analysis of the defense capabilities of the police officer, the armed security guard and the security guard cannot be a novelty in itself, as the legislation is known and available to all professionals. However, it cannot be unnecessary either, because despite all this, many misunderstandings and inaccuracies complicate the everyday life of the profession, which is waiting to be clarified. To clarify, I define the concept of theoretical defense capability and deduce its legal source to the level of the individual. I delimit the rights of defense attached to the individual and the monopoly of force provided by the state, and then, on the basis of this, I examine the rights of the individual and the organizations to take action and use the tools. Based on the conclusions of the investigation, it can be determined in which spectrum of protection the police officer, the armed security guard and the security guard can be used optimally. However, the level of defense ability derived on a theoretical level is realized only in the case of the coexistence of several practical factors, therefore it forms the starting point for further professional research.

Keywords

police officer, armed security guard, security guard, theoretical defense capability, violence monopoly

Absztrakt

A rendőr, a fegyveres biztonsági őr és a személy- és vagyonőr védelmi képességeinek összehasonlítás alapú elemzése önmagában nem lehet nóvum, hiszen a jogszabályok minden szakember számára ismertek, elérhetők. Nem lehet azonban szükségtelen sem, mert mindezek ellenére sok félreértés, pontatlanság nehezíti a szakma mindennapjait, melyek tisztázásra várnak. A tisztázás érdekében meghatározom az elméleti védelmi képesség fogalmát, valamint levezetem annak jogszabályi forrását az egyén szintjéig. Elhatárolom az egyénhez, illetve az állam által biztosított erőszak-monopóliumhoz fűződő védelmi jogosultságokat, majd ez alapján végzem el az egyén, valamint a szervezetek intézkedési és eszközhasználati jogosultságainak vizsgálatát. A vizsgálat következtetései alapján meghatározható, hogy a rendőr, a fegyveres biztonsági őr, illetve a személy- és vagyonőr mely védelmi spektrumban alkalmazható optimálisan. Az elméleti síkon levezetett védelmi képesség szintje azonban csak számos gyakorlati tényező együttes fennállása esetén valósul meg, ezért jelen tanulmány kiindulóalapját képzi a további szakmai kutatásoknak.

Kulcsszavak

rendőr, fegyveres biztonsági őr, személy- és vagyonőr, elméleti védelmi képesség, erőszak-monopólium

[1] boruzsh@orfk.police.hu | ORCID: 0000-0002-1795-9387 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A rendészeti szakterület a különböző védelmi spektrumok kielégítésének legmegfelelőbb biztosítása érdekében differencializálódott, így a különböző védelmi feladatok ellátására különböző szervezetek optimálisak. A köz- és magánbiztonság fenntartását biztosító szervek, szervezetek intézkedési, eszközhasználati jogosultságai úgy kerültek kidolgozásra, hogy létrehozásuk célját a lehető leginkább kielégítsék. A szervezetek jelen jogszabályi környezetére irányuló összehasonlítás alapú tudományos kutatás annak ellenére nem érhető el, hogy a szervezetek specialitásai és a szakterület fokozódó fontossága ezt indokolná. Szükséges megvizsgálni a hazai szervezetek védelmi képességeit a védelem fogalmának teljes körében. A különböző szervezetek milyen védelmi területen hatékonyabbak a másiknál, így optimálisan milyen területre alkalmazhatók?

AZ ELMÉLETI VÉDELMI KÉPESSÉG FOGALMI MEGHATÁROZÁSA ÉS FORRÁSA

Az elméleti védelmi képesség alatt joguralmi keretrendszerben a jogszabályok által biztosított védelmi lehetőségeket értjük. Az állam jogszabályok által ruház védelmi lehetőségeket az egyének szintjén bizonyos alapjogok útján, valamint a közös érdekek szintjén az erőszak-monopóliumából fakadó legitim erőszak biztosításának lehetőségével. Az egyén személyének, tulajdonának védelme alapvetően az egyén joga, míg a közrend, közbiztonság védelmét az állam a közhatalom által legitimált erőszak-monopólium útján, annak kötelességeként gyakorolja. A jogok forrásuk alapján történő megkülönböztetésének szemlélete elengedhetetlen ahhoz, hogy szétválaszthassuk az állampolgárok egyéneihez fűződő jogainak gyakorlását, illetve azok átruházását az állam védelmi feladatainak szintjétől.

Az egyéni védelmi képességek megalapozását az egyéntől elidegeníthetetlen módon Magyarország Alaptörvényének V. cikke a következőképpen deklarálja: „Mindenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához.” [1] Ez az alkotmányos alapjog törvényi szinten tovább osztódik a büntetőjog területén a jogos védelem és végszükség, a polgárjog területén a jogos önhatalom meghatározására.

A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 22. § (1) bekezdése alapján „nem büntetendő az a cselekmény, amely a saját, illetve más vagy mások személye, javai vagy a közérdek ellen intézett, illetve ezeket közvetlenül fenyegető jogtalan támadás elhárításához szükséges”. A Btk. 23. § (1) bekezdés alapján „nem büntetendő annak a cselekménye, aki saját, illetve más személyét vagy javait közvetlen és másként el nem hárítható veszélyből menti, vagy a közérdek védelme érdekében így jár el, feltéve, hogy a cselekmény nem okoz nagyobb sérelmet, mint amelynek elhárítására törekedett”. [2] A Polgári Törvénykönyvről szóló 2013. évi V. törvény 5:5. § (1) bekezdése alapján „a birtokost birtokvédelem illeti meg, ha birtokától jogalap nélkül megfosztják vagy birtoklásában jogalap nélkül háborítják”, valamint 5:6. § (1) bekezdése alapján „a tilos önhatalom ellen a birtokos – a birtok megvédéséhez szükséges mértékben – önhatalommal is felléphet”. [3]

Megállapítható tehát, hogy az egyén védelmi alapjogai közé sorolható a jogos védelem, valamint a végszükség. Továbbá állampolgári alapjog a birtokos birtokvédelmi jogosultsága, vagyis a jogos önhatalom. Ezen a ponton lefektethető, hogy az említett alapjogok gyakorlásának vagy átruházásának esetében nem beszélhetünk legitim állami erőszakról.

Az állam erőszak-monopóliumát Magyarország Alaptörvényének C) cikkének (3) bekezdése a következőképpen alapozza meg: „Az Alaptörvény és a jogszabályok érvényre juttatása érdekében kényszer alkalmazására az állam jogosult." [1] A legitim erőszak részletszabályai törvényi szinten kerülnek meghatározásra, de megállapítható, hogy a fogalom kötelező tartalmi elemei közé tartozik, hogy ennek célja a jogszabályok érvényre juttatása, valamint eszköze a kényszer.

ESZKÖZHASZNÁLAT A VÉDELEM ÉRDEKÉBEN

A jogszabályok az egyénnek a részletezett módon biztosítják a védekezés jogát, a védekezéshez használható eszközöket azonban közterületen a közbiztonságra különösen veszélyes eszközökről szóló 175/2003. (X. 28.) Korm. rendelet, köz- és magánterületen a Btk. bizonyos eszközök birtoklásának tiltásával vagy engedélykötelessé tételével szűkíti. Ennek értelmében tilos a közbiztonságra különösen veszélyes eszközt közterületen, nyilvános helyen - ideértve az ott lévő járművek belső tereit is -, valamint közforgalmú közlekedési eszközön birtokolni, ezáltal védekezésre használni. A közbiztonságra különösen veszélyes eszközök közé tartozik többek között az olyan szúró- vagy vágóeszköz, amelynek szúróhosszúsága vagy vágóéle a 8 cm-t meghaladja, a dobócsillag, a rugóskés és a szúró-, vágóeszközt vagy testi sérülés okozására alkalmas egyéb tárgyat kilövő készülék; a jellegzetesen ütés céljára használható és az ütés erejét, hatását növelő eszköz; a lánccal vagy egyéb hajlékony anyaggal összekapcsolt botok, nehezékek; az olyan eszköz, melyből a szem és a nyálkahártyák, illetve a bőrfelület ingerlésével támadásra képtelen állapotot előidéző anyag permetezhető ki; az olyan eszköz, amely az utánzás jellege és méretarányos kivitelezése miatt megtévesztésre alkalmas módon hasonlít a lőfegyverre; valamint az olyan eszköz, amely elektromos feszültség útján védekezésre képtelen állapot előidézésére alkalmas. [4] Továbbá a Btk. köz- és magánterületen is tiltja a 324-325. §-ában meghatározottak szerint a robbanóanyag vagy robbantószer, valamint a lőfegyver vagy lőszer engedély nélküli megszerzését illetve tartását, ezáltal az általuk való védekezést is. [2] Ugyan a lőfegyver illetve lőszer tartására bizonyos esetekben – legfőképp vadászati vagy sport, az esetek töredékében önvédelmi céllal – a részletszabályok engedélyt adnak, az előírt tartási, tárolási rendszabályok a legtöbb esetben nem biztosítják az eszközök jogos védelmi helyzetben történő használatát.

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: Szvmt.) 27. § (3) bekezdése alapján „a személy- és vagyonőr arányos mérvű kényszerítő testi erő alkalmazásával a védett személy biztonságát fenyegető támadást elháríthatja; a védett létesítménybe, területre való jogosulatlan belépést megakadályozhatja, a jogosulatlanul bent tartózkodót onnan eltávolíthatja; a rendezvényt zavaró vagy annak biztonságát veszélyeztető személyt a rendezvényről eltávolíthatja; a pénz- és értékszállítást jogtalanul akadályozó személyt eltávolíthatja, illetve a szállítmány biztonságát fenyegető támadást elháríthatja". Az Szvmt. (4) bekezdése alapján „a személy- és vagyonőr a feladata ellátása során vegyi eszközt, gumibotot, őrkutyát, valamint - az erre vonatkozó jogszabályok rendelkezései szerint - lőfegyvert tarthat magánál és

azokat csak jogos védelmi helyzetben, illetve végszükség esetén alkalmazhatja". [5] A törvényi meghatározásokból levezetve megállapíthatjuk, hogy a személy- és vagyonőrökre vonatkozó eszközhasználati szabályok csupán az egyénhez fűződő alapjogok gyakorlását teszik lehetővé, az erőszak-monopóliumból fakadó legitim erőszak biztosításáról esetükben nincs szó. Mivel a személy- és vagyonőr eszközhasználata csak jogos védelmi helyzetben, jogos önhatalom gyakorlásával, illetve végszükség esetén biztosított, ebben az esetben az eszközöket támadáselhárító eszközöknek nevezhetjük. Esetükben nincs lehetőség tehát a jogszabályok érvényre jutását kényszerrel elérni, csupán a személyek, javak, valamint a közérdek ellen intézett közvetlen támadást háríthatják el, illetve a birtokos jogaival élnek.

A személy- és vagyonőrökkel szemben a rendőr, illetve a fegyveres biztonsági őr esetében kényszerítő eszközökről rendelkeznek a jogszabályok. A kényszer fogalma egyértelműen az erőszak-monopóliumra utal, hiszen ebben az esetben a cél a jogszabályok érvényre juttatása, és az alkotmányos meghatározás szerint ennek érdekében kényszer alkalmazására az állam jogosult. Kényszerítő eszköz mindazon törvények és rendeletek által megengedett, rendelkezésre bocsájtott technikák és technológiák összessége, melyek szükségszerűen, az intézkedés törvényes céljának megvalósulása érdekében az alapvető emberi jogok (így különösen az emberi méltóság, személyes szabadság, testi épség, végső esetben az élethez fűződő jogok) korlátozásával, illetve sérelmével jár. [6] További ismérve tehát a kényszerítő eszközöknek, hogy használatuk által legitim módon korlátozhatók, sérthetők meg bizonyos alapvető emberi jogok. A jogszabályok érvényre juttatása érdekében használható legitim erőszak részletszabályait a kényszerítő eszközök terén törvényi szinten a rendőr esetében a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) 47. – 59. §-a, a fegyveres biztonsági őr esetében a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX. törvény (a továbbiakban: Fbő Tv.) 10. § (2) bekezdése határozza meg. A rendőr kényszerítő eszközei közé tartozik a testi kényszer, a bilincs, a vegyi eszköz, elektromos sokkoló eszköz, rendőrbot, illetve kardlap, a szolgálati kutya, az útzár, a lőfegyver, a csapaterő, illetve a tömegoszlatás. A fegyveres biztonsági őr kényszerítő eszközei közé tartozik a testi kényszer, a bilincs, a vegyi vagy elektromos sokkoló eszköz, a rendőrbot, a szolgálati kutya és a lőfegyver. [7] A rendőrség alapfeladata a közrend és a közbiztonság védelme – ami a használható kényszerítő eszközök számából és fajtájából is látható –, míg a fegyveres biztonsági őrségek szűkebb védelmi spektrumban képesek hatékony védelmet nyújtani. A két szervezet kényszerítőeszköz használati jogosultságainak összehasonlító elemzésével megállapítható, hogy melyik ez a védelmi spektrum, és ezáltal mely területen optimális a fegyveres biztonsági őrség alkalmazása.

A testi kényszer alkalmazásának jogalapját vizsgálva megállapítható, hogy a rendőr, illetve a fegyveres biztonsági őr azt egyaránt cselekvésre vagy cselekvés abbahagyására való kényszerítésre alkalmazhatja. A bilincs alkalmazását vizsgálva eltérés tapasztalható, hiszen a fegyveres biztonsági őr csak a visszatartott személy szökésének, illetve személyőrzési vagy kísérési feladat végrehajtása során a személyes szabadságában korlátozott személy szökésének, önkárosításának megakadályozására használhat bilincset, míg a rendőr ezt megteheti a személyi szabadságában korlátozni kívánt vagy korlátozott személy önkárosításának, támadásának, szökésének megakadályozására, illetve ellenszegülésének megtörésére is. A fegyveres biztonsági őr tehát nem használhat bilincset a támadás megakadályozására, valamint az ellenszegülés megtörésére sem. Ez a szabályzás számos esetben

csökkentheti a fegyveres biztonsági őr védelmi képességét, különösen személyőrzési feladatok végrehajtása során. Szemléletes példaként, személyi szabadságukban korlátozott személyek intézményen belüli verekedése esetén az elsődleges intézkedésekért felelős fegyveres biztonsági őri állomány – mivel önkárosítási vagy szökési szándék az esemény kapcsán nem merül fel – a további támadás megakadályozására, vagy az ellenszegülés megtörésére nem használhatja bilincsét. A fegyveres biztonsági őr vegyi vagy elektromos sokkoló eszközt, rendőrbotot a támadás megakadályozására vagy az ellenszegülés megtörésére használhat. A rendőr vegyi vagy elektromos sokkoló eszközt, illetőleg rendőrbotot vagy kardlapot a fegyveres biztonsági őrrel azonos esetekben alkalmazhat. Van-e eltérés a lőfegyverhasználat kapcsán? Fegyveres biztonsági őrként az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány ellen fegyveresen vagy felfegyverkezve intézett támadás elhárítására lehet lőfegyvert használni. Ugyan az Fbő Tv. külön nem említi, de alapvető állampolgári jogosultságként jogos védelmi helyzetben, valamint végszükség esetén használható lőfegyver esetükben is. Az Rtv. a rendőr lőfegyverhasználati jogosultságaként külön említést tesz a jogos védelem, illetve végszükség eseteiről is, sőt a taxatív felsorolásban is találhatóak olyan elemek, amelyek egyébként is ezekbe a kategóriákba sorolhatók, vagy ezektől élesen nem elválaszthatók. „A rendőr lőfegyvert használhat az élet elleni közvetlen fenyegetés vagy támadás elhárítására; a testi épséget súlyosan veszélyeztető közvetlen támadás elhárítására; a terrorcselekmény, a jármű hatalomba kerítése vagy a közveszély okozása bűncselekmények megakadályozására vagy megszakítására; bűncselekmény lőfegyverrel, robbanóanyaggal vagy az élet kioltására alkalmas más eszközzel való elkövetésének megakadályozására; lőfegyver, illetőleg robbanóanyag jogosulatlan, erőszakos megszerzésére irányuló cselekmény megakadályozására; az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos létesítmény ellen felfegyverkezve intézett támadás elhárítására; az emberi élet kioltását szándékosan elkövető elfogására, szökésének megakadályozására; azzal szemben, aki a nála lévő fegyver vagy élet kioltására alkalmas más eszköz letételére irányuló rendőri felszólításnak nem tesz eleget, és magatartása a fegyver vagy más az élet kioltására alkalmas eszköz ember elleni közvetlen felhasználására utal; az elfogott, bűncselekmény elkövetése miatt őrizetbe vett, vagy bírói döntés alapján fogva tartott személy erőszakos kiszabadításának megakadályozására, az azt megkísérlővel szemben; a saját élete, testi épsége, személyi szabadsága ellen intézett támadás elhárítására”. [7] [8] Megállapítjuk, hogy a rendőr lőfegyverhasználati jogosultsága széleskörű a közrend és közbiztonság fenntartását illetően. Ezzel szemben a fegyveres biztonsági őrök lőfegyverhasználati jogosultsága az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány védelmére korlátozódik, azonban ezek védelmét azonos elméleti védelmi szinten biztosítja a jogszabály.

INTÉZKEDÉSEK A VÉDELEM ÉRDEKÉBEN

A személy- és vagyonőr intézkedési jogosultságait az Szvmt. 25-30. §-a határozza meg. „A személy- és vagyonőr a megbízó közterületnek nem minősülő létesítményének őrzése során például jogosult a területre belépő vagy az ott tartózkodó személyt kiléte igazolására, a belépés, illetőleg a tartózkodás céljának közlésére, jogosultságának igazolására felhívni, ennek megtagadása vagy a közölt adatok nyilvánvaló valótlansága esetén az érintett belépését, ott-tartózkodását megtiltani, és távozásra felszólítani”. [5] Továbbá jogosult

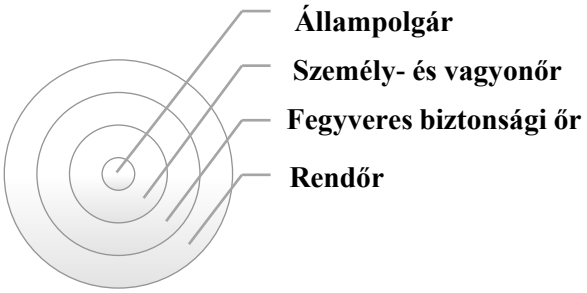
„a területre belépő vagy onnan kilépő személyt csomag, illetve menet-, szállítási okmány bemutatására felhívni; a területen tartózkodó vagy onnan kilépő személyt csomagja tartalmának, járművének, valamint a szállítmánynak bemutatására felhívni, valamint a jogsértő személyt magatartása abbahagyására felhívni". [5] A rendezvénybiztosítási feladatokat ellátó személy a meghatározottakon túl többek között jogosult „zárt területen vagy helyen tartott rendezvényre belépő személyt csomagja tartalmának bemutatására felszólítani, ennek visszautasítása esetén a rendezvényen való részvételét megtiltani; a rendezvény megtartását akadályozó vagy zavaró, annak biztonságát veszélyeztető, illetve az ott jogellenesen tartózkodó személyt kilétének igazolására felszólítani, a rendezvényen való részvételét megtiltani, távozásra felszólítani, amennyiben az érintett személy ennek nem tesz eleget, és az élet- és vagyonbiztonság érdekében szükséges, a rendezvényről kivezetni; a sportrendezvényről eltávolítandó személyt visszatartani, ha az személyazonosságát felhívásra nem igazolja". [5] „A pénz- és értékőrzési, értékszállítási, szállítmánykísérési, valamint szállítási feladatokat ellátó személy jogosult a szállítást jogtalanul akadályozó, illetve az őrzött vagy szállított érték biztonságát veszélyeztető személyt kilétének igazolására, a tevékenységét akadályozó, veszélyeztető magatartásának abbahagyására felhívni". [5] Az Szvmt. 25. § kimondja, hogy a személy- és vagyonőr jogosultságait a törvényben meghatározottak szerint vagy az érintett személy önkéntes hozzájárulása alapján gyakorolja. Megállapítható, hogy a felhívni, felszólítani kifejezések az önkéntes beleegyezésre utalnak, melynek megtagadása esetén a jogszabály nem biztosít eszközt az intézkedés kikényszerítésére. Az Szvmt 27. § alapján ha a személy- és vagyonőr által személyazonosításra felkért személy önként és hitelt érdemlően nem igazolja kilétét, a személyazonosság megállapítására – indokolt esetben – igazoltatásra jogosult hatósági személyt kérhet fel, ami szintén nem tér el az állampolgári jogosultságoktól. Ugyan a megbízó közterületnek nem minősülő létesítményének őrzése során az említett esetben a személy- és vagyonőr adott személy ott-tartózkodását megtilthatja – ami az érintett személy személyi szabadságát korlátozza – de a szabályozás ezen része a jogos önhatalomból fakad. Az Szvmt. 27. § (2) bekezdése alapján „a személy- és vagyonőr jogosult a bűncselekmény és a szabálysértés elkövetésén tetten ért személyt a cselekmény abbahagyására felszólítani, a cselekmény folytatását megakadályozni, az elkövetőt elfogni és a birtokában lévő, bűncselekményből vagy szabálysértésből származó vagy annak elkövetéséhez használt dolgot, illetve támadásra alkalmas eszközt elvenni. Köteles azonban az elfogott személyt haladéktalanul az ügyben eljárni jogosult nyomozó hatóságnak átadni, ha erre nincs módja, e szervet nyomban értesíteni. Így kell eljárni a tetten ért személytől elvett dolgokat illetően is." [5] Az Szvmt. 27. §-a szintén személyi szabadságot korlátozó intézkedésre utal, azonban a büntetőeljárásról szóló 2017. évi XC. törvény 273. §-a alapján a bűncselekmény elkövetésén tetten ért személyt bárki elfoghatja, köteles azonban őt a nyomozó hatóságnak haladéktalanul átadni, vagy ha erre nincs módja, a rendőrséget tájékoztatni. Hasonló jogosultságot állapít meg a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény 73. § (8) bekezdése, ami alapján a tulajdon elleni szabálysértés elkövetésén tetten ért személyt bárki visszatarthatja, köteles azonban őt a rendőrségnek haladéktalanul átadni. [5] [9] [10] Megállapítható tehát, hogy a bűncselekmény elkövetésén tetten ért személy elfogása, valamint a tulajdon elleni szabálysértésen tetten ért személy visszatartása állampolgári jogosultság. Mindezekkel szemben érdekes jogszabályváltozást hozott az új típusú korona-

vírus 2020-as első hulláma, aminek következtében 2020. június 18-tól egészségügyi válsághelyzetben az egészségügyi készlet megóvása érdekében eljáró vagyonőr az emberi méltóság tiszteletben tartásával jogosult az érintett beleegyezése nélkül ruházat, csomag, jármű átvizsgálására. [5] Megállapítható, hogy ebben az esetben nem beszélhetünk az intézkedés alá vont személy önkéntes beleegyezéséről. A törvénymódosítás világossá teszi, hogy bizonyos válsághelyzetekben az állam szélesebb körben biztosíthatja az erőszak-monopóliumának megosztását, ezzel segítve a hatékony védekezést.

Az Rtv. 29-46. §-ban meghatározott rendőri intézkedések elemzéséből megállapítható, hogy a közrend és közbiztonság védelme érdekében az állam a lehető legszélesebb erőszak-monopóliumból fakadó eszköztárat biztosítja a rendőr számára. A rendőri intézkedések közé tartozik többek között az igazoltatás, a dolog helyszíni elvétele, a fokozott ellenőrzés, ruházat, csomag és jármű átvizsgálása, az elfogás, az előállítás és az elővezetés, a helyszín biztosítása, valamint a közlekedésrendészeti intézkedés is. [7] Ezzel szemben a fegyveres biztonsági őrökre vonatkozó intézkedési jogosultság meglehetősen szűkített eszköztárat biztosít, azonban bizonyos területeken az elméleti védelmi szint megegyezik a rendőrével. „A fegyveres biztonsági őr az őrzött objektumba történő be- és kiléptetésre irányuló szolgálatának teljesítése során jogosult az őrzött objektumba a belépő személyt kiléte igazolására, a belépés céljának közlésére, jogosultságának igazolására felhívni; az őrzött objektumba a belépő vagy onnan kilépő személyt csomagja tartalmának, járművének, valamint a szállítmányának bemutatására felhívni; a belépő személy családi és utónevét, születési helyét és idejét, a személyazonosításhoz bemutatott okmány számát, ha azt nem magyar hatóság állította ki, az okmányt kiállító ország megnevezését is, illetve a belépésre használt jármű rendszámát és típusát rögzíteni". [8] Megállapítható, hogy a felhívni, felszólítani kifejezések – hasonlóan az Szvmt. által meghatározottakhoz – az önkéntes beleegyezésre utalnak, azonban a jogszabály a fegyveres biztonsági őrök részére biztosít bizonyos erőszak-monopóliumból fakadó eszközöket az intézkedések kikényszerítésére. „A felhívásban foglaltak teljesítésének megtagadása vagy a közölt adatok valótlanságának vélelmezése esetén a fegyveres biztonsági őr jogosult a személy beléptetését megtagadni; valamint az objektumba belépő, illetve az objektumból kilépő személyt a csomagja tartalmának, járművének, valamint a szállítmányának bemutatásáig feltartóztathatja". [8] „A fegyveres biztonsági őr szolgálatának jogszerű teljesítése során továbbá jogosult és köteles a biztonságot sértő vagy veszélyeztető személyt tevékenysége abbahagyására felszólítani és igazoltatni; az intézkedésének tettlegesen ellenszegülő, valamint bűncselekmény vagy tulajdon elleni szabálysértés elkövetésén tetten ért személyt a rendőrség megérkezéséig visszatartani; az igazoltatott, visszatartott vagy előállított személytől a bűncselekményből származó vagy annak elkövetéséhez használt dolgot, illetve támadásra alkalmas eszközt elvenni, ennek érdekében ruházatát, csomagját átvizsgálni". [8]

ÖSSZEGZÉS

Elméleti védelmi képesség alatt tehát a jogszabályok által biztosított védelmi lehetőségeket, kötelezettségeket értjük. A védelmi képességeket forrásuk alapján szétválaszthatjuk az állampolgárok számára biztosított jogokra, valamint az állam erőszak-monopóliumából fakadó jogokra.



1. ábra: Az elméleti védelmi képesség hierarchikus szintjei, saját szerkesztés

Az egyén védelmi alapjogai közé sorolható a jogos védelem, a végszükség, valamint a birtokos birtokvédelmi jogosultsága, a jogos önhatalom. A személy- és vagyonőrök intézkedési és eszközhasználati jogosultságai – az Szvmt. egészségügyi válsághelyzetről rendelkező szakaszának kivételével – részben a személyükhöz fűződő alapjogokból, részben a megbízó által átruházott alapjogokból fakadnak. Az egyénnek tehát joga van a személyének, tulajdonának, birtokának védelmére, ezt a jogot pedig polgárjogi szerződés keretében személy- és vagyonvédelmi vállalkozásokra is ruházhatja.

A rendőr, illetve a fegyveres biztonsági őr intézkedési és eszközhasználati jogosultságainak célja a jogszabályok érvényre juttatása, ami az alapvető emberi jogok – bizonyos kényszer-intézkedés vagy kényszerítő eszköz használat általi – korlátozásával, illetve sérelmével járhat. Részükre az állam a védelmi feladatainak ellátásához jogszabályok útján biztosítja az erőszak-monopóliumából fakadó legitim erőszakot. A rendőrök intézkedési és eszközhasználati jogosultságainak elemzése alapján megállapítható, hogy a lehető legszélesebb körű védelmi képességekkel kerültek felhatalmazásra a közrend és közbiztonság fenntartása érdekében, míg a fegyveres biztonsági őrök szűkebb védelmi spektrumban képesek hatékony védelmet nyújtani. A fegyveres biztonsági őrök intézkedési jogosultsága és kötelezettsége csak a határozattal őrzésre rendelt tevékenység, létesítmény, szállítmány őrzésére terjed ki. Általánosságban azonban elmondható, hogy az állam működése vagy a lakosság ellátása szempontjából kiemelten fontos tevékenység, létesítmény, szállítmány védelme során – a bilincshasználati jogosultságok szűkebb körét leszámítva – a rendőrrel azonos elméleti védelmi képességgel rendelkeznek.

Az elméleti síkon levezetett védelmi képesség szintje azonban csak számos gyakorlati tényező együttes fennállása esetén valósul meg. A gyakorlati védelmi képességet meghatározza a személyi állomány képzettsége, fegyelme, leghangsúlyosabb eleme pedig a biztonságtechnika, hiszen az intézkedés minden fázisában – az észlelés, a késleltetés és a válaszintézkedés során – kiemelt szerepet játszik. A fegyveres biztonsági őrséggel őrzésre rendelt tevékenység, létesítmény vagy szállítmány védelme tekintetében a gyakorlati védelmi képesség – szemben a Rendőrség által végrehajtott azonos őrzéssel – az elméleti védelmi képesség korlátain belül a végletekig növelhető. A fegyveres biztonsági őrzés esetén nagyobb mozgásteret biztosít, hogy az őrzés költségvonzatait az őrzésre kötelezett szervezet viseli, így a gyakorlati védelmi képességet megalapozó humán-erőforrás, illetve eszközbéli tényezők nagyobb mértékben befolyásolhatók.

A gyakorlatban az eltérő jogszabályi háttér miatt a fegyveres biztonsági őrzésre kötelezett szervezetek a személy- és vagyonvédelmi tevékenységet személy- és vagyonőrök által végzik, a fegyveres biztonsági őrzésre rendelt tevékenység, létesítmény vagy szállítmány védelmét pedig fegyveres őrök által hajtják végre. Az egyes tevékenységek gyakorlati összehangolásával az őrzésvédelmi tevékenység hatékonysága fokozható. [11]

FELHASZNÁLT FORRÁSOK

[1] Magyarország Alaptörvénye
[2] A Büntető Törvénykönyvről szóló 2012. évi C. törvény
[3] A Polgári Törvénykönyvről szóló 2013. évi V. törvény
[4] A közbiztonságra különösen veszélyes eszközökről szóló 175/2003. (X. 28.) Korm. rendelet
[5] A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény
[6] Hautzinger Zoltán: A rendészeti kényszerítő eszközök alkalmazásának alapelvei, Pécsi Határőr Tudományos Közlemények I., 69. oldal (Pécs, 2002)
[7] A Rendőrségről szóló 1994. évi XXXIV. törvény
[8] A fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX. törvény
[9] A büntetőeljárásról szóló 2017. évi XC. törvény
[10] A szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről szóló 2012. évi II. törvény
[11] Szabó Anikó, Papp József, Kovács Tibor, Szűcs Endre, Berek Tamás: A személy- és vagyonőrök és a fegyveres biztonsági őrök tevékenységének összehasonlítása a MÁV Zrt.-n keresztül, Műszaki Katonai Közlöny, XXVIII. évfolyam, 2018. 4. szám, 164-173. oldal

USING ARTIFICIAL INTELLIGENCE FOR OBJECT DETECTION (SECOND PART)

A MESTERSÉGES INTELLIGENCIA FELHASZNÁLÁSI LEHETŐSÉGEI AZ OBJEKTUMFELISMERÉSBEN (MÁSODIK RÉSZ)

KOLLÁR Csaba[1] – NAGY Barna[2]

Abstract

In the first part of our study, we dealt with machine vision, the history of technical and information science of machine vision, neural networks, and the teaching of networks. The main topics of the second part of our paper are the support of machine vision with neural networks, the framework of neural networks, the presentation of the platform for practical development, the detection of objects in moving images, and finally the thoughts that conclude our two-part study. There are a relatively large number of hardware and software solutions to choose from for using artificial intelligence in object recognition. The strength of the solution we have chosen is that it provides a relatively inexpensive solution that can inspire not only practitioners but also students to try out the development and test environment presented and to think further about the possibilities.

Keywords

security systems, artificial intelligence, computer vision, Intel Neural Compute Stick, Raspberry Pi

Absztrakt

Tanulmányunk első részében a gépi látással, a gépi látás technika- és információtudományi történetével, a neurális hálózatokkal, a hálózatok tanításával foglalkoztunk. Írásunk második részének fontosabb témái a gépi látás támogatása neurális hálózatokkal, a neurális hálózatok keretrendszere, a gyakorlati fejlesztést biztosító platform bemutatása, az objektumok detektálása mozgóképen, s végül a kétrészes tanulmányunkat záró gondolatok. A mesterséges intelligencia objektumfelismerésben történő használatára viszonylag sok hardveres és szoftveres megoldás közül lehet választani. Az általunk választott megoldás erősségét az adja, hogy használatával egy relatíve olcsónak tekinthető megoldás áll rendelkezésre, amelyik nem csak a gyakorló szakembereket, hanem a hallgatókat is inspirálhatja a bemutatott fejlesztési- illetve tesztkörnyezet kipróbálására és a benne levő lehetőségek továbbgondolására.

Kulcsszavak

biztonságtechnika, mesterséges intelligencia, gépi látás, Intel Neural Compute Stick, Raspberry Pi

[1] kollar.csaba@uni-obuda.hu | ORCID: 0000-0002-0981-2385 | senior research fellow, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | tudományos főmunkatárs, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] nagy.barna@blx.hu | ORCID: 0000-0002-8101-1080 | software architect, Blumenthal Consulting Kft. | szoftver architect, Blumenthal Consulting Kft.

A GÉPI LÁTÁS TÁMOGATÁSA NEURÁLIS HÁLÓZATOKKAL

Az utóbbi években a Computer Vision alkalmazásokban uralkodó lett a konvolúciós neurális hálózatok (Convolutional Neural Networks (CNN)) használata. A CNN egy deep neural network (DNN), azaz mély neurális hálózat. A hálózatokat többnyire felügyelt tanítással teszik alkalmassá egy-egy konkrét feladat elvégzésére.

A neurális hálózatok tanítása meglehetősen erőforrásigényes feladat. Általában nagy mennyiségű képre (tanító pontokra) és komoly számítási kapacitásra van szükség az elvégzéséhez. Ugyanakkor a hálózat használata, az előhívás (inference) sokkal kevesebb erőforrást igényel. Már edge eszközökben is futtatható és a hálózat válasza (alkalmazástól függően) akár milliszekundum alatt előáll. Mind a tanításra, mind az előhívásra (inference) igénybe szoktak venni hardveres gyorsítókat (accelerator), melyek a CNN számításait segítik. [1]

A hálózatok tanítása sohasem egy lépésben, hanem iteratívan, lépésenként történik, amely több fogalmat is bevezetett. Egy epoch a teljes tanítóminta-készlet (training dataset) egy alkalommal történő „végigtanítását" jelenti. Egy tanítóminta (bemenet és kimenet páros) tanítása ebben az esetben egy előreterjesztés (forward propagation) és egy hiba-visszaterjesztés (backward propagation of errors) folyamatot jelent.

Az előreterjesztés során a hálózat bemenetére illesztett bemeneti érték alapján számoljuk a hálózat aktuális válaszát. A visszaterjesztés során pedig a számított aktuális válasz és a tanítómintában lévő elvárt válasz közötti eltérés alapján kismértékben módosítjuk a többrétegű hálózat kapcsolati súlyait.

A neurális hálózatok néhány keretrendszere

A neurális hálózatok elterjedése magával hozta az azokat támogató, modellező rendszerek nagy számát is. Részben üzleti, részben más megfontolásból, de sokan fogtak ilyen rendszerek fejlesztésébe. A későbbi vizsgálatokhoz célszerű kiválasztani egyet, mely illeszkedik az elvárásainkhoz és a lehetőségeinkhez. Összegyűjtöttünk néhány ismert rendszert és kiértékeltük őket több szempont alapján. Az általunk vizsgált keretrendszerek a következők voltak:

Google Tensorflow. A Google fejlesztőcsapata által készített nyílt forráskódú TensorFlow az egyik legnépszerűbb machine learning platform. Az eszköz a modellezést, a tanítást és az éles környezetben történő futtatást is támogatja. A TensorFlow nemcsak neurális hálózatok, azon belül is deep neural network modellezésére használható. Egy általános eszköz, mellyel számos machine learning feladat megoldható, ráadásul csekély változtatással sokféle eszközön is futtatható. [2]

Apache MXNet. Az Apache alapítvány egyik projektje, melyben egy skálázható mélytanuló rendszert fejleszthettek. Előnye, hogy nagyon sok nyelven elérhető hozzá interfész, továbbá nagyon könnyen futtatható egyszerre több eszközön is. [3]

ONNX. Az Open Neural Network Exchange (ONNX) egy nyílt formátum, melyet eredetileg a Facebook és a Microsoft készített, hogy a már meglévő gépi tanulást segítő keretrendszerek közötti átjárást segítsék. A formátum eszközei támogatják a legtöbb keretrendszert, például Caffe, Keras, MXNet, PyTorch, TensorFlow és továbbiakat. [4]

Keras. A Keras egy Python nyelven írt, nyílt forrású, neurális hálózat könyvtár (library), amely más keretrendszerekhez (pl. TensorFlow) biztosít magasszintű hozzáférést. A TensorFlow a saját high-level API-jának választotta, de más rendszerekkel is integrálható. [5]

Caffe. A Caffe (Convolutional Architecture for Fast Feature Embedding)) keretrendszert eredetileg Yangqing Jia a Berkeley egyetem PhD hallgatója készítette konvolúciós neurális hálózatok modellezésére és futtatására. Előnyei közzé tartozik, hogy nagyon könnyű vele modelleket készíteni, ami gyakorlatilag egy szöveges állomány. Meglehetősen elterjedt akadémiai és egyéb kutató projektekben, ezért rengeteg modell érhető el a formátumában, illetve nagyon sok más modellt implementáltak újra a Caffe rendszerében. [6]

Darknet. A Darknet egy nyílt forráskódú neurális hálózati keretrendszer, amelyet C-ben és CUDA-ban írtak. Gyors, könnyen telepíthető, és támogatja a CPU és a GPU számítását. Legfontosabb tulajdonsága, hogy osztályozza a képeket olyan népszerű modellekkel, mint a ResNet és a ResNeXt. [7]

A felsorolt rendszerek közül kiemelkedik a TensorFlow, mely sokoldalúsága és dokumentáltsága a többi rendszer elé helyezi. Ugyanakkor komplexitása nagy, a betanulási, megismerési idő sokáig tart. Mindezek mellett – ahogy írtuk – a Caffe is nagy mértékben elterjedt a tudományos és startup körökben. Nem olyan univerzális, mint a TensorFlow, viszont pont arra alkalmas, amire mi szeretnénk használni (konvolúciós neurális hálózatok). Használata egyszerű, számos cikk, publikáció foglalkozik vele. A számunkra fontos OpenCV és OpenVINO támogatással is rendelkezik, így ezt a keretrendszert választottuk, annak ellenére, hogy jelenleg nem fejlesztik. A vizsgálatokban használt hálózatokat Caffe formátumban kerestük, amiket közvetlenül és (szükség esetén) konvertálva használtunk. Az első táblázatban a fontosabb keretrendszerek összehasonlító elemzését ismertetjük.

Elnevezés	**TensorFlow**	**MXNet**	**ONNX**	**Keras**	**Caffe**	**Darknet**
Aktuális verzió	2.4.1	1.8.0	1.9.0	2.4.0	1.0 (2.0)	
Utolsó verzió	2021.01.21.	2021.03.03.	2021.04.19.	2020.06.17.	2017.04.18.	kb. 2 éve
Fejlesztő	Google BrainTeam	Apache Foundation	Facebook, Microsoft	François Chollet	Berkeley Vision and Learning Center	Joseph Redmon
Megjelenés	2015.11.09.	2017.09.05.	2017 szept.	2015.03.27.	2017.04.18.	2016
API nyelve	Python, C/C++ (C++, Go, Java, Javascript, Swift, stb.)	Python, C++, Java, Scala, R, Perl	Python, C++	Python	Python, C++	C++

Elnevezés	TensorFlow	MXNet	ONNX	Keras	Caffe	Darknet
Operációs rendszerek	Linux, macOS, Windows, Raspbian[3]	Linux, macOS, Windows, Raspbian	Linux, Windows	Linux, macOS, Windows	Linux, macOS, Windows	Linux, macOS, Windows
Futtató eszközök	CPU, Nvidia CUDA based, GPU, TPU[4]	CPU, GPU, Nvidia Jetson		CPU, GPU, TPU	CPU, GPU	GPU, (CPU)
OpenCV támogatás	igen[5]	nincs	igen	nincs	igen	igen
OpenVINO támogatás	igen, az OpenVINO közvetlenül konvertál TensorFlow modelleket	igen, az OpenVINO közvetlenül konvertál MXNet modelleket	igen, az OpenVINO közvetlenül konvertál ONNX modelleket	nincs közvetlen konverzió	igen, van közvetlen konverzió	nincs közvetlen konverzió
Nyílt forráskód	Apache License 2.0	Apache License 2.0	MIT License	igen	BSD License	igen
Elérhető modellek	nagyon sok	sok	közepes	sok	nagyon sok	pár darab

1. Táblázat: A főbb neural networks keretrendszerek paraméterei (saját összehasonlító elemzés és szerkesztés)

AZ INTEL NEURAL COMPUTE STICK 2 VIZSGÁLATA

Funkcionális tesztelések, az OpenVINO toolkit vizsgálata

Az alábbi alkalmazások, illetve modellek futtatásával azt vizsgáltuk, hogy az OpenVINO Toolkit fejlesztőeszköz egyes eszközei megfelelően működnek-e a környezetemben.

A hello_query_device alkalmazás. Az alkalmazás kilistázza az OpenVINO által elérhető eszközöket. Ezeken a hardvereken tudunk az Inference Engine segítségével modelleket futtatni.

Az alkalmazás futtatása:

```
python3 hello_query_device.py
```

Az alkalmazás segítségével több környezetben is lekérdeztük az elérhető eszközöket:

Environment / Computer (környezet/számítógép)	Available device (lehetséges eszköz)	Full device name (az eszköz teljes neve)
Mac mini (Mid-2011)	CPU	Intel(R) Core(TM) i5-2415M CPU @ 2.30GHz
Mac mini (Mid-2011)	MYRIAD	Intel Movidius Myriad X VPU
Raspberry Pi 3B	MYRIAD	Intel Movidius Myriad X VPU
Macbook Pro (Mid-2014)	CPU	Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz

[3] A Raspberry Pi-re fordított Debian alapú Linux operációs rendszer

[4] TPU – Tensor Processing Unit: a Google által fejlesztett alkalmazásspecifikus IC, amit elsősorban számítóközpontokba szánt, de létezik belőle *edge* változat is (https://cloud.google.com/edge-tpu/).

[5] az OpenCV be tudja tölteni a modellt a *cv2.dnn.readNetFromTensorflow()* függvényhívással

Macbook Pro (Mid-2014)	MYRIAD	Intel Movidius Myriad X VPU

2. Táblázat: A hello_query_device alkalmazás segítségével történő lekérdezés (saját szerkesztés)

OpenVINO Model Downloader. A Model Downloader parancssori eszközzel számos open source, előre tanított (pre trained) hálózat modelljét lehet letölteni. Ezek a modellek valamelyik népszerű modellező eszköz (pl. Caffe, TensorFlow) formátumában vannak, ezért konvertálni kell azokat az Intermediate Representation (IR) formátumra. Ez az a formátum, amit az OpenVINO csomagban található Inference Engine (IE) fel tud olvasni, illetve futtatni tud a támogatott eszközön.

Az eszköz az alábbi útvonalon érhető el:

```
$INTEL_OPENVINO_DIR/deployment_tools/open_model_zoo/tools/downloader/downloader.py
```

Az AlexNET modell letöltése (half-precision FP16 / Caffe Model):

```
./downloader.py --name alexnet --output_dir . --precisions FP16

################|| Downloading models ||################

========== Downloading my_dir/public/alexnet/alexnet.prototxt
... 100%, 3 KB, 12302 KB/s, 0 seconds passed

========== Downloading my_dir/public/alexnet/alexnet.caffemodel
... 100%, 238146 KB, 2930 KB/s, 81 seconds passed
```

Az AlexNet modell tesztelése

Az AlexNet egy régi és ismert neurális hálózat. Már több, sokkal jobban teljesítő társa is elérhető, de a népszerűsége és a fórumokban fellelhető gazdag dokumentáltsága ideálissá teszi arra, hogy ennek segítségével vizsgáljuk az Intel Neural Compute Stick performanciáját. Az AlexNet az a konvolúciós neurális hálózat (CNN), mely 2012-ben megnyerte az ImageNet (ImageNet Large Scale Visual Recognition Challenge – ILSVRC) versenysorozatot. A modellt az OpenVINO Model Zoo-jából töltöttük le Caffe formátumban, ezért konvertálnunk kellett IR-re (Intermediate Representation):

```
python3 mo_caffe.py \
--input_model ./alexnet/alexnet.caffemodel --output_dir . \
--data_type=FP16 \
--model_name=alexnet_fp16

./mo.py \
--input_model ../tools/model_downloader/public/alexnet/alexnet.caffemodel \
--input_proto ../tools/model_downloader/public/alexnet/alexnet.prototxt \
--model_name=alexnet_fp32
```

A modell image classification-re használható, ezért egy alkalmas kép segítségével teszteltük a funkcionális működését:

1. Ábra: Dalmata fajtájú kutya (forrás: Hungarovet Állatkorház honlapja[6])

A hálózat egy 1000 elemű vektort ad vissza, az egyes címkék[7] valószínűségével. A tesztelés során egy Intel CPU-n és a Movidius VPU-n is futtattuk a hálózatot:

index	**valószínűség**	**címke**	**index**	**valószínűség**	**címke**
251	0,9404	dalmatian, coach dog, carriage dog	251	0,9390	dalmatian, coach dog, carriage dog
246	0,0498	Great Dane	246	0,0509	Great Dane
176	0,0053	Saluki, gazelle hound	176	0,0052	Saluki, gazelle hound
MYRIAD (Movidius VPU)			CPU (Mac mini 2011)		

3. Táblázat: Az AlexNet funkcionális tesztelése két eszközön (saját szerkesztés)

Mindkét eszközön nagyságrendileg azonos „magabiztossággal" találta el a hálózat, hogy mi található a képen. A kép eredeti mérete 512 * 302 pixel, amit a teszt szkript a hálózat bemenetére vág: 227 * 227 képpontra. A hálózat adott eszközön, minden futtatásakor ugyanazokat az valószínűségeket adta vissza.

Az AlexNet performancia vizsgálata. Az OpenVINO saját eszközt ad a teljesítmény vizsgálatokhoz. Ez a benchmark_app, melyet Python és C++ nyelven elérhet a fejlesztő. Ez utóbbit, használat előtt szükséges lefordítani az adott környezetre, mert a C++ mintaprogramoknak csak a forráskódja található meg a csomagban.

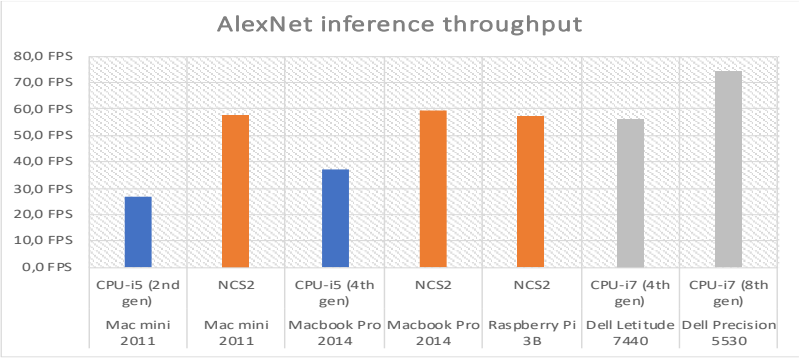
A teljesítménymérő alkalmazás futtatásához több paramétert is meg kell adni:

- *model:* a teszteléshez használt IR formátumú modell
- *images:* a teszteléshez használt kép vagy képek sorozata
- *api:* szinkron vagy aszinkron hívással érje el az Inference Engine-t
- *device:* az eszköz, amin futtatni kell a mérést

```
python3 ../tools/benchmark_tool/benchmark_app.py \
-m alexnet.xml \
-i ~/Downloads/alexnet/dog_03.jpg \
-d CPU -api async
```

[6] Webes elérhetőség: http://vetnetinfo.com/tudasbazis/2016/03/09/dalmata-dalmatian-kutya/
[7] Az ImageNet1000 classification indexei: https://gist.github.com/yrevar/942d3a0ac09ec9e5eb3a

A teljesítményt ötféle környezetben vizsgáltuk. Négy esetben személyi számítógépen (CPU és Neural Compute Stick 2) és az ötödik esetben pedig a Raspberry Pi kártyaszámítógépen. A benchmark_app 60 másodpercig futott aszinkron módban és ezalatt az idő alatt igyekezett minél többször feldolgozni ugyanazt a képet. A futtatások száma alapján volt kalkulálható az egységnyi időre jutó képfeldolgozások száma: FPS (frame per sec).



2. Ábra: Az egyes konfigurációk képfeldolgozási teljesítménye az AlexNet hálózaton mérve (saját szerkesztés)

A méréseket többször elvégeztük. Az eszközök teljesítménye (throughput in FPS) a számítógépek aktuális állapotától és egyéb tevékenységétől függően ingadozott. Az összesítésben egy átlagos értéket vettünk figyelembe.

A Neural Compute Stick 2 közel azonos teljesítményt nyújtott (narancs színű oszlopok) mindhárom számítógépben, és egyben számottevően jobb volt, mint a régebbi Intel CPU-k (kék oszlopok). A mért eredményekhez hozzátettünk két (az interneten publikált[8]) teszteredményt is. Ezek csak korlátozottan hasonlíthatóak össze a mi eredményeinkkel, mert nem ugyanabban, de nagyon hasonló tesztkörnyezetben készültek. Jól mutatják, hogy az újabb, erősebb Intel CPU-k nagyobb teljesítményre képesek, mint az NCS2.

A YOLOv3 modell tesztelése

A YOLO neurális hálózat. A YOLO (You Only Look Once) egy objektum detektáló neurális hálózat, illetve módszer, melyet Joseph Redmon publikált[9] negyedmagával együtt 2016-ban. A módszer újszerűsége (és a nevét is innen kapta), hogy az objektum detektálás összes lépését (localization + classification) a hálózat egy kiértékelése alatt teszi meg. A hálózat gyors elterjedése a kiemelkedő sebességének köszönhető. [8] Az Intel NCS2 további vizsgálatához előzetesen jó ötletnek gondoltuk, hogy egy népszerű és valós idejű objektum detektálást ígérő hálózattal teszteljük az eszközt.

[8] Jonas Werner (Cloud Solutions Architect) blogja: https://jonamiki.com/2019/02/27/trying-out-the-intel-neural-compute-stick-2-movidius-ncs2/
[9] Joseph Redmon YOLO weboldala: https://pjreddie.com/darknet/yolo/

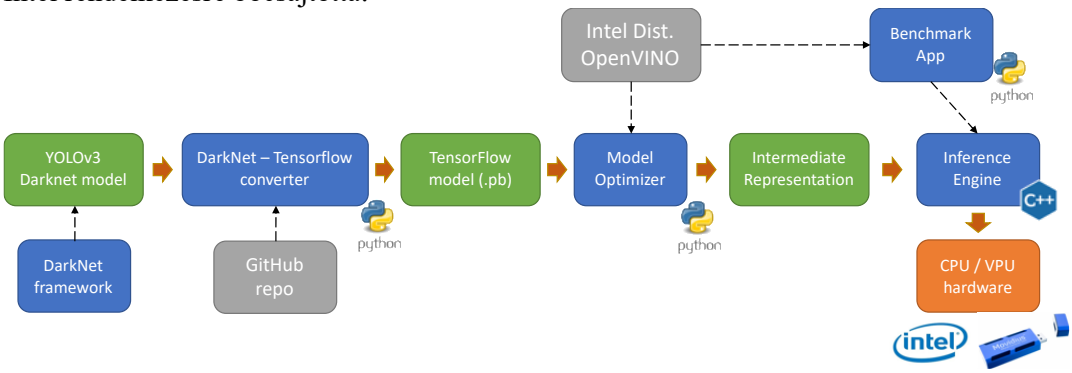
A YOLOv3 modell konvertálása IR formátumra. A YOLO v3-as verziója is a Darknet neurális hálózat modellező eszközben készült. Ez közvetlenül nem futtatható az OpenVINO Inference Engine-jén, ezért két lépésben konvertálni kellett az IR (Intermediate Representation) formátumra. A konverzióhoz a modell készítőjének weboldaláról[10] letöltöttük a betanított modellt (.weights fájl), valamint egy „külső[11]" eszközt, mellyel a Google TensorFlow modellezőjének a formátumára konvertáltuk. A TensorFlow model a gyakorlatban egy .pb (Protocol Buffer) kiterjesztésű fájlt jelentett.

```
# konvertáló eszköz letöltése
git clone https://github.com/mystic123/tensorflow-yolo-v3.git

# címkék letöltése
wget https://raw.githubusercontent.com/pjreddie/darknet/master/data/coco.names
# súlyok letöltése
wget https://pjreddie.com/media/files/yolov3.weights

# konvertálás TensorFlow modellre
python3 convert_weights_pb.py --class_names coco.names --data_format NHWC \
--weights_file yolov3.weights
```

Ez a modellek közötti konverzió rámutatott a különböző modellező keretrendszerek közötti átjárhatóság korlátoltságára. Például a Region réteg (layer) létezik a Darknet eszköztárában, de jellemzően nincs benne más keretrendszerekben, pl a TensorFlow-ban sem, így azokat egyedi implementációval szükséges pótolni. Ezt az egyedi implementációt az Intel rendelkezésre bocsájtotta.



3. Ábra: A Darknet YOLO modelljének konverziója és futtatása (saját szerkesztés)

A TensorFlow-IR konverzióra már az OpenVINO saját eszközét használtuk, a Model Optimizer-t.

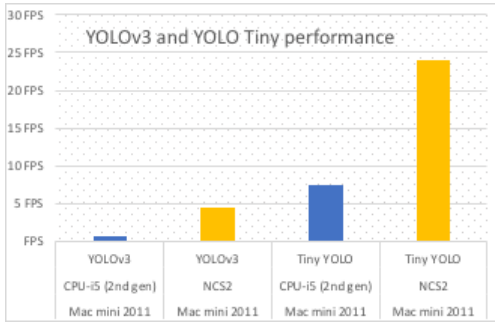
```
# konvertálás IR modellre (Model Optimizer)
python3 mo_tf.py \
--input_model ~/tensorflow-yolo-v3/frozen_darknet_yolov3_model.pb \
--tensorflow_use_custom_operations_config ~/tensorflow-yolo-v3/yolo_v3.json \
--batch 1
```

[10] A YOLO hálózat weboldala: https://pjreddie.com/darknet/yolo/
[11] Paweł Kapica (mystic123): GitHub oldal: https://github.com/mystic123

A YOLOv3 modell performancia vizsgálata. A YOLO modell performancia vizsgálatát az OpenVINO benchmark_app eszközével végeztük el, hasonlóan paraméterezve, mint ahogy az AlexNet esetében tettük.

```
python3 benchmark_app.py \
-m ~/Downloads/yolov3/frozen_darknet_yolov3_model.xml \
-i ~/Downloads/alexnet/dog_03.jpg \
-d CPU
```

A hálózat vizsgálat közben 60 másodperc alatt minél többször próbálta feldolgozni ugyanazt a képet. A vizsgálatot 2 környezetben végeztük el, egy személyi számítógép CPU-ját és az Intel NCS2-t tesztelve. Bár a hálózat a sebessége miatt lett igazán népszerű, a teszteredmények ezt nem igazolták. Az eredeti YOLO v3-as hálózat (a vizsgált környezetekben) nem alkalmas valós idejű feldolgozásra. A YOLO hálózatokhoz készített a fejlesztő egy-egy egyszerűsített változatot is. Ezek közül a YOLOv3 Tiny-at próbáltuk ki. Ez már sokkal jobb teljesítménnyel futott, ugyanakkor a hálózat „Tiny" verziója sokkal pontatlanabb, mint az eredeti változat.



4. Ábra: A YOLOv3 teljesítménye (OpenVINO benchmark_app) CPU-n és az Intel NCS2-n (saját szerkesztés)

Környezet	Modell	Iterációk száma	Performancia (FPS)
Mac mini 2011 CPU-i5 (2nd gen)	YOLOv3	44	0,62
Mac mini 2011 NCS2	YOLOv3	276	4,46
Mac mini 2011 CPU-i5 (2nd gen)	YOLOv3 Tiny	456	7,38
Mac mini 2011 NCS2	YOLOv3 Tiny	1452	24,07

4. Táblázat: Az egyes környezetekben mért teljesítmények (saját szerkesztés)

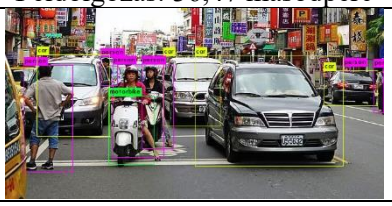
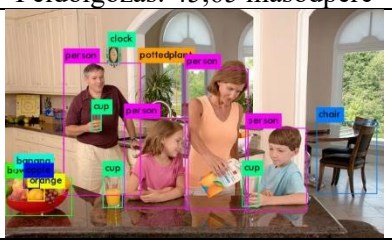
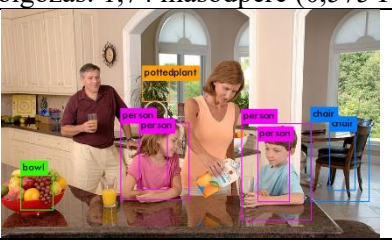
A mérési eredmények (ugyanabban a környezetben) minden alkalommal eltérőek voltak, ezért egy átlagos értéket tűntettük fel a táblázatban.

A YOLOv3 vizsgálata a Darknet környezetében. Feltételeztük, hogy a hálózat gyenge performanciáját a YOLOv3 modelljének dupla konvertálása okozhatta. Az eredeti hálózat (ahhoz, hogy használni tudjam) két lépésben is konvertálva lett, először a TensorFlow formátumára, majd az OpenVINO IR formátumra. Ahhoz, hogy ezt a feltételezésünk alá tudjam támasztani a Darknet keretrendszerében is kipróbáltuk a hálózatot. Első lépésben letöltöttük a rendszer forrását, majd az általunk használt asztali számítógépre fordítottuk:

```
git clone https://github.com/pjreddie/darknet.git
cd darknet
make
```

A modell ebben az esetben is nagyon lassan futott az asztali számítógép CPU-ján:

```
~/Downloads/alexnet/dog_03.jpg: Predicted in 36.684101 seconds.
dog: 100%
```

Darknet YOLOv3	Darknet YOLOv3 Tiny
	
Feldolgozás: 36,47 másodperc	Feldolgozás: 1,43 másodperc (0,70 FPS)
	
Feldolgozás: 45,65 másodperc	Feldolgozás: 1,74 másodperc (0,575 FPS)
	
Feldolgozás: 37,16 másodperc (0,027 FPS)	Feldolgozás: 1,51 másodperc (0,662 FPS)

5. Táblázat: A YOLOv3 és a YOLOv3 Tiny modellek pontosságának összehasonlítása Intel i5 CPU-n futtatva. (saját szerkesztés, képek forrása: www.pikrepo.com és Hungarovet Állatkorház)

A mérési eredmények alapján megállapítható, hogy a Darknet YOLOv3 hálózatának gyenge teljesítménye elsősorban nem a modellek konvertálásából fakad. A modell egyszerűen rosszul teljesít CPU-n futtatva, az Nvidia GPU-n viszont – a fejlesztő szerint – nagyságrendekkel gyorsabb [9] A YOLOv3 modellel kapcsolatos vizsgálódások több dologra mutattak rá. Az egyes modellek struktúrája, belső működése – implementációtól függően – speciális is lehet. Erre példa a Darknet rendszer Region layer-e, ami ebben a rendszerben jelent meg először. [10] Ez nemcsak a más modellező eszköz formátumára való konverziót nehezíti meg, de jelentős teljesítmény különbségek is felléphetnek, ha más eszközön is futtatni akarjuk. [9]

Objektum detektálása mozgóképen

Az eddigi vizsgálatok után egy mintaalkalmazás segítségével vizsgáltuk az Intel NCS2 eszközt. Az alkalmazás egy videostream-en végez objektum detektálási feladatot. Az objektum detektálást a MobileNet-SSD hálózattal végeztük. A hálózat a YOLO-hoz hasonlóan egy kép egyszeri futtatására (Single Shot) végzi el az objektum detektálást.

Az SSD hálózatok. Az SSD (Single Shot Detector) hálózatok a YOLO-hoz hasonlóan egy lépésben végzik el az objektumok lokalizációját és azonosítását (image classification). Első lépésben egy feature extraction történik a bemenetre helyezett képen, második lépésben pedig konvolúciós filterek segítségével add vissza téglalapokat (bounding boxes) és az azokhoz társított objektumokat (classes).

Mérés egy mintaalkalmazással. Az alkalmazás egy Python-ban írt szkript, mely megnyit egy videostream-et, minden egyes képkockára elvégzi az objektumdetektálást, majd ennek eredményét megjeleníti a képkockán. A megjelenítés a megtalált objektumok bekeretezését és címkézését jelenti. Az alkalmazást eredetileg úgy készítettük el, hogy egy webkamera képén dolgozott, de többszöri futtatás összehasonlíthatósága megkívánta, hogy mindig ugyanazon a videostream-en dolgozzon a szkript. A szkriptek szinkron, illetve aszinkron hívással érik el az IR-t (inference engine-t). A szinkron hívás során az OpenCV API-ját használtuk, az aszinkron hívásnál viszont az OpenVINO-ban lévő Python API-t. A méréshez használt videófájlt a Pikrepo[12] ingyenesen felhasználható videótárából töltöttük le.

A videó felbontása	320 x 240 pixel
Az osztályozás címkéinek száma	20 db (ennyi különböző objektumot tud felismerni)
Használt programozási környezet	Python (OpenCV és OpenVINO API-k)

6. Táblázat: A mérés paraméterei (saját szerkesztés)

A futtatás során arra voltunk kíváncsiak, hogy a környezetekben milyen sebességgel tudja a szkript feldolgozni a videó egyes képkockáit. A szemléletes eredményhez a mért feldolgozási időkből az egységnyi idő alatti feldolgozható képkockák (frame per sec) számát számoltuk.

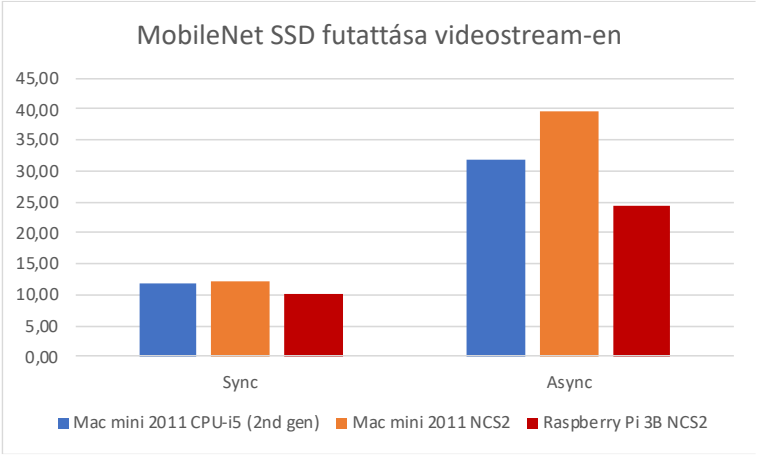
[12] https://www.pikrepo.com

5. Ábra: Képkocka feldolgozása videóból (saját szerkesztés)

	Szinkron feldolgozás sebessége (FPS)	Aszinkron feldolgozás sebessége (FPS)
Mac mini 2011 i5-CPU	11,92	31,70
Mac mini 2010 NCS2	12,24	39,52
Raspberry Pi 3B NCS2	10,21	24,51

7. Táblázat: Objektumdetektálás sebessége különböző környezetekben (saját forrás)

A mérési eredményeken szembeötlő, hogy az Inference Engine aszinkron elérése mennyivel gyorsabb feldolgozást eredményez. Az eddigi tapasztalatok alapján nem meglepő, hogy az Intel NCS2 eszköze jól teljesít a Intel második generációs i5-ös CPU-val szemben.



6. Figure: Objektumdetektálások összehasonlítása szinkron és aszinkron hívások kapcsán (saját forrás)

Az aszinkron hívásokkal megvalósított objektum detektálás már egy kis teljesítményű eszközön, a Raspberry Pi 3B-n is hasznosítható eredményt hozott. A 24 FPS feletti eredmény igazolja az Intel eszközének az – igaz, korlátozott – használhatóságát Edge eszközökben is. Az NCS2-t alkalmazó gépi látást használó alkalmazások tervezésekor figyelembe kell venni, hogy a mért eredmény egy kis felbontású videón készült, a felismerhető objektumok száma sem túl sok, ugyanakkor a Python interfészek használata (C++ helyett) is ront a teljesítményen.

Az alkalmazást (és teljesítményét) többféleképpen is tovább fejleszthetjük. A C++ API használatával elhagyhatjuk a Python okozta overhead-et, bár ez a C++ fordítási ideje miatt valamennyire lassabb fejlesztést teszt lehetővé. Egyszerre több Intel NCS2 használatával, az egymást követő képeket párhuzamosan tudjuk feldolgozni. Az NCS2 a számítógép USB interfészén csatlakozik, így egy alkalmas USB Hub segítségével könnyen több eszközt is csatlakoztatni tudunk a rendszerünkhöz. Az Intel által adott Inference Engine API támogatja több eszköz használatát, így szoftver oldalon is támogatott a „multi stick" felhasználás.

Az alkalmazás teljesítményére természetesen nemcsak a gyorsítóhardver és az azt meghívó kód van hatással, hanem a használt neurális hálózat is. Ahhoz, hogy az alkalmazásunkkal egy optimális teljesítményt érjünk el, a megfelelő neurális hálózat kiválasztása is fontos. Ez nemcsak a megfelelő struktúrát, hanem a megfelelő tanítást is jelenti. Azt láthattuk, hogy az egyszerűsített (pl.: YOLO Tiny) hálózatok hiába gyorsabbak, egyúttal pontatlanabbak is. Ezek a pontatlanságok részben javíthatók tanítással. Egy speciális feladatra szánt hálózatnak nem biztos, hogy több tucat vagy több száz objektumot kell felismernie, ezért érdemes a hálózatot az alkalmazásnak megfelelő módon tanítani. A tanítás azonban nagyon erőforrásigényes. Ezalatt nemcsak gépidő értendő, hanem a szükséges adatok (jelen esetben főleg képek) összeszedése, majd a tanítópontok összeállítása, amire sok-sok emberórát kell fordítanunk. A tanulmány készítése során csak előre tanított hálózatokat használtunk. Ez korlátozta a felhasználási lehetőségeket, hiszen a hálózatok csak a tanításkor megismert objektumokat ismerik fel.

A tanítás vizsgálata meghaladta jelent tanulmány kereteit, eredetileg sem vállalkoztunk rá, de a sokféle kipróbált hálózat azt mutatta, hogy egy komplett computer vision alkalmazás fejlesztési idejének jelentős részét kell erre a feladatra fordítani.

ÖSSZEFOGLALÁS

A neurális hálózatok gyakorlati alkalmazásakor számtalan feltételt, jellemzőt kell figyelembe venni ahhoz, hogy a megoldás ne csak funkcionális választ adjon a feladatra, hanem egyfajta optimális megoldás legyen. Optimális abban az értelemben, hogy úgy teljesíti a funkcionális és nem funkcionális követelményeket, hogy egyben takarékos is. Takarékos a számítási kapacitással, a felhasznált hardver elemekkel, az energiafogyasztással, a sávszélességgel, a memóriával, a tárterülettel. Ugyanakkor teljesítménye és pontossága kielégíti az alkalmazás által elvárt értékeket.

Természetesen egyszerre nem lehet minden elvárásnak megfelelni. Különösen úgy, hogy ezek gyakran „egymás ellen dolgoznak". A tanulmányban láthattunk példát arra, hogy egy hálózat kisebb és gyorsabban futtattható változata számottevően pontatlanabb, mint a nagyobb, de egyben erőforrásigényesebb párja. Azt is láthattuk, hogy az erősebb számítási erőforrások (lásd erősebb Intel CPU-k) természetesen jobb teljesítménnyel futnak, de mindez visszaköszön a magasabb árukban is.

Ezek az optimalizálási feladatok gyakran megoldhatatlanok, ami alatt azt értjük, hogy a rendelkezésre álló erőforrásokkal nem lehet az alkalmazás kívánt céljait teljesíteni.

Például több és gyorsabb gépi látást szeretnénk egy konkrét hardveres környezetbe tenni, de azok teljesítménye nem elegendő a feladatra. Ezekre gyakran az a megoldás, hogy a számításigényes feladatot „kiszervezik" egy számítási felhőbe. Különösen a kisebb teljesítményű, végponti eszközökben fordul elő, hogy a feladathoz szükséges neurális hálózatot nem lokálisan futtatják.

Az utóbbi években megjelentek olyan eszközök, melyek a neurális hálók speciális számítási igényeit igyekeznek támogatni kisteljesítményű, végponti eszközökben. Ide sorolható az Intel Movidius VPU családja, melyet a saját eszköze (Intel Neural Compute Stick) mellett, más partnerek[13] is termékeikbe építettek. Tanulmányunkban azt vizsgáltuk, hogy mennyire könnyű ezzel az USB-s eszközzel dolgozni, mennyiben segíti az egyre több helyen megjelenő objektum detektálás feladatot. A mérések eredményeképpen az igazolódott, hogy nemcsak összevethető teljesítményű az idősebb, de még használatban lévő általános célú processzorokkal (Intel i5 CPU: 2nd / 4th generation), hanem önállóan is megállja a helyét az információs rendszerek végpontjain futó kis teljesítményű eszközökben.

Ezeknek a számítást támogató eszközöknek a fejlődése folyamatos. Az Intel mellett más vállalatok, például a Google és Nvidia is megjelentek a saját megoldásaikkal, ami azt vetíti előre, hogy a végponti (például IP kamera) eszközökben is egyre inkább megjelennek komolyabb gép látást igénylő alkalmazások. Ennek információbiztonsági vonatkozása is van. Egyrészt ezek az eszközök olyan komplex információkat fognak előállítani, továbbítani és adott esetben tárolni is, ami eddig csak a rendszerek adatközpontjában volt meg.

Gondoljunk arra, hogy egy gépi látást használó IP kamera is tudhatja majd, hogy pontosan kik és mikor közlekedtek a látómezejében. Az objektumazonosítás, az objektumkövetés segítségével pontos képe lehet a mozgó járművekről, tárgyakról. Ezek új információbiztonsági kihívást jelentenek az eszközök használóinak, de egyben új eszközök is lehetnek az információbiztonság fizikai védelmének biztosításához. Például egy okos kamera, mely nemcsak rögzíti az eseményeket, hanem elemzi is azt, képes arra, hogy ne csak általános mozgás érzékelése esetén küldjön riasztást, hanem összetettebb feltételeket is ki tudjon értékelni. Például riasztás munkaidőn kívüli teheráru forgalom észlelésekor vagy riasztás, ha egy rendezvényre többen léptek be, mint az előre meghatározott érték.

A gépi látást használó rendszerek alkalmazási lehetősége nagyon széles és különösen akkor lesz széles, ha általánosan elterjednek, mert lehetőség nyílik rá, hogy egyszerűbb eszközök is használhassák ezt a technológiát. Az Intel ezt a lehetőséget teremti meg a saját VPU (Visual Processing Unit) megoldásával.

[13] Intel VPU-t használó termékek: https://software.intel.com/content/www/us/en/develop/topics/iot/hardware/vision-accelerator-movidius-vpu.html

FELHASZNÁLT FORRÁSOK

[1] J. Hanhirova, T. Kämäräinen, S. Seppälä, M. Siekkinen, V. Hirvisalo és A. Ylä-Jääski, *„Latency and Throughput Characterization of Convolutional Neural Networks for Mobile Computer Vision”* 2018. [Online]. https://arxiv.org/pdf/1803.09492.pdf. [hozzáférés dátuma: 2021. május 18.].

[2] Buzáné Kis P., *„Ismerkedés a TensorFlow rendszerrel”* [Online]. http://biointelligence.hu/pdf/tf_bkp.pdf. [hozzáférés dátuma: 2021. május 18.].

[3] O. Kharkovyna, *„Top 10 Best Deep Learning Frameworks in 2019,”* 2019. [Online]. https://towardsdatascience.com/top-10-best-deep-learning-frameworks-in-2019-5ccb90ea6de. [hozzáférés dátuma: 2021. május 18.].

[4] ONNX, *„ONNX Weboldal,”* [Online] https://onnx.ai/about.html. [hozzáférés dátuma: 2021. május 18.].

[5] Keras, 2020. [Online]. https://keras.io/. [hozzáférés dátuma: 2021. május 18.].

[6] B. Vision, *„Caffe,”* 2020. [Online]. https://caffe.berkeleyvision.org/. [hozzáférés dátuma: 2021. május 18.].

[7] https://pjreddie.com/darknet/ [Online] [hozzáférés dátuma: 2021. május 18.].

[8] J. Redmon, S. Divvala, R. Girshick és A. Farhadi, *„You Only Look Once: Unified, Real-Time Object Detection,”* 2016. [Online]. https://arxiv.org/pdf/1506.02640.pdf. [hozzáférés dátuma: 2021. május 18.].

[9] J. Redmon, *„Installing Darknet,”* [Online]. https://pjreddie.com/darknet/install/. [hozzáférés dátuma: 2021. május 18.].

[10] „Converting YOLO Models to the Intermediate Representation (IR),” Intel Corporation, [Online]. https://docs.openvinotoolkit.org/2020.1/_docs_MO_DG_prepare_model_convert_model_tf_specific_Convert_YOLO_From_Tensorflow.html. [hozzáférés dátuma: 2021. május 18.].

Follow, like, post, publish! | Kövess, lájkolj, posztolj, publikálj!

https://biztonsagtudomanyi.szemle.uni-obuda.hu

https://www.linkedin.com/company/safety-and-security-sciences-review

https://www.facebook.com/biztonsagtudomanyi.szemle