ISSN 2676-9042

Vol 5, No 3, 2023.

2023, V. évf. 3. 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
**BORS Györgyi**
painter/festőművész
**Metamorphosis** painting | **Metamorfózis** című festménye látható

The Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences classified our journal as a "C" category.

Folyóiratunkat a Magyar Tudományos Akadémia IX. Gazdaság- és Jogtudományok Osztályának Hadtudományi Bizottsága „C" kategóriás folyóiratnak minősítette.

The Safety and Security Sciences Review is a classified journal by Hungarian Science Bibliography.

A Biztonságtudományi Szemle a Magyar Tudományos Művek Tára (MTMT) által minősített folyóirat.

**Our journal is indexed by the following databases**

**Folyóiratunkat a következő adatbázisok indexelik**

EBSCO

Electronic Periodicals Archive & Database | Elektronikus Periodika Adatbázis
https://epa.oszk.hu/04100/04186

Hungarian Periodicals Table of Contents Database | Magyar folyóiratok tartalomjegyzékeinek kereshető adatbázisa
https://matarka.hu/szam_list.php?fsz=2267&nyelv=hun

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

National Széchenyi Library Digital Library | OSZK Digitális Könyvtár
https://oszkdk.oszk.hu/DRJ/39186

Global Serials Directory | Globális Sorozatok Könyvtára
http://ulrichsweb.serialssolutions.com/title/1678275514425/863974

| 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 | Élelmiszer-biztonság |
| 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 |
| Facility Security | Létesítménybiztonság |
| Private Security | Magánbiztonság |
| Artificial Intelligence | Mesterséges intelligencia |
| Safety and Security in General | Munkabiztonság |
| Technical Security | Műszaki biztonság |
| Fire Safety and Disaster Management | Tűzbiztonság és katasztrófavédelem |

The **aim** of the journal is to publish studies, research reports, book reviews for professionals working in the field of security science or related scinces, or for those interested in the subject of the broadly disciplinary framework of military technical sciences, and for security awareness and developing a safety culture. We know that the cultivation of security sciences includes the study of the history of military and law enforcement security, as well as the knowledge of the historical aspects of our field of science, and its development. We are working towards to present the latest theoretical models and empirical research findings in our journal. We believe that our Journal and our authors can contribute to the creation of a world that enables a (more) secure life for all the inhabitants of the Earth by knowing the historical past and examining the events of the present with precision and accuracy.

**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.

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.

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 **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek, vagy a téma iránt érdeklődők számára a katonai műszaki tudományok, s így a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése. Tudjuk, hogy a biztonságtudományok művelésébe beletartozik a had-, rendészet- és biztonságtörténet vizsgálata, tudományterületünk történeti és történelmi vetületeinek, s így fejlődésének megismerése. Azon dolgozunk, hogy Folyóiratunkban bemutassuk jelenkorunk legújabb teoretikus modelljeit és empirikus kutatási eredményeit. Hiszünk benne, hogy Folyóiratunk és szerzőink a történelmi múlt ismeretével, a jelenkor eseményeinek precíz és akkurátus vizsgálatával hozzá tudunk járulni egy olyan világ megteremtéséhez, amelyik lehetővé teszi a Föld minden lakója számára a biztonságos(abb) életet.

**Megjelenés** negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.

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.

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 |

| 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 5, No 3, 2023.** | **2023. V. évf. 3. szám**

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

## HANKA László

hanka.laszlo@uni-obuda.hu

Dr. HANKA László Ph.D., is associate professor at Bánki Donát Faculty of Mechanical and Safety Engineering of Óbuda University. He has over 30 years' experience in higher education both in Hungarian and English and in research. She was the supervisor of several bachelor and master theses and consulted successfully defended PhD thesis as well. His basic research topics are applied mathematics, application of mathematical statistics and probability theory, risk assessment. He has over 60 scientific papers in Hungarian and Engish. Author of one book in Hungarian. He is member of an editorial board of university journal (Bánki Reports).

Dr. HANKA László Ph.D., az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának főállású egyetemi docense. Több mint 30 éves magyar és angol felsőoktatási és kutatási tapasztalattal rendelkezik. Számos alap- és mesterdolgozat témavezetője volt, valamint konzultált sikeresen megvédett PhD-dolgozatot is. Alapvető kutatási témái az alkalmazott matematika, a matematikai statisztika alkalmazása, kockázatelemzés. Több mint 60 tudományos közleménye van magyar és angol nyelven. Egy magyar nyelvű szakkönyv szerzője. A Bánki Közlemények nevű egyetemi tudományos folyóirat szerkesztőbizottságának tagja.

## JÓKAI Erika

jokai.erika@bgk.uni-obuda.hu

Erika JÓKAI, PhD, human and technical consultant in vocational rehabilitation, rehabilitation engineer, hospital and medical engineer, she is been working as a university lecturer and researcher since 2004. Professional leader of postgraduate trainings of Rehabilitation engineering and Human and Technical Consultant of Vocational Rehabilitation at Óbuda University. Her main research fields are the assistive technologies for rehabilitation, work-related ergonomics and vocational rehabilitation, and usability testing of worksimulators and work-assessment equipments in vocational guidance/rehabilitation.

JÓKAI Erika, PhD, foglalkozási rehabilitációs szaktanácsadó, rehabilitációs környezettervező szakmérnök, kórház- és orvostechnikai szakmérnök, 2004 óta dolgozik a felsőoktatásban oktatóként és kutatóként. Szakmai vezetője a Foglalkozási rehabilitációs humán és műszaki szaktanácsadó, valamint a Rehabilitációs környezettervező szakmérnök szakirányú továbbképzéseknek az Óbudai Egyetemen. Fő kutatási területe a rehabilitációs segítő technológiák, munkahelyi ergonómia és foglalkozási rehabilitáció, pályaválasztás során és a foglalkozási rehabilitációban alkalmazható munkaszimulátorok és munkaképességmérő műszerek használhatósági vizsgálatai.

## KARTALI Gabriella

kartali.gabriella@uni-obuda.hu

Gabriella KARTALI is currently the student of Óbuda University Doctoral School on Safety and Security Sciences. She graduated from Budapest Rejtő Jenő Technical College in 2006 and then in 2014 she gained her Business Development degree at the Commercial and Marketing department of Óbuda University. Her main research areas are the marketing solution aiming to help visually impaired people and connection between safety and altruism.

KARTALI Gabriella, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója. 2006-ban diplomát szerzett a Budapesti Műszaki Főiskola Rejtő Sándor Könnyűipari mérnöki Karán, valamint 2014-ben végzett az Óbudai Egyetemen Kereskedelem és Marketing BSc szakon, majd 2018-ban Vállalkozásfejlesztés MSc szakon. Főbb kutatási területei a látássérülteket segítő marketing megoldások vizsgálata, az altruista viselkedés, a biztonság és kapcsolata az altruizmussal.

## KERÉK Gábor

kerek.gabor@eduvizig.hu

Diploma in Civil Engineering (Eötvös József College, Faculty of Engineering, Baja 2000; Budapest University of Technology and Economics, Budapest 2008), Diploma in Hydroinformatics and Water Management (Budapest University of Technology and Economics, Budapest 2016), Deputy Head of Department – North-Transdanubian Water Directorate, Győr, Department of water protection and river basin management. Hydrological Expert - Subcommittee of the Hungarian-Austrian Water Committee, Danube Subcommittee of the Hungarian-Slovak Border Water Committee. Areas of expertise: hydrologic forecasting and assessment, hydrographic monitoring, river hydrometry, surface water resource management. Currently a doctoral student at the Doctoral School of Military Engineering at the National University of Public Service. Research thema: development possibilities of flood forecasts in the Rába river basin. Member of the Hungarian Hydrological Society since 2006, and currently a member of the board of the Győr regional organization. Member of the water management and hydraulic engineering department of the Győr-Moson-Sopron County Chamber of Engineers with planning permission.

Okleveles építőmérnök (Eötvös József Főiskola Műszaki Fakultás, Baja 2000; Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2008.), Hidroinformatikai és Vízgazdálkodási Szakmérnök (Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2016.), az Észak-dunántúli Vízügyi Igazgatóság Vízvédelmi és Vízgyűjtő-gazdálkodási osztályának helyettes vezetője, a magyar-osztrák vízügyi bizottság albizottságnak hidrológiai szakértője, a magyar-szlovák határvízi bizottság Duna-albizottságának hidrológiai szakértője. Szakterülete: hidrológiai előrejelzés és állapotértékelés, vízrajzi monitoring, folyami hidrometria, felszíni vízkészletgazdálkodás. Jelenleg a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának doktorandusza. Kutatási területe: árvízi előrejelzések fejlesztési lehetőségei a Rába vízgyűjtőjén. 2006 óta a Magyar Hidrológiai Társaság tagja, jelenleg a Győri területi szervezet elnökségi tagja. A Győr-Moson-Sopron megyei Mérnöki Kamara vízgazdálkodási és vízépítési szakcsoportjának tervezői és felelős műszaki vezetői jogosultsággal rendelkező tagja.

## MANDIĆ Dorottya

mandic.dorottya@uni-obuda.hu

My name is Dorottya MANDIĆ, and I graduated from the Technical College of Applied Sciences in Bachelor of Management Engineering in Subotica, Serbia. I received my master's degree in Mechatronical Engineering from the Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering. I am currently a doctoral student in Safety and Security Sciences at the Óbuda University Doctoral School. My research area is the analysis of the security of smart devices.

MANDIĆ Dorottyának hívnak, és a Műszaki Szakfőiskolán fejeztem be a tanulmányaimat Szabadkán, Szerbiában, mint mérnök menedzser. A mesterképzést az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnika Mérnöki Karán szereztem meg, mint okleveles mechatronikai mérnök. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója vagyok. A kutatási témám az okoseszközök biztonságának az elemzésével foglalkozik.

## MÓDNÉ TAKÁCS Judit

modne.t.judit@amk.uni-obuda.hu

Judit MÓDNÉ TAKÁCS is an assistant lecturer at Óbuda University and Deputy Head of the Science and Software Engineering Institute at the Alba Regia Technical Faculty. Currently, she is PhD student at Óbuda University, Security Sciences PhD School. Her main research interests are engineering educa-

MÓDNÉ TAKÁCS Judit az Óbudai Egyetem egyetemi tanársegéde és Alba Regia Műszaki Karának Természettudományi és Szoftvertechnológiai Intézetének helyettes vezetője. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatója. Fő kutatási területe a mérnökképzés, a biztonságtudatos-

tion, safety awareness, the role and development of soft skills in engineering education, adult education methodology, research on methods to inspire and motivate students to learn and practice STEM subjects.

ság, a soft skills szerepe és fejlesztése a mérnökképzésben, a felnőttképzés módszertana, a hallgatókat a STEM tantárgyak tanulására és gyakorlati alkalmazására inspiráló és motiváló módszerek kutatása.

## MOLNÁR Máté

molnar.mate@kgk.uni-obuda.hu

Máté MOLNÁR is a historian-sociologist, teacher of the University of Óbuda, Faculty Keleti Károly. Objects of his researches: course of the globalization, history of the geografic discoveries, the colonization, caracteristics of the western civilization, history of the ideas of the European Union, contemporary problems of the EU, and some questions of the life and political theory and activity of Dante Alighieri, and the historical significance of the chivalry.

MOLNÁR Máté történész-szociológus, az Óbudai Egyetem Keleti Károly Gazdasági Karának oktatója. A nemzetközi történelem és a jelenkori nemzetközi, globális világ politikai, társadalmi és gazdasági kérdéseit kutatja. Fő kutatási területei: a globalizáció folyamata, a nagy földrajzi felfedezések és a gyarmatosítás, az európai civilizáció (a Nyugat) fő jellegzetességei, az európai egységtervek és az Európai Unió története és jelenkori problémái, Dante életének, politikai eszméinek és politikai szerepének kérdései, és a lovagi kultúra jellegzetességei.

## MOLNÁR ZSOLT

molnar.zsolt@kvk.uni-obuda.hu

Zsolt MOLNÁR has MSc degree in electrical engineering, currently is assistant lecturer at the Kandó Kálmán Faculty of Electrical Engineering, Institute of Electronics and Communication Systems at Óbuda University. He is a PhD candidate at the Doctoral School of Security Sciences of the Óbuda University, his research area is "Concurrent, in-service testing of critical embedded systems". His main areas of teaching is electronic testing and medical devices, and the courses supporting these topics. He has led and participated in several successful industrial projects in the fields of measurement automation, electronic manufacturing and testing, industrial controls, and biological (agricultural and research-related) measurement and data collection.

MOLNÁR Zsolt okleveles villamosmérnök, jelenleg az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, Elektronikai és Kommunikációs Rendszerek Intézet tanársegéde. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorjelöltje, kutatási területe a „Kritikus beágyazott rendszerek üzem közbeni tesztelése". Oktatási területe az elektronikai tesztelés és az orvostechnikai készülékek, és az ezeket a témákat megalapozó tárgyak. Számos sikeres ipari projektet vezetett, illetve projektben vett részt a mérésautomatizálás, az elektronikai gyártás és tesztelés, az ipari vezérlések és a biológiai (mezőgazdasági és kutatásokhoz kapcsolódó) mérés és adatgyűjtés témakörében.

## NAGY Rudolf

nagy.rudolf@uni-obuda.hu

Dr. habil. Rudolf NAGY, retaired Colonel, is currently senior lecturer at Óbuda University. He studied in foreign educational institutions. He served as a CBRN defence officer, and took part in industrial safety tasks. He gained experience as an operations officer in the NATO SFOR mission. After that he became Deputy Head of the Emergency Management Department of Hungarian National Directorate General for Disaster Management. Summa cum laude earned a PhD degree in field of Critical Infrastructure

Dr. habil. NAGY Rudolf nyugalmazott ezredes, jelenleg az Óbudai Egyetem adjunktusa. Külföldi oktatási intézményekben tanult. Vegyivédelmi tisztként szolgált, és részt vett iparbiztonsági feladatokban. A NATO SFOR misszióban műveleti tisztként szerzett tapasztalatokat. Ezt követően az Országosl Katasztrófavédelmi Főigazgatóság Veszélyhelyzetkezelési Főosztályának helyettes vezetője lett. Summa cum laude minősítéssel szerzett PhD fokozatot a kritikus infrastruktúrák védelme területén. Később a Kataszt-

Protection. Later he was appointed Deputy Head of the Disaster Management Training Centre. He has been teaching subjects of safety and security sciences since 2015, and is responsible for the fire protection engineering specialization. He obtained a habilitated doctorate in the scientific study of self-ignition.

rófavédelmi Oktatási Központ vezetőjének helyettesévé nevezték ki. 2015 óta oktatja a biztonságtudományok tantárgyakat, a tűzvédelmi mérnöki specializáció felelőse. Habilitált doktori címet szerzett az öngyulladások tudományos vizsgálatából.

## NAGY Sarolta

nagy.sarolta@nnk.gov.hu

Sarolta NAGY is an occupational health specialist, she has been working in field of occupational health since 1996. She completed the „Training of trainers – Preparation for the teaching of training programs on accessibility in healthcare", organized by Ltd. for Equal Opportunities for Persons with Disabilities (FSZK) in 2013, and she completed the post-graduate training in employment rehabilitation human and technical consultant at the Budapest University of Technology and Economy in 2017. Her research topics are the factors influencing the disabled persons' employment, especially the aspects of occupational health and safety. Since 2011 she has conducted research with employees belonging to three disability groups (hearing-impaired, visually-impaired, mobility-impaired), mainly on their employment difficulties and about the assistive technologies they use, and the possible discrimination they experienced in the world of work. She participates in specialist training and also teaches at the Pedagogy and Rehabilitation of Hearing Impaired Persons Cours at the Eötvös Lorand University BGGYK Institute of Therapeutic Pedagogy and Rehabilitation.

NAGY Sarolta foglalkozás-egészségügyi szakorvos, 1996 óta dolgozik a foglalkozás-egészségügy területén. 2013-ban elvégezte az FSZK szervezésében a „Képzők képzése - Felkészítés akadálymentesítés témájú képzési programok oktatására az egészségügyben" képzést, 2017-ben pedig a Budapesti Műszaki Egyetemen a foglalkoztatási rehabilitációs humán és műszaki szaktanácsadó postgraduális képzést. Kutatási témái a megváltozott munkaképességű, fogyatékos személyek foglalkoztatását befolyásoló tényezők, különös tekintettel a munkavédelemre. 2011-től három fogyatékossági csoportba tartozó (hallássérült, látássérült, mozgáskorlátozott) munkavállalókkal végzett kutatásokat, elsősorban a munkavállalási nehézségeikről, az általuk használt segítő technológiákról és az esetlegesen megélt hátrányos megkülönböztetésről a munka világában. Részt vesz a szakorvos képzésben és az ELTE BGGYK Gyógypedagógiai Módszertani és Rehabilitációs Intézet Hallássérült személyek pedagógiája és rehabilitációja szakon óraadóként oktat.

## PAULIK László

paulik.laszlo@bgk.uni-obuda.hu

László PAULIK (1976) is a certified biology-physics teacher. He is currently an assistant lecturer at the Donat Banki Faculty of Mechanical and Safety Engineering at Obuda University and a first-year PhD student at Obuda University's Doctoral School of Safety and Security Sciences. His enthusiasm in science fiction is mirrored in his artificial intelligence research. Furthermore, he is quite interested in trend research and attempts to study the links between technological developments and societal changes. He operates as a water tour leader and tour guide as a proponent of an active lifestyle. He has been doing martial arts for over a decade. In addition, as a starting amateur diver, he gets to know the deep-water environment. His field of research: investigation of robots and artificial intelligence based on security science and cyber security aspects.

PAULIK László (1976) okleveles biológia-fizika szakos tanár. Jelenleg az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán tanársegéd, valamint az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának első éves PhD hallgatója. Science-fiction iránti érdeklődése a mesterséges intelligencia területén való kutatásban is megmutatkozik. Emellett behatóan érdeklődik a trend-kutatás iránt és igyekszik nyomon követni a technológiai fejlődés és a társadalmi változások összefüggéseit. Aktív életmód híveként vízitúravezetőként és túravezetőként tevékenykedik. Több, mint tíz éve foglalkozik harcművészettel. Mindemellett kezdő amatőr búvárként ismerkedik a mélyvízi világgal. Kutatási területe: robotok és a mesterséges intelligencia vizsgálata biztonságtudományi és kiberbiztonsági szempontok alapján.

## POGÁTSNIK Monika

pogatsnik.monika@amk.uni-obuda.hu

Monika POGÁTSNIK is an associate professor at the University of Óbuda and a vice dean of the Alba Regia Technical Faculty. Her main area of research is engineering pedagogy, with a particular focus on work-based learning, non-cognitive skills, career attitudes. More than 120 citations have been received for her more than 90 scientific publications.

POGÁTSNIK Monika az Óbudai Egyetem docense és az Alba Regia Műszaki Kar dékánhelyettese. Fő kutatási területe a mérnökpedagógia, különös tekintettel a munkaalapú tanulásra, a nem kognitív készségekre és a pályaorientációs attitűdökre. Több mint 90 tudományos publikációjára több mint 120 idézet érkezett.

## RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Zoltán RAJNAI (1962) engineer colonel, dean of the Óbuda University, Donát Bánki Faculty of Mechanical and Security Engineering, operating manager of the Doctoral School of Security Sciences of the University, cyber coordinator of Hungary. He completed his military studies at the Máté Zalka Military Technical College and then at the Miklós Zrínyi Military Academy. From 1993 he worked as a university adjunct at the Miklós Zrínyi Military Academy and the Miklós Zrínyi National Defense University, the predecessor institutions of the University of Public Service. Under its leadership the Telecommunication Department at NKE was established in 2008 by merging the Faculties of Telecommunication of the János Bolyai Faculty of Military Engineering and the National Defense University. He received his doctorate in 2001 and his habilitation in 2006. He won a research scholarship named after János Bolyai of the Hungarian Academy of Sciences. Between 2007 and 2011 he was the Hungarian program director of the COMMIT French-Hungarian International Science (R & D & I) project, and at the same time a guest lecturer in France at the Military Technical College in Rennes. He is the president of the Puskás Tivadar Telecommunication Comrades Association since 2012. His research interests include security of communication networks in qualified periods, protection of critical infrastructure, information security.

RAJNAI Zoltán (1962) mérnök ezredes, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar dékánja, az Egyetem Biztonságtudományi Doktori Iskolája operatív vezetője, Magyarország kiberkoordinátora. Katonai tanulmányait a Zalka Máté Katonai Műszaki Főiskolán, majd a Zrínyi Miklós Katonai Akadémián végezte. 1993-tól a Zrínyi Miklós Katonai Akadémián, illetve a Zrínyi Miklós Nemzetvédelmi Egyetemen, a Nemzeti Közszolgálati Egyetem jogelőd intézményeiben dolgozott egyetemi oktatóként. A vezetésével alakult meg 2008-ban a Bolyai János Katonai Műszaki Kar és a Nemzetvédelmi Egyetem Híradó tanszékeinek összevonásával az NKE-n ma is működő híradó tanszék. 2001-ben doktori fokozatot, 2006-ban habilitációt szerzett. Elnyerte a Magyar Tudományos Akadémia Bolyai Jánosról elnevezett kutatási ösztöndíját. 2007 és 2011 között a COMMIT francia-magyar nemzetközi tudományos (K+F+I) projekt magyarországi programigazgatója volt, ezzel párhuzamosan vendég-oktató Franciaországban a Rennes-i Katonai Műszaki Főiskolán. 2012-től a Puskás Tivadar Híradó Bajtársi Egyesület elnöke. Kutatási területei: minősített idő-szakok kommunikációs hálózatainak biztonsága, kritikus infrastruktúra védelme, információbiztonság.

## REVOLY András

Revoly.Andras@uni-mate.hu

András REVOLY graduated from the Faculty of Electrical Engineering and Information Technology of the Technical University of Budapest. He has been working for years on the development of software and elearning materials. He is currently engaged in teaching and research at the Hungarian University of

REVOLY András a Budapesti Műszaki Egyetem Villamosmérnöki és Informatika Karán szerzett villamosmérnöki diplomát. Évek óta foglalkozik szoftver- és elearning anyagok fejlesztésével. Jelenleg a Magyar Agrár- és Élettudományi Egyetemen végez oktatási és kutatási tevékenységet. Az egyetem In-

Agriculture and Life Sciences (MATE). He is a departmental staff member at the Department of Computer Science of the University and a 2nd year PhD student at the Doctoral School of Mechanical Engineering. In his teaching activities he teaches basic computer science and programming courses. His research field include modelling of AI-based crop management programs for vertical farms, and hardware and software development of related cloud-based sensor systems. His developments integrate closed plant production system (CPPS) data collection with cloud computing and mobile visualization.

formatika Tanszékén tanszéki munkatárs és a Műszaki Doktori Iskola 2. éves PhD hallgatója. Oktatási tevékenysége során informatikai alapozó és programozási tantárgyakat oktat. Kutatási területe a vertikális farmokban alkalmazható AI alapú termesztési programok modellezése, valamint az ehhez kapcsolódó felhőalapú szenzorrendszerek hardveres és szoftveres fejlesztése. Fejlesztéseiben integrálja a zárt mezőgazdasági rendszerben keletkezett adatok gyűjtését a felhőalapú adatfeldolgozással és mobil megjelenítéssel.

## SÁNDOR Barnabás

sandor.barnabas@gmail.com

Barnabás SÁNDOR is a security engineer and cybersecurity researcher. He currently holds the position of Cyber Security Architect at MOL Group. He has more than ten years of experience in IT design, operation, and security. His main area of expertise is cybersecurity, where he is involved in the design and vulnerability assessment of IoT devices, software, and system platforms. His main research area is cyber security for smart buildings. The experience and knowledge gained over the years have led to continuous development being of utmost importance to him, which is why he is currently a Ph.D. candidate at the Doctoral School of Security Sciences at Óbuda University. Since 2018, he has also been an external lecturer at the university. Furthermore, he regularly participates in national and international conferences and is constantly invited by the media on professional issues.

SÁNDOR Barnabás okleveles biztonságtechnikai mérnök és kiberbiztonsági kutató. Jelenleg a MOL-csoportnál Cyber Security Architect pozíciót tölt be. Az informatika területén több, mint 10 éves tervezői és üzemeltetői és biztonsági tapasztalattal rendelkezik. Fő szakterülete a kiberbiztonság, ahol az IoT eszközök, szoftverek és rendszerterek tervezésében és sérülékenység-vizsgálatában vesz részt. Fő kutatási területe az intelligens épületek kiberbiztonsága. Az évről évre megszerzett tapasztalat és tudás vezetett oda, hogy kiemelten fontos számára a folyamatos fejlődés, éppen ezért jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában doktorjelölt. Mellette 2018 óta külsős óraadó az egyetemen. Folyamatosan vesz részt hazai és nemzetközi konferenciákon, illetve szakmai kérdésekben folyamatos felkéréseket kap a médiában.

## SEPRÉNYI Patrik

patrik.seprenyi@gmail.com

Patrik SEPRÉNYI, PhD student at The Doctoral School of Military Sciences, University of Public Service. He obtained his bachelor's and master's degree in International Security and Defence Policy at the same university's Faculty of Military Science and Officer Training. He spent the 2019/2020 academic year at the Beijing International Studies University (BISU). He is a former member of the Chinese Scientific Student Association and the Advanced College for Security Policy of the University of Public Service. He is currently researching the security policy trends of the XXI. century.

SEPRÉNYI Patrik a Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskolájának doktorandusz hallgatója. Alap és mesterszakos diplomáját ugyanezen egyetem, Hadtudományi- és Honvédtisztképző Karának, Nemzetközi biztonság- és védelempolitika szakán szerezte. Tanulmányai során a 2019/2020-as tanévet a Pekingi Nemzetközi Tanulmányok Egyetemén (BISU) töltötte. A Nemzeti Közszolgálati Egyetem, Kínai Tudományos Diákkörének és Biztonságpolitikai Szakkollégiumának egykori tagja. Jelenleg a XXI. század biztonságpolitikai trendjeit kutatja.

## SOMOGYI Tamás

somogyi.tamas@phd.uni-obuda.hu

Holds a Master's degree in IT engineering and a complementary degree in Legal Studies. He is currently a PhD student at the Doctoral School on Safety and Security Sciences, Óbuda University. His research area is the security issues of the financial sector's infrastructure.

Mérnök-informatikus, mérnök-szakjogász. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója. Kutatási területe a bankszektor létesítményi infrastruktúrájának védelme és ellenállóképességének fokozása.

## SZABÓ István

Szabo.Istvan.prof@uni-mate.hu

Dr. István SZABÓ, Professor, is Vice-Rector of the Hungarian University of Agriculture and Life Sciences (MATE). He is also the Head of the Institute of Technology and a permanent member of the Council of the Doctoral School of Mechanical Engineering. In his teaching and research work, he has long been involved in the challenges and novel solutions of precision agriculture. He is also the supervisor of several PhD students researching in this field. In his research, he has worked on several topics: the role of agricultural machinery in precision agriculture, the use of intelligent sensors and the application of artificial intelligence algorithms in engineering and agriculture. He has extensive international contacts and has led several international inter-university collaborations.

Dr. SZABÓ István egyetemi tanár a Magyar Agrár- és Élettudományi Egyetem rektorhelyettese. Emellett ez egyetem Műszaki Intézetének vezetője és az Műszaki Doktori iskola tanácsának állandó tagja. Oktatói és kutatói munkája során régóta foglalkozik a precíziós mezőgazdaság kihívásaival és újszerű megoldásaival. Több a témában is kutató doktorandusz témavezetője. Kutatási tevékenysége során több tématerülettel is foglalkozott: a mezőgazdasági gépek precíziós mezőgazdaságban elfoglalt szerepe, intelligens szenzorok használata, valamint mesterséges intelligencia algoritmusok alkalmazás a gépészet és mezőgazdaság területén. Kiterjedt nemzetközi kapcsolatokkal rendelkezik, számos nemzetközi egyetemközi együttműködés vezetője.

## TAKÁCS-GYÖRGY Katalin

takacsnegyorgy.katalin@kgk.uni-obuda.hu

Prof. Dr. TAKÁCS-GYÖRGY, Katalin Ph.D., is full time professor at Keleti Faculty of Business and Management of Óbuda University. She has over 35 years' experience in higher education both in Hungarian and English and in research, engaged in talent management. She was the supervisor of over 150 bachelor and master theses and consulted 13 successfully defended PhD thesis. Her key research topics are economic aspects of sustainability, food safety and security, enterprise behavior, adaptation and attitudes to innovative solutions. She has over 100 scientific papers, book chapters in Engish. She is the editor and member of the editorial board of several international and domestic scientific journals (Journal of Central European Green Innovation and Acta Carolus Robertus, furthermore she is co-chief editor of Hungarian scientific journal of agricultural economics: Gazdálkodás).

Prof. Dr. TAKÁCS-GYÖRGY Katalin Ph.D., az Óbudai Egyetem Keleti Gazdasági Karának főállású egyetemi tanára. Több mint 35 éves magyar és angol felsőoktatási és kutatási, tehetséggondozási tapasztalattal rendelkezik. Több mint 150 alap- és mesterdolgozat témavezetője volt, valamint 13 sikeresen megvédett PhD-dolgozat konzultált. Kiemelt kutatási témái a fenntarthatóság gazdasági vonatkozásai, az élelmiszer- és élelmezésbiztonság, a vállalati magatartás, az innovatív megoldásokhoz való alkalmazkodás és attitűdök. Több mint 100 tudományos közleménye, angol nyelvű könyvfejezetei vannak. Számos nemzetközi és hazai tudományos folyóirat (Journal of Central European Green Innovation és Acta Carolus Robertus) szerkesztője és szerkesztőbizottsági tagja, valamint a Gazdálkodás című magyar agrárgazdasági tudományos folyóirat társfőszerkesztője.

## TARR Bence

Tarr.Bence.Gyula@uni-mate.hu

Bence TARR is an electrical engineer at the Hungarian University of Agriculture and Life Sciences (MATE). He is an assistant professor at the Department of Computer Science and a 3rd year PhD student at the Doctoral School of Mechanical Engineering. He has been working for years on the development of textbooks and educational materials in various fields of informatics. In his teaching activities he teaches subjects in computer science, including data science and programming. His research interests include the development of AI-based prediction algorithms for crop and livestock production and their efficiency. His developments focus on methods, software and mobile applications supporting precision agriculture.

TARR Bence villamosmérnök a Magyar Agrár- és Élettudományi Egyetemen munkatársa. Az egyetem Informatika Tanszékén egyetemi tanársegéd és a Műszaki Doktori Iskola 3. éves PhD hallgatója. Évek óta foglalkozik szakkönyvek és oktatási anyagok fejlesztésével az informatika különböző területén. Oktatási tevékenysége során informatikai azon belül adattechnológiai és programozási tantárgyakat oktat. Kutatási területe a növény és állattenyésztés során használható MI alapú predikciós algoritmusok fejlesztése és hatékonyságuk vizsgálata. Fejlesztései a precíziós mezőgazdaságot támogató eljárások, szoftverek, mobil applikációk területére fokuszálnak.

## WU Yue

wuyue.budapest@gmail.com

Wu Yue is a Ph.D. student at Doctoral School on Safety and Security Sciences, Obuda University. Her research interest is food security and sustainable agriculture. She is the president of Chinese Students and Scholars Association in Hungary at Obuda University.

Wu Yue Ph.D. az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója. Kutatási területe az élelmezésbiztonság és a fenntartható mezőgazdaság. Az Óbudai Egyetem Magyarországi Kínai Diákok és Tudósok Egyesületének elnöke.

## ZAKARIÁS Rebeka

zakarias.rebeka@gmail.com

My name is Rebeka ZAKARIÁS, I work as an HSE expert in the pharmaceutical industry. I graduated from the Faculty of Bioengineering at Szent István University in 2018, and then further developed my knowledge with a degree in Industrial Safety Engineering from the Faculty of Mechanical and Safety Engineering at Óbuda University in 2023. In the course of my professional work, I was exposed to the importance of occupational hygiene measurements and gained experience in the validated and accredited performance of these measurements.

ZAKARIÁS Rebekának hívnak, HSE szakértőként dolgozom gyógyszeripar területén. Szent István Egyetem Biomérnöki szakán szereztem meg első diplomámat 2018-ban, majd ezt követően fejlesztettem tovább tudásomat az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnika Mérnöki Karán megszerzett Munkavédelmi szakmérnök diplomámmal 2023-ban. Szakmai munkám során kerültem kapcsolatba a munkahigiénés mérések fontosságával, illetve tapasztalatot nyertem az említett mérések validált és akkreditált elvégzésében.

**Creator of the cover image** | **A borítón látható kép alkotója**

## BORS Györgyi

borsgyorgyi77@gmail.com

She was born in 1977 in Tapolca, Hungary. The tragic early death of his mother was decisive in her life because she was then raised in state care until she was 18 years old. During her years there, she realized

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött

that she found the greatest pleasure in art. She studied graphic art for several years at the Railway School of Music and Fine Arts in Budapest with the painter and sculptor György BENEDEK, and later with Árpád "Pika" NAGY and Zoltán SEBESTYÉN. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán GASZTONYI, from whom she learned the different techniques of oil painting. She is narrative painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

rá, hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában BENEDEK György festő és szobrászművésznél, majd később NAGY Árpád „Pika"-nál és SEBESTYÉN Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere GASZTONYI Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

| 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 5, No 3, 2023.** | **2023. V. évf. 3. szám**

**CONTENT** | **TARTALOM**

# THE QUESTION OF INTERNAL STABILITY AND SECURITY IN THE FLORENCE OF DANTE'S TIME (PART I.)

# A BELSŐ STABILITÁS ÉS BIZTONSÁG KÉRDÉSE A DANTE KORABELI FIRENZÉBEN (I. RÉSZ)

MOLNÁR Máté[1]

**Abstract**

Corso Donati was the member of a famous and great family in Florence in the 13. and 14. century, the leader of the Parte Guelfa, and the Blacks, and the relativ of Dante Alighieri, who was in the faction white of the party. This study treat the short history of the family Donati, the life and career of Corso, who was an important protagonist of the last decades of 13. and the first years of the 14. century in Florence. Relate the events significant in the war between the Guelfs and Ghibellines, and the struggle for power in Florence between the nobility (Magnati) and bourgeoisie (Popolani), and the Clans Donati and Cerchi. Present the civil war at the end of 13. century and at the beginning of 14. century in Florence. Describe and analyse the caracter of Corso Donati, and his role in the history of Florence and Italy, and in the expulsion of the Whites (and Dante), and his ambition for the overlordship (signoria) of his city.

**Keywords**

Ghibellines, Guelfs, „Blacks", „Whites", Chivalry, Clans

**Absztrakt**

Corso Donati az egyik leghíresebb és legnagyobb firenzei család tagja volt és vezetője a Guelf Pártnak, valamint azon belül a Feketéknek, és rokona Danténak, aki a párt fehér frakciójához tartozott. A jelen tanulmány röviden ismerteti a Donatiak történetét és Corso életútját, aki főszereplője volt a firenzei politikának a 13. század utolsó évtizedeiben, és a 14. század első éveiben. Szót ejt a pápapárti guelfek és a császárpárti ghibellinek közötti harcokról, valamint a nemesség (Magnati) és a nagypolgárság (Popolani), illetve a Donati és a Cerchi klánok közötti hatalmi harcokról, a polgárháborús helyzetről, amely a 13-14. század fordulóját jellemezte Firenzében. Jellemzi Corso személyiségét, és bemutatja szerepét Dante és a fehérek száműzetésében, valamint elemzi hatalmi ambícióit a város feletti uralom (signoria) megszerzésére.

**Kulcsszavak**

ghibellinek, guelfek, „feketék", „fehérek", lovagság, klánok

[1] molnar.mate@kgk.uni-obuda.hu | ORCID: 0009-0006-5943-0277 | assistant professor, University of Óbuda Department of Marketing and Business Sciences | adjunktus, Óbudai Egyetem Keleti Károly Gazdasági Kar Marketing és Üzleti Tudományok Intézete

## A DONATIAK

A Donatiak Firenze régi, gazdag, befolyásos nemesi családjai közé tartoztak. 1065-ben már ispotályt alapítottak a Pinti kapu és a Porta San Piero Maggiore közelében, számos birtokkal rendelkeztek a város falain kívül, elsősorban Mugello területén, de gyapjúfeldolgozó műhelyt és malmokat is üzemeltettek (melyeket az Arno vizével hajtottak), és több házat és tornyot birtokoltak a városon belül. Fő szálláshelyük a mai Donati téren volt, de egy másik torony is az övék volt a mai Alighieri utcában, amelyet az Alighieri-család vásárolt meg (itt született és élt 1301-ig Dante is), más lakásaik a porta San Piero utcában voltak, szemben a Portinari és Ricci házakkal. A Donatiak már a XIII. század elejétől aktívan részt vettek Firenze politikai életében, a guelfek, tehát a pápapártiak oldalán harcoltak a császárság ellen, ezért a guelfek Montapertinél, 1260-ban elszenvedett nagy veresége után sokan közülük emigrációba kényszerültek, házaik, tornyaik egy részét lerombolták, súlyos vagyoni veszteségeket szenvedtek. 1268-ban, két évvel a beneventói győztes csata után térhettek vissza otthonaikba, ahol a születési-katonai nemesség státuszának megfelelő életvitelt folytatták, mesterségeket többnyire nem tanultak és nem léptek be a céhekbe (bár egyesek közülük ügyvédi tevékenységet vállaltak). A Donati-klán fő jövedelmei a földbirtokokból, városi házaik egy részének bérbe adásából, katonai parancsnoki (condottiero) és egyéb városi tisztségek, így a podestà (kb. városbíró) és a népkapitány, esetenként a rektor (kormányzó) tisztségek betöltéséből származtak.

Oerter megállapítása szerint a régi nemesi családok közül a Donati volt az egyetlen, amely hasonló címert mert viselni, mint Firenze városa (felül vörös, alul fehér mező, míg a városé ennek a fordítottja volt). Stahl is kihangsúlyozza, hogy a Donatiak Firenze legharciasabb nemzetségeihez tartoztak, a XIII. században az összes utcai harcban részt vettek a városban. A német szerző a Donatiakat az Abbatiakkal együtt a XII. század utolsó harmadától Firenze vezető klánjának tekinti, és kiemeli annak jelentőségét, hogy a Donatiak 1172-ben, 1174-ben és 1204-ben is konzuli tisztségeket töltöttek be Firenzében, amely akkoriban a legfontosabb magisztratúrának számított (számuk általában 2-5 között mozgott). Giovanni Villani, a kortárs történetíró azonban azt is megjegyzi, hogy a Donatiak, bár vitéz nemesemberek és bátor harcosok voltak, sokak szemében rossz hírűnek („Malefami") számítottak.

E rossz hírnév egyik fő oka az volt, hogy a firenzei hagyomány a ghibellinek és guelfek közötti háborúskodás kezdetét is a Donati-klánhoz kötötte. Történt ugyanis egyszer (valószínűleg 1215-ben), hogy Gualdrada Donati asszony (Corso nagymamája) megszólított egy fiatal nemesembert, Buondelmonte Buondelmontit, aki a háza előtt haladt el, hogy neki szánta egyik szép lányát feleségül (akit rögtön be is mutatott a fiatalembernek), és megfeddte őt, amiért az egy másik lányt jegyzett el magának az Amidei családból. Buondelmonti úr nagyon bánta ezt (a lány valóban nagyon szép lehetett), de az eljegyzési szerződés megszegése akkoriban súlyos sértésnek számított a nemesi családok között, amire Machiavelli is rámutat Firenze történetéről szóló művében. Tény azonban, hogy megfelelő bírság kifizetésével az érintett család bocsánatát el lehetett nyerni (ezt a bírságot Gualdrada asszony magára vállalta), de az előkelő Amideiek – más velük rokon és velük szimpatizáló nemzetségek, mint az Ubertiek és a Lambertiek biztatására – úgy döntöttek, hogy nem nyelik le az őket ért sérelmet, sőt bosszút állnak a megaláztatásért. 1216 Húsvét reggelén a Ponte Vecchio közelében megtámadták és megölték Buondelmontét, aminek következtében egy állandóan kiújuló klán-háború kezdődött a két érintett család között, és mivel az Amideiek és pártfogóik a ghibellinek, a Buondelmontiak és a Donatiak a guelfek közé tartoztak,

ez a konfliktus is súlyosbította a császárpártiak és a pápapártiak közötti ellentéteket Firenzében.

Corso Donati minden valószínűség szerint 1250 táján, de legkésőbb 1253-ban született, mivel 1278-ban tagja volt a firenzei Század Tanácsának, amihez be kellett töltenie a 25. életévét. Ugyancsak e mellett szól azon tény, hogy Corsót az 1270-es évek második felében a korabeli iratok már dominus-ként, tehát lovagként emlegetik, 1280 táján (Oerter szerint 1277-ben) pedig már gyámja lett özvegy nővérének, Ravennának és gyermekeinek. 1284-ben több alkalommal szerepelt a firenzei tanácsokban, február 27-én pedig Bologna népkapitányává választották (a megbízás általában fél évre szólt), és mivel Bologna Észak-Itália legjelentősebb városai közé tartozott, nem neveztek ki népkapitánnyá egy kezdő fiatal lovagot, Corso pedig ekkoriban már kb. 31 éves lehetett. Corso renoméjának bizonyítékaként említhetjük, hogy 1287-ben Padova, 1288-ban Bologna podestája, 1289-ben Pistoia „helyettes" népkapitánya, 1292-ben pedig Parma podestája lett, tehát Itáliában elismerték vezetői képességeit is (a podestà és a népkapitány tisztségekre többnyire más városból származó nemeseket hívtak, biztosítandó a pártatlanságukat egy adott városban).

Firenzében ekkoriban a családi klánok voltak a legfőbb politikai egységek, nagy létszámuk, házassági kapcsolataik és katonai erejük miatt döntő szerephez jutottak a politikai harcok során. Corso Donati 1277-ben lett a Donati-klán feje (capo), vezetője (a pátriárka elnevezést is használták a korban), ami egyúttal azt is jelentette, hogy a guelf párt vezetőjévé is vált, valamint a születési nemesség politikai csoportosulása („Magnati", kb. mágnások, arisztokraták) irányítása is az ő befolyása alá került, bár természetesen más nagy nemzetségek, így a Visdominiak, a Tosinghiak (della Tosák) is jelentős szerepet töltöttek be a város vezetésében, lakóhelyük kerületében, a Porta San Pieróban pedig korlátlan urak voltak. Corso tehát a belső hatalmi harcokban, - amelyek a főnemesi párt (Magnati) és az üzleti, kereskedő-ipari vállalkozói burzsoázia vezette polgári erők („Popolani", kb. néppártiak, plebejusok) között zajlottak - főszerepet játszott. De ezek a konfliktusok, sőt időnkénti összecsapások váltakozó sikerrel folytak, és esetenként a katonai nemesség kudarcához vezettek, amit egy 1286-ban bekövetkezett esemény is mutatott. Ekkor a Corso vezette magnatik fegyveres csapata ki akart szabadítani egy közülük való, bátor, de gyilkosság vádjával halálra ítélt lovagot (Totto dei Mazzinghi-t), a túlerőben levő közrendű lakosság azonban felfegyverkezett, és az összecsapásban meghátrálásra kényszerítette a számbelileg jóval kisebb nemeseket. Giovanni Villani beszámolója szerint az akció után a Comune (a városállam vezetősége) pénzbírságra ítélte Corsót, mivel ő kezdeményezte a zavargást, és akadályozta az igazságszolgáltatás működését.

Corso azonban természetesen nem elsősorban a Firenzében zajló városi csetepatékban vitézkedett, hiszen a kor egyik legjobb itáliai lovagja, katonai parancsnoka (kapitánya) volt. Már fiatalon lovaggá ütötték (ezt a címet nem lehetett örökölni!), és többnyire a városi tanácsokban is figyeltek a felszólalásaira, ha a ghibellinek és a guelfek, illetve Firenze és a közeli városállamok konfliktusairól, harcairól volt szó. Így Donati részt vett 1285-ben Genova és Lucca mellett a ghibellin Pisa elleni harcokban, 1286-ban a ghibellin száműzöttek menedékeként szolgáló Poggio Santa Cecilia elleni támadásban (e hadjáratban valószínűleg Dante is jelen volt), 1289-ben a Guelf Liga és az arezzóiak vezette ghibellin sereg nagy csatájában, valamint a Pisa elleni új háborúban 1290-ben (e városállam erőbeli hátrányait a kor kétségkívül legnagyobb itáliai hadvezére, Guido da Montefeltro tudta időnként kompenzálni, akinek két fia is elesett a campaldinói csatamezőn a firenzeiek ellen, illetve az

üldözés során). Mivel Corso lovagi és katonai parancsnoki hírnevét a campaldinói csatában tanúsított bátorsága és helyzetfelismerése öregbítette leginkább, röviden kitérek az ütközetben játszott szerepére.

Corso Donati, Pistoia helyettes népkapitányaként a kb. 200 fős pistoiai és luccai haderő élén érkezett meg 1289. június 11-én a campaldinói csatamezőre, ahol egy rendkívül fontos feladatot, a tartalék vezetését bízták rá (ennek fő funkciója az volt, hogy vereség esetén fedezze a visszavonuló sereget, és megakadályozza a nagyobb ember veszteséget). Corsónak fővesztés terhe mellett megtiltották, hogy külön parancs nélkül beavatkozzék az ütközetbe, csapatát egy kis dombon rejtették el a fák mögé, ott kellett várakoznia. Ő azonban a magaslatról a csata egész lefolyását jól láthatta, és egy idő után észrevette, hogy a ghibellinek kezdenek felülkerekedni, így az ütközet vesztésre áll (ezt a csatában részt vevő Dante is leírta később egy levelében!). Corso ekkor a csapatához fordult, és kijelentette, hogy ha a csata elvész, akkor ő a honfitársaival együtt akar meghalni, ha pedig győznek, akkor bárki megtalálja őt Pistoiában, hogy a fejét vegye. Meg kell itt jegyeznünk, hogy az adott helyzetben már nem is volt a guelf seregben parancsadásra képes személy, a fővezér, Amerigo da Narbona ugyanis megsebesült, a helyettese, Guillaume de Durfort lovag pedig már az ütközet elején elesett. Corso tehát rohamra vezette a tartalékot, amely a dombról lendületet véve oldalba támadta az ellenséget, és percek alatt megfordította a csatát. Mind a korabeli történetírók, mind a kutatók egyetértenek abban, hogy ezt az ütközetet (amelyben egyébként kb. 20 000 fő vett részt a két oldalon) Corso Donati zseniális helyzetfelismerése, bátorsága és azonnali (parancsmegszegést is vállaló) beavatkozása döntötte el a Guelf Liga és Firenze javára.

## CORSO ÜGYEI ÉS A HATALMI HARCOK FIRENZÉBEN

Ebben a fejezetben Corso pályafutásának alakulásáról és a Donati-klán (consorteria) vezetőjeként felvállalt családi ügyeiről, valamint a firenzei belpolitikai, hatalmi harcokról és azokban játszott szerepéről lesz szó az 1290-1300 közötti évtized időszakában. Nem követek szigorú kronológiai rendet, hanem tematikusan tárgyalom a kérdéseket, hogy az összefüggések világosabbak legyenek (bár a klán-ügyek és a politikai harcok között is találhatunk összefüggéseket, melyekre utalni is fogok). Az előzőekben leírtak folytatásaként először néhány mondatban visszatérek Firenze és szövetségesei ghibellin-ellenes harcához, amelyekben Corso jelentős szerephez jutott, köszönhetően a campaldinói hőstettének. Miután 1289-ben és 1290-ben a Guelf Liga csapatai tisztogató hadműveleteket hajtottak végre Toszkánában, 1291-ben a pisaiak ellencsapásokat indítottak Guido da Montefeltro vezetésével, és egészen Empoli-hoz értek (amely néhány kilométerre van Firenzétől). A Comune ezért megtagadta az engedélyt Corsótól, hogy újra elvállalja Bologna podestaságát, mivel számított rá katonai parancsnokként a harcokban. Corso ennek megfelelően sienaiakkal és luccaiakkal megerősített serege élén Empolihoz nyomult, de a megfontolt Montefeltro ütközet nélkül visszavonult előle. Corso sikerének értékét az is növelte, hogy legfőbb politikai ellenfele, Vieri dei Cerchi 1292-ben súlyos kudarcot vallott Pontedera felmentése ügyében a ghibellinekkel szemben.

Ebben az időszakban barátkozott össze a ghibellin-ellenes harcokba bekapcsolódó üzletemberrel és katonai parancsnokkal, Geri Spinivel. Spini már 1274-től bankára és tanácsadója lett Benedetto Caetaninak, a későbbi VIII. Bonifác pápának, akinek révén azután a pápai udvarban az ottani magas rangú egyházi személyekkel is üzleti kapcsolatba került,

ami előnyt jelentett nemcsak neki, hanem a vele szövetséges Corsónak is. A kereskedelemmel, üzlettel és ipari tevékenységgel foglalkozó polgárok között szokás volt a korban helyetteseket vagy zsoldosokat állítani háborús időszakokban, de Geri Spini személyesen is részt vett a harcokban, 1292-ben a Comune és az Anjou-ház zászlóvivője volt, az egyik elitegység (a feditori) parancsnoka pedig Vanni dei Mozzi lett (családja szintén jelentős üzleti tevékenységet folytatott). Ebben az évben a guelfek Firenze vezetésével olyan jelentős haderőt állítottak ki (2 500 lovas és 8 000 gyalogos, szemben Montefeltro 800 lovasával és ismeretlen, de valószínűleg igen csekély számú gyalogosával), hogy komolyabb ghibellin támadásra már nem került sor. Corso mindeközben rendszeresen jelen volt a városi tanácsok ülésein, és tovább építette „külföldi" (vagyis más városállamokban realizálódó) karrierjét is, így podestà volt például 1294-ben Pármában, 1299-ben Orvietóban.

Miután 1280 táján Corso (valószínűleg apja, Simone Donati halála után) a Donati-klán feje, vezetője lett, pozíciójánál fogva minden házassági, vagyoni, gyámsági, vagy akár politikai ügyben érintett volt, és a szokásjognak megfelelően eljárhatott a Donati família ügyeiben. Így 1293-1294-ben több vitás ügye, pere is volt Firenzében, amelyek némileg rossz fényt vetettek rá, pedig ő csak a „hivatásának" megfelelően járt el (nem véletlen, hogy egyik fő szövetségesét, majd későbbi vetélytársát és ellenségét, Rosso della Tosát éppen a saját rokonai közül utálták a legtöbben, hiszen nemzetségi vezetőként minden családi ügybe beleszólása volt, és anyagi-örökségi ügyekben – úgy tűnik – mindenkit meg is rövidített a maga javára!). Mivel Corso egy kis közterületet a háza közelében (a Porta San Piero térségében) saját maga számára beépített és elfoglalt, a Comune kártalanításra kötelezte őt. 1294-ben távollétében (ekkor volt Parma podestája) pert indítottak ellene a rokonai vagyonának eltékozlása miatt, ugyanis a klánon belül a Corso dominálta csoport ellen Maso Donati vezetésével egy másik érdekcsoport alakult (a nagy létszámú klánoknál ez a megosztottság általános volt, és ezzel magyarázható például azon tény, hogy egyes családi csoportok guelfek, mások ghibellinek lettek, vagy ez tükröződött a fekete és fehér guelfek csoportjainak kialakulásában a guelf táboron belül). Ravenna nevű nővérének örökségi perét is újra indították Corso ellen, a testvére férjének, a Ferrante-családnak a tagjai, visszaköveteltek tőle földbirtokokat, házakat és egy Fiesole közelében lévő malmot is.

A legnagyobb visszhangja Corso családi ügyei közül (a későbbieket is bele számítva!) az unokatestvérével, Simone Galastrone Donatival való súlyos (örökséggel kapcsolatos) viszályának, konfliktusának volt a városban. Az ügyben tettlegességre is sor került, mivel Corso elküldte néhány emberét (egyesek, mint Machiavelli szerint maga Corso is részt vett az összecsapásban) Simonéhoz, akik őt megsebesítették, egyik szolgáját vagy katonáját (fante) pedig megölték. Az ügy természetesen a podestà elé került, aki kiadta azt az egyik bírájának, ő azonban ártatlannak hozta ki Corsót, unokatestvérét, Simonét viszont bűnösnek, így teljes vagyonelkobzásra és fővesztésre ítélte azt (az ítéletet végre is hajtották!). Bár Corsót is pénzbírsággal sújtották, és öt évre eltiltották tisztségek betöltésének lehetőségétől más városokban (így nem lehetett népkapitány vagy podestà), a köznép (popolo minuto) rendkívüli módon felháborodott, mivel az eljárás során az egyik jegyző meghamisította a vallomások jegyzőkönyvét (amiről a podestà valószínűleg nem tudott), és ez kitudódott a városban! Fegyveres lázadás tört ki és 1295 január 19-én a feldühödött tömeg megostromolta a bírósági palotát, és az ott talált iratok egy részét megsemmisítette, a podestà és a felesége is csak nehezen tudott elmenekülni. Ez az esemény az éppen ott tartózkodó Corsónak is igen kalandosra sikeredett, ugyanis fel kellett másznia a palota tetejére,

és onnan a szomszédos épületek tetőin átugrálva tudta csak elkerülni a lincselést. Mindezek után azonban meglepetésként hatott, hogy Corso teljesen győztesen került ki az ügyből, sőt politikai tőkét is tudott kovácsolni belőle, ugyanis legnagyobb politikai ellenfele, a Popolani vezére, Giano della Bella, aki nagyon népszerű politikus volt, megpróbálta megfékezni a feldühödött tömeget, amely ellene fordult, és maga is alig tudott elmenekülni a városból (ahová ugyanúgy, mint Dante, sohasem tért vissza!).

Még ugyanebben az évben újabb bonyodalom támadt, ugyanis első felesége (keresztnevét nem tudjuk, de a Cerchi családból származott) hirtelen bekövetkezett halála miatt a Cerchiek részéről az a gyanú támadt, hogy Corso esetleg megmérgezhette őt. E feltételezésnek nem sok alapja lehetett, hiszen a feleség kb. egy évvel az után halt meg, hogy fiú gyermeket szült Corsónak, ami a nemesemberek (de általában a férfiemberek) számára a legnagyobb örömet szokta jelenteni (ennek hiányában már inkább szoktak a férfiak agresszívak lenni, amit később VIII. Henrik angol király példája is bizonyítani fog), a gyanú tehát minden bizonnyal alaptalan volt, de Corso hírnevét ez sem öregbítette nagyon… De az sem, hogy a következő feleségét, Tessa degli Ubertinit az egyik legjelentősebb ghibellin családból választotta, akinek óriási hozománya (6 000 aranyforint) mindenképpen némi gyógyírt jelenthetett a hírnevében megtépázott Corso számára. Corsónak azonban meg kellett küzdenie az új feleségért és a hozományért egyaránt, a Cerchiek kérésére ugyanis VIII. Bonifác pápa megtiltotta a tervezett házasságot. Corso azonban nem csinált túl nagy gondot ebből (mint ahogyan VIII. Henrik sem), és a pápai tiltás ellenére mégis megtartották az esküvőt. Ezek után a pápa változtatott álláspontján, és utólag mégis engedélyezte a házasságot.

Néhány évvel később (1299-ben) Corso kártérítési pert indított az anyósa, Giovanna degli Ubertini ellen, mivel szerinte az rosszul kezelte a lánya birtokait, és eltüntette a birtokok pénzügyi iratait. Az ügyben eljáró podestà megítélt Corsónak 3 000, a feleségének 2 000 aranyat, amire egy népfelkelés tört ki Corso és a podestà ellen, az utóbbit bebörtönözték (később sikerült megszöknie), újra tárgyalták a pert, és Corsót 1 000 libra pénzbírságra ítélték. Mivel azonban ő ezt nem fizette ki, 1299 májusában száműzetésre ítélték, de szorult helyzetében VIII. Bonifác pápa a segítségére sietett: 1299 második felére Orvieto podestájává, 1300-ban pedig egy pápai tartomány, Massa Trabaria kormányzójává (rector) nevezte ki Corsót. A Comune a következő évben ráadásul egy újabb elmarasztaló ítéletet hozott Corso ellen egyéb örökségi szerzeményei ügyében is, mégpedig egy 1300. március elsején elfogadott törvény alapján, tehát visszamenőleges hatállyal. Mindez azonban már a belpolitikai harcok következménye volt, Corsón a Popolanihoz tartozó ellenfelei akartak bosszút állni túlzott befolyása miatt, így e lépésnek nem sok köze volt a korrekt igazságszolgáltatáshoz (korábban persze Corso is igyekezett minden módon maga felé hajlítani az ügyeiben eljáró bírákat…).

Az 1280-90-es években Corso Donati fokozatosan a Magnati, a születési-katonai nemesség érdekeit képviselő politikai csoport elismert vezérévé vált. Sestan utal egy 1284-ben szervezett arisztokrata hatalom átvételi kísérletre, amelyet Corso vezetett, és amelyet a túlerőben levő popolani fegyveresek végül meghiúsítottak. Antonetti állítása szerint a guelf vezér sohasem fogadta el azon törekvést, hogy Firenzét a kereskedők és iparosok, kézművesek irányítsák, nem fogadta el őket egyenrangúként. Corso álláspontja szerint a várost ellenségeivel szemben mindig a katonai nemesség védte meg, így volt ez a döntő jelentőségű campaldinói csatában is. A Comune már korábban is igyekezett rendszabályokat hozni a nemesekkel szemben, mivel közülük többen visszaéltek státuszbeli fölényükkel és azzal,

hogy rangjuknak megfelelően fegyvert viselhettek. Az 1293-ban elfogadott Ordinamenti di Giustizia (az Igazság Rendeletei) rendkívül markánsan fogalmazta meg a nemesek megrendszabályozására való törekvést a városban. Az új rendelkezések megalkotása időszakában (1293 január-április) kihasználták azon helyzeti előnyüket a popolani képviselői, hogy Corso ez év első felében távol volt Firenzétől, mivel Parma podestájává nevezték ki. A Comune létre hozott egy új, büntető, kényszerítő erővel rendelkező, rendőri jellegű tisztséget: a gonfaloniere di giustiziát (az igazság zászlóvivője). A gonfaloniere fő feladata az volt, hogy ha egy bírói döntésnek vagy más rendelkezésnek valamelyik nemes ellenáll, akkor a rendelkezésére mozgósított milícia (1 000 fő) segítségével katonai erővel kikényszerítse a jog érvényesítését (E hivatal második betöltője Dino Compagni, a híres történetíró volt, akinek vezetésével lerombolták a Galligai család városbeli házát, mert nem állították bíróság elé egy gyilkossággal vádolt, külföldön tartózkodó tagjukat. A klán vezetője ugyanis ekkoriban annak összes tagjáért büntetőjogi felelősséggel tartozott!). Még nagyobb csapás volt azonban a nemességre az a döntés, hogy 140 családot kizártak a városi hivatalok viselésének jogából, közöttük természetesen a Donatiakat is!

Az Ordinamenti rendelkezései súlyosan sértették a nemesség érdekeit és presztízsét, így nem véletlen, hogy amikor a fekete guelfek hatalomra kerültek, 1304-ben az összes jogszabály megszüntetésében gondolkodtak, és csak a nemesi klánok közötti ellentétek, a hatalmon lévők megosztottsága miatt nem került erre sor. Max Weber meglátása szerint az Ordinamenti annak alapján válogatta ki a kizárandó nemesi családokat, hogy kik folytattak a lovagi-nemesi szokásoknak megfelelő életvitelt, életmódot Firenzében. Weber a kérdés elemzése során kimutatja, hogy az Ordinamenti a perrendtartási rendelkezésekben egyoldalúan a polgároknak kedvezett a nemesekkel szemben, kirekesztették a nemeseket a városi hivatalokból és a közigazgatásból, a gonfaloniere tisztségével egy különleges végrehajtó, rendőri erőt hoztak létre a nemesek ellen, egy személy bűnéért az egész nemzetséget büntették, bátorították a besúgásokat és a feljelentéseket, összességében tehát súlyosan diszkriminálták a nemességet. A tisztségekből kizárt nemesi famíliák körülbelül fele a vidéken (contado) élt, a másik fele, konkrétan 72 család pedig Firenzében. Átnézve a Stahl által az utóbbiakról közzé tett teljes listát, nem csodálkozhatunk, hogy a maga egészében e rendeletet nem lehetett hosszú ideig érvényben tartani! Csak a Porta San Piero Maggiore kerületet nézve (amelyhez az Alighierik is tartoztak) olyan nevekkel találkozunk, mint az Adimari, Abbati, Cerchi, Pazzi, Visdomini és a Donati nemzetségek, amelyekről túlzás nélkül állítható, hogy a leghatalmasabb, leggazdagabb és legbefolyásosabb firenzei klánok közé tartoztak. Mindezek miatt 1295-ben egy jelentős módosítást hajtottak végre a nemesség kizárásával kapcsolatban: azon személyek, akik hajlandóak voltak beiratkozni valamelyik céh regiszterébe, részt vehettek a város kormányzásában és betölthettek tisztségeket, függetlenül attól, hogy a céhes mesterséget, foglalkozást valóban gyakorolták-e (így vehetett részt a városi tanácsokban és a tisztségekben Dante Alighieri is, aki az orvosok és gyógyszerészek céhébe iratkozott be!). A Parmából visszatérő Corsót tehát a Comune kész helyzet elé állította, de hamarosan világossá vált, hogy a „báró" (il Barone, ahogyan a kortársak nevezték őt) hosszabb távon nem fog belenyugodni a születési-katonai nemesség jogfosztásába (a céhekbe nem volt hajlandó belépni), és a felháborodott magnatiak benne bíztak leginkább vezetőként az elkövetkezendő harcokban, az olyan elszánt „ellenállók", mint Forese degli Adimari, Vanni dei Mozzi és Geri Spini mellett.

## FELHASZNÁLT IRODALOM

[1] P. Antonetti, *La vita quotidiana a Firenze ai tempi di Dante*, Milano, Rizzoli, 1992.
[2] W. Bowsky, *Henry VII in Italy*, Lincoln, Nebraska, University of Nebraska Press, 1960.
[3] R. Davidsohn, *Geschichte von Florenz, Zweiter Band: Guelfen und Ghibellinen. Zweiter Theil: Die Guelfenherrschaft und der Sieg des Volkes, Vol. II/*2. Berlin, Mittler und Sohn, 1901.
*[4]* R. Davidsohn, *Geschichte von Florenz. Die letzten Kämpfe gegen die Reichsgewalt, Dritter Band, Vol. III*, Osnabrück, Biblio Verlag, 1969.
[5] I. Del Lungo, Ed., *Dino Compagni e la sua Cronica*, Firenze, Successori Le Monnier, Vols. I-III, 1879-1887. Vol. I/2. 1880., Vol. II. 1879.
[6] *Dizionario Biografico degli Italiani, Vol. 41*. 1992, pp. 18-24. /S. Raveggi, Donati, Corso/
[7] *Enciclopedia dantesca, Vol. II*. 1970, pp. 558-560. /E. Sestan, Donati, Corso/
[8] J. Favier, *Philippe le Bel*, Paris, Fayard, 1998. /édition revue, 1978/
[9] J. Heers, *Le Clan familial au Moyen Âge*, Paris, P.U.F., 1993(1974).
[10] G. Holmes „Dante and the Popes" in *The World of Dante*, C. Grayson, Ed. Oxford, Clarendon, 1980, pp. 18-43.
[11] *Niccolò Machiavelli Művei, Vols. I-II.*, Budapest, Európa, 1978. Vol. II./Firenze története, ford. Iványi Norbert, pp. 5-410/
[12] H. L. Oerter, *The Florence of Corso Donati*, University of Colorado, Ph. D., 1965. /University Microfilms, Inc., Ann Arbor, Michigan/
[13] H. L. Oerter, „Campaldino, 1289", *Speculum*, vol. 43. 1968. n. 3. pp. 429-450.
[14] M. Scardigli, *Le battaglie dei cavalieri*. *L'arte della guerra nell'Italia medievale*, Milano, Mondadori, 2012.
[15] E. Sestan, *Italia medievale*, Napoli, 1968.
[16] B. Stahl, *Adel und Volk im Florentiner Dugento*, Köln-Graz, Böhlau Verlag, 1965.
[17] M. Weber, *Állam, politika, tudomány,* Budapest, KJK, 1970.

### Források

Cronica fiorentina compilata nel secolo XIII, in *Testi fiorentini del Dugento e dei primi del Trecento*, A Schiaffini, Ed. Firenze, Sansoni, 1954, pp. 82-150.
*Dante Alighieri Összes Művei (DAÖM*), T. Kardos, Ed. Budapest, Helikon, 1965.
*Dino Compagni Krónikája korának eseményeiről*, A. Kiss, Ed. and Transl. Bucuresti, Kriterion, 1989.
Giovanni Villani, *Istorie Fiorentine Fino all'anno 1348, Vol. I-VII*, Milano, Soc. Tip. de Classici Italiani, 1802-1803. Vols. III-IV. 1802.
Giovanni Villani, *Cronica. Con le continuazioni di Matteo e Filippo*, G. Aquilecchia, Ed. Torino, Einaudi, 1979.

# NATO – THE STEPS OF ADAPTATION | NATO - AZ ADAPTÁCIÓ LÉPCSŐFOKAI

KARTALI Gabriella[1] – SEPRÉNYI Patrik[2]

**Abstract**

The rapid recognition and analysis of changes in the international environment and the development of res-ponses to the resulting challenges, the implementation of the appropriate adaptation process, is such an important act for NATO that failure or delay would lead to question the organization's raison d'être. Therefore, NATO periodically reviews its own strategic directions, analyzes and evaluates the changes in the security environment, and then, it renews or replaces its strategic directions, and designates the operational framework of the Alliance for the coming period, if necessary. In the last decade, many new challanges have appeared on NATO's horizon to which the organization had not previously paid sufficient attention, therefore nowadays, the Alliance is taking another step on the path of adaptation with its 8th strategic concept.

**Keywords**

International security, NATO, strategic concept, new challenges, adaptation, Russia, China

**Absztrakt**

A nemzetközi térben beállt változások gyors felismerése, elemzése és ezek következtében megjelenő kihívásokra adott válaszlépések kidolgozása, a megfelelő adaptációs folyamat lefolytatása olyan jelentőségű mozzanat a NATO esetében, melynek elmulasztása vagy halogatása a szervezet létjogosultságának, megkérdőjelezéséhez vezetne. Ezért a NATO időről-időre felülvizsgálja saját stratégiai irányait, elemzi és értékeli a biztonsági környezetben beállt változásokat, és amennyiben szükséges, megújítja vagy lecseréli stratégiai irányvonalait, és kijelöli a Szövetség működési kereteit az elkövetkezendő időszakra. Az elmúlt évtizedben számos olyan kihívás jelent meg a NATO horizontján, melyekre korábban nem fordított elegendő figyelmet és amelyek következtében a NATO jelenleg ismét az adaptáció újabb lépcsőfokán áll a 8. stratégiai koncepciójával.

**Kulcsszavak**

Nemzetközi biztonság, NATO, stratégiai koncepció, új kihívások, adaptáció, Oroszország, Kína

[1] kartali.gabriella@uni-obuda.hu | ORCID: 0009-0000-2957-8269 | PhD student, Óbuda University
Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] patrik.seprenyi@gmail.com | ORCID: 0000-0003-1223-4245 | PhD Student, Doctoral School of Military Sciences, University of Public Service | PhD Hallgató, Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola

## INTRODUCTION

"The history of mankind is the history of war"[1] The saying attributed to the former Prime Minister of the United Kingdom, Winston Churchill, is unfortunately still a useful quote today, since after his death on January 24, 1965, many wars broke out that Churchill could no longer live through, such as the Soviet Union's war in Afghanistan, the wars in Iraq , the Yugoslavic wars, the African wars of the 1990s and 2000s, which in total claimed millions of victims, the war on terrorism, the consequences of the Arab Spring, and the currently most watched Russian-Ukrainian war, which Russia refers to as a special military operation.[2]

Therefore, despite the fact that the European continent has been relatively peaceful, i.e. mostly free of classical conventional war, for nearly 80 years since the end of the Second World War, it does not mean that this phenomenon has disappeared from the world, and above all, it does not mean that this type of threat may not occur again for European states in the future. And as a colletcive defence organization, the main task of the North Atlantic Treaty Organization (NATO), is precisely to prevent and deter international actors outside the organization from the idea of a possible external armed attack and to protect the security of its member states, the freedom of their peoples, democracy and the rule of law within the organization.[3]

Since the end of the Cold War and the disintegration of the Soviet Union, as the organization was left without an enemy, NATO increasingly shifted from direct collective defence tasks to crisis management and stability projecting tasks. This is also reflected in the organization's previous, 2010 strategic concept, which describes in the chapter "Basic tasks and principles"[4] that although collective defence remains a priority task, a conventional attack against NATO member countries is highly unlikely. At the same time, the events of the 2010s and the war that broke out in February 2022 highlighted that the resolutions of that strategic concept must be reviewed and updated in several respects, and that the collective defence nature of the organization along with the unity of the member states may be more important, than at any time in the last three decades. As a result, the eighth strategic concept, which the member states adopted at the 2022 summit in Madrid, puts the emphasis back on collective defense. [5]

## ADAPTATION PROCESSES IN THE ORGANIZATION

### NATO's role in the world

In order to understand why it is extremely important to talk about the need for NATO's further development, it is worth devoting a few sentences to illustrate the importance of the organization and its role in the international environment.

NATO was established on April 4, 1949 with the signing of the organization's foundation document, the 14-article North Atlantic Treaty, also known as the Washington Treaty. The organization, which had only 12 member states at the time, now includes 30 countries, and Finland and Sweden, by giving up their independent status and submitting their membership applications, opened up the possibility for NATO to expand to a 32-member organization in a short time, although Turkey gave a clear signal that it would not participate to support the accession of the two candidate countries, which represents a serious obstacle,

since accession can only take place with the unanimous decision and consensus of the NATO member states. [6]

The creation of NATO was primarily induced by the prevention of another large-scale, extensive war in Europe, the Western European fear of the restrengthening of Germany, and the opposition to the Soviet Union. [7]

After the Second World War, the Soviet Union and the West became increasingly estranged from each other, one of the important moments of this is, for example, Winston Churchill's Fulton speech on March 5, 1946 about the lowering of the Iron Curtain [8] that divided Europe into Western and Eastern parts or the foreign policy guideline drawn up by Harry S. Truman, the President of the United States in 1947, according to which the United States does not tolerate violent changes to the status quo on the one hand, and on the other hand provides assistance to countries where communism is at risk of gaining ground.[9]

The gradual alienation and the long-term security needs of the Western European states finally, shortly after the 1948 Treaty of Brussels and the Vandenberg Resolution [10] led to the establishment of NATO, the goals of which the organization's first secretary, Lord Hastings Lionel Ismay, stated that the purpose of NATO is nothing more than to "keep the Soviet Union out, the Americans in, and the Germans down." [11]

NATO was thus created as a defence organization that prevents wars, and is able to counterbalance the Soviet Union and later the Warsaw Pact, and as an organization which can exercise its collective self-defence rights, (written in Article 5 of the Washington Treaty [12] -, based on Article 51 of the United Nations Charter on legitimate individual and collective self-defence) [13], NATO member states, in the sense of collective (self) defence, agree that an armed attack against one or more of them, in Europe or North America, will be considered as an attack against all of them, and in this way they will help each other to restore peace and security in the Euro-Atlantic region. [14]

The main honour of NATO, which determines its role in the international environment, is that it connects North America with Europe, which creates a strong Euro-Atlantic defence cooperation that is complemented by many partner countries (for example, Japan or Australia among the global partners), with whom, in the spirit of cooperative security, the organization works together to overcome several different challenges occurring in the security environment.[15]

Nevertheless, NATO's goals and tasks have expanded significantly over the past seven decades, for example with crisis management tasks, handling problems that go beyond the borders of the organization but directly or indirectly affecting the member states, as well as a broader interpretation of security that goes beyond the military dimension, therefore it is no exaggeration to say that the history of NATO is actually a history of continuous adaptation to a dynamically changing security environment. This continuous adaptation however helped the organization to successfully survive different crisis periods and was able to maintain its raison d'etre in situations such as the beginning of the nineties, when with the dissolution of the Soviet Union, the NATO was practically left without enemies.

In my opinion, one of the famous comparisons of the ancient Chinese philosopher and general, Sun Tzu, can be paralleled with NATO's adaptation processes, according to which the shape of the army (and there, the shape of the NATO) should be likened to water: it should always be flexible and have the ability to adapt to unexpected situations. [16]

With similar flexibility, NATO tries to continuously adapt to the changing security environment, in which the strategic concepts serving as a strategic compass play a key element.

**NATO's strategic concepts**

NATO's strategic concepts are the clearest impressions of the organization's adaptation steps. From such a concept, together with the 2022 concept, which is currently in force, a total of eight pieces were created during the history of NATO, four of which were created during the Cold War (1949-50, 1952, 1957, 1967), three in the post-bipolar era (1991, 1999, 2010) [17] and I separate the new, 2022 concept from the previous ones because it may indicate a new, so called multipolar era, which term is frquently used nowadays not only by the security policy experts, but also by governments too. A good example for that is the Shanghai Cooperation Organisation (SCO) whose member states, China, Russia, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, India and Pakistan reaffirmed their commitment to new multipolar world order. [18]

The strategic concepts, as I mentioned earlier, serve as a kind of strategic compass for the organization, which analyzes the characteristics and challenges of the current security environment, determines the organization's nature and tasks and the longer-term goals which are valid for about a decade in advance, It also provides guidelines regarding the organization and the application of forces, on the basis of which the various capacity development plans of the organization can be compiled. Concepts are therefore extremely important documents, and it is no coincidence that the four concepts adopted during the Cold War, together with their supplementary documents, were not made public for a long time. Today, however, they are also available on the Internet, and by comparing the concepts, NATO's direction of its development can be well visualised.

**Concepts of the Cold War**

The concepts of the Cold War placed an extremely high emphasis on the nuclear deterrence, which is still a main pillar of the organization to this day, however during the Cold War period, these capabilities (the nuclear triad – strategic bomber aircraft, land-based missiles, ballistis missile submarines) were given a much stronger role.[19] The first and second strategic concepts (1949, 1952), for example, between which documents only a little bit more than two years have passed, explain in detail the way of carrying out strategic bombings and the importance of supporting them with all means. Interestingly, although the United States provided the main defense umbrella for Europe, the two documents placed great emphasis on the ground forces of European countries whose main task was to hold the enemy forces until the Alliance's reinforcements arrive. [20]

Earlier it was stated that a strategic concept plans a decade in advance, here on the other hand, it is seen that a new concept was adopted in just a couple of years. The brevity of the period between the first two concepts can be justified by significant changes affecting the organization, which required updating the concept that had just been created. Such changes were the accession of Greece and Turkey in 1952, the establishment of the integrated military command system, the appointment of the first Supreme Allied Commander Europe (SACEUR) in the person of General Dwight D. Eisenhower (the 34th president of the United States, 1953-1961) [21], the start of infrastructural developments, and a not negligible event, the outbreak of the Korean War. This shows perfectly, how the NATO could react

and adopt to the dynamically changing security environment and today, the organization is trying to keep this ability as functioning as it was always.

Not so long after the second strategic concept (1952), which was similar in content to the first document, the third strategic concept was adopted in 1957, which is usually called the concept of mass retaliation, which comes from the Eisenhower administration.[22] This concept has already openly stated the primary role of weapons of mass destruction in NATO's strategy, which meant that the organization must be able to survive the attacks of a state or states acting as an aggressor against it, and then with all available means, including weapons of mass destruction, to retaliate in the most destructive way.[23]

Such a high degree of reliance on nuclear weapons can also be attributed to the fact that, in terms of conventional forces, NATO never had any deterrent power, which can successfully scare away a possible soviet aggression and also, the organization would never have been capable of larger-scale offensive operations guaranteeing success, which also proves, that NATO is not an offensive, but a defensive organization which can also be read in the North Atlantic Treaty.[24]

As a result of the increase in the Soviet Union's nuclear capability however, the concept of mass retaliation had a strong negative impact already in 1957, because the security policy experts, military officers, generals, diplomats, politicians all realized that this way of thinking would lead to mutual assured destruction (MAD), which almost really happened in 1962 during the Cuban Missile Crisis and therefore the NATO member states had to find a new approach.[25]

It only took a few years after the Crisis, for a new concept to emerge, which document abolished the principle of mass retaliation and changed the orientation tot he principle known as flexible response. In 1968, the concept of Flexible Response, which strikes a lighter tone, was accepted as a result of Pierre Harmel, Belgian foreign minister's 1967 report which emphasized the role of political communication, and as he wrote, in addition to maintain the deterrent capability, it is also important to devote space to the political dimension. [26] The strategy of the organization had been softened with regard to nuclear weapons, because instead of the previous immediate retaliation with weapons of mass destruction, a multi-stage reaction principle had come into focus, the essence of which is that the enemy considering an attack against the organization cannot calculate the level of the expected escalation of the conflict that breaks out. The organization could respond with forces of the same size, with forces larger than the size of the attacking forces, or with nuclear weapons.[27] The concept can be said to be successful, so it is no coincidence that after adopting this concept, it is replaced only by the first post-Cold War strategic concept (1991), which is also the first public concept.

Summarizing the years of the Cold War, eighteen after its birth, NATO came to the point where it recognized the importance of political communication in addition to military factors, which meant that the Alliance’s portfolio began to expand and deepen. Although, the nuclear deterrence and the collective defense remained the dominant factors throughout the Cold War, the softer tools started to come to the surface. It is quite interesting though, that the Soviet Union considered the changes of NATO's strategic directions as a success of its own deterrent capabilites.

## Concepts of the post-bipolar age

The end of the Cold War appeared as a serious crisis for NATO, since with the end of hostilities, the organization practically lost its „raison d'être" (right to exist), as a result of which the necessity of its existence was questioned and if the Alliance wanted to remain relevant, it had to find its new identity in the new era.

However, NATO remained true to its excellent adaptation capabilities and managed to find its place and role after the Cold War, which role was nothing more than the preservation and the projection of stability, since the new world order seemed to bring instability, especially in Eastern and South-Eastern Europe. In Eastern Europe, countries like the Baltic states, Poland, Hungary etc. turned towards Euro-Atlantic integration which required NATO and EU to revise their approaches to the region(s).[28]

Besides the integration processes, a series of ethnic conflicts broke out in the Balkan region which led to mass killing amond ethnic Serbians, Croatians, Bosnian Muslims, and Kosovo Albanians as Yugoslavia broke apart step by step. Since the conflitcs could have a major impact on the European economy and stability, the region attracted the NATO's attention too and to this day, maintaining the fragile stability of the region is a priority for the organization.[29]

After the realization of the unstable and fragile environment, the projection of stability became one of the main tasks of NATO which helped the organization to find its new identity. Later on in the nineties, it became more clear, that crisis management and the „out of area" (beyond NATO's „borders") operations were now among the Alliance's core tasks, as it is written in the 1999 Strategic Concept.[30] The projection of stability appears as a task that is still decisive to this day, and which also induced the creation of such partnerships as, for example, the Partnership for Peace (PfP), the Mediterranean Dialogue or the Istanbul Cooperation Initiative.

Besides the projection of stability, the European continent was also extremely important to the United States because of the further maintenance of good transatlantic relations, disarmament and arms limitation processes and military cooperation.[31]

In conclusion, NATO's predictions about the importance of the role of out of area operations, crisis management, and stability projection turned out to be true and the NATO successfully found its role in the new world order and based on the experiences of the decade and the integration processes of the Eastern countries that wanted to join the organization, the strategic concept of 1999 was adopted, which concept placed great emphasis on the threats of religious-ethnic conflicts, on cooperation with partner countries, and on the progress of European integration processes, so on the experiences of the nineties.[32]

The only problem with the concept was that it did not take sufficient account of problems such as terrorism, which later will receive sufficient attention, but only after the disastrous terrorist attacks in New York in 2001.

We have therefore arrived at the strategic concept that was in effect untin 2022, which was adopted by the organization in 2010. The concept with the subtitle "Active role, Modern defence" presents the challenges affecting the organization in a very extensive interpretation of security, which thus greatly contributes to the expansion of NATO's world view and tasks. This concept shows terrorism as an extremely important challenge, the challenges of information operations in cyberspace, and also shows several different challenges

in the field of human security, such as climate change or energy security. The important role of civil-military cooperation during crisis management is also shown.[33]

This brings us to the most important point of the study, namely to examine what new challenges have appeared since 2010, which NATO has to face both now and in the future, and which made the 2010 concept outdated. The next chapter therefore focuses on new types of challenges from NATO's point of view.

## NEW CHALLENGES

### Hybrid and cyber threats

One of the most important challenges, which more and more relevant in the 2010s, are the threats appearing in cyberspace, which are closely related to another, equally challenging phenomenon, hybrid threats. Basically, both the amazingly fast pace of technological development and the globalization process contributes to the growth of the role of both phenomena, since the technological development has resulted in a closer connection of the countries of the world, strengthening the interdependence. Nowadays, the key social systems and activities are organized around electronic information networks, which are exceptionally vulnerable. Reliance on information networks and exposure to the Internet serve as just the right basis for modern information warfare and the aforementioned hybrid threats or warfare.[34]

Hybrid warfare is a controversial concept, the development of which is linked to Valery Gerasimov, the Russian military leader, and the annexation of the Crimean Peninsula in 2014, although Gerasimov did not use the term hybrid warfare in the article he wrote, it was rather spread among experts from Western countries away.[35]

The essence of this form of warfare is the combined use of soft, medium and hard tools of traditional and irregular warfare elements, as well as a form of interest enforcement where the interest of the attacker is to keep the given conflict below the threshold value and to avoid escalation, i.e. to keep the conflict in the gray zone.[36]

A common example of this type of conflict is the South China Sea dispute, where the parties involved, such as the People's Republic of China, Taiwan, and even the United States, try to force the opposing party to back down with frequent cyber attacks, demonstrations of naval power, and diplomatic tools, for example Nancy Pelosi’s, the speaker of the U.S. House of Representatives, visit to Taiwan (Republic of China) on August 2, 2022. This event stirred up a lot of dust and The People’s Republic of China reacted aggressively. In the period following the visit, the People’s Liberation Army launched ballistic missiles, conducted combined maneuvers in airspace and waters surrounding Taiwan. [37] China even released a white paper on Taiwan question which focuses on the future reunification in the new era.[38]

One of the key elements of these hybrid threats is cyberspace, which provides space for various information operations and which was declared an operational area by NATO at the 2016 NATO summit in Warsaw.[39]

Cyberspace, which means the totality of information systems and the information flowing through them, creates a perfect opportunity to carry out hybrid operations. On the one hand, the information and disinformation operations launched here are capable of disrupting internally the target country's society, turning it against the government, and driving

it into a panic, for example through fake news, which weakens the internal stability of the given country or organization, and on the other hand, such a serious attack can be launched in the information space, for example, against critical infrastructures, as a result of which entire countries and groups of countries can be paralyzed, for example in terms of energy supply or telecommunications equipment, and even the IT systems of the armed forces can be disabled through cyberspace, which can thus make a country vulnerable to a possible armed attack from the outside.[40]

Overall, therefore, in relation to hybrid and cyber threats, these challenges are challenges that NATO should pay particular attention to and as it is clear now, the Alliance is definitely trying to improve its capabilites to maintain security and stability.

**NATO-Russia relations**

The 2010 strategic concept in relation to Russia speaks of a strategic partnership, the need to strengthen cooperation, but also about the troubled relations. Based on the document, the Alliance does not mean a threat to Russia, but at the same time, an important NATO principle also found in the text, according to which any European democracy that shares the Alliance's values can join the Alliance, results in a serious conflict of interests between NATO and Russia, since, as the Russian President Vladimir Putin also stated in his speech on February 21, 2022, that the expansion of the Alliance towards the East presents itself as a security threat on Russia's side. [41]

After the outbreak of the Russian-Ukrainian war, China also stated that NATO countries should have thought before pushing a large country like Russia to the wall. At the same time however, calling the invasion as preventive self-defence is at least as unacceptable on the part of Russia in connection with the attack of Ukraine, as it was not acceptable in the case of the United States' war in Iraq.

According to international law, violence may only be used in individual or collective self-defense, in case of the occurrence of an armed attack or the authorization of the UN Security Council.[42] Russia was not hit by an armed attack, and the areas it wants to defend (Donetsk and Luhansk) are not recognized states, so the reference to the right of individual or collective self-defense is not valid. The authorization of the UN Security Council (SC) could possibly have arisen if Russia turned to the SC with accusations of genocide and after the investigation it decides on the possible necessary non-armed or armed regulations, but Russia did not turn to the SC, so overall the Russian intervention is nothing more than illegal intervention in the internal affairs of another state, or aggression. [43]

The annexation of the Crimean Peninsula in 2014 and the invasion since February 2022 resulted in a very serious deterioration in the relationship between NATO and Russia. Since 2014, the organization has suspended all serious civil and military cooperation with Russia, deeply condemned the Russian aggression in 2022 and expressed its solidarity with Ukraine, athough the diplomatic channels are maintained with Russia in order to find a constructive solution to the situation. The attitude towards Russia is clearly one of, if not the most decisive issue to which NATO must concentrate on in the upcoming times.[44]

**The Rise of China**

In addition to the Russian threat, a new challenger appeared, especially in the 2010s, which is most relevant from the point of view of the United States, since the two states are

competing for the leading position in the world economy, and the United States is trying to assert its interests within the framework of NATO too.

Since the Second World War, the United States has practically been the protective umbrella for Europe to keep threats at bay, and in this way it is not surprising if the strategic interests of the States also appear at European negotiating tables. According tot he interests, while the goal of the United States is to maintain the post-Cold War unipolar world order and its own hegemony, China's goal is to restore the country's pre-19th century greatness and at the same time emphasize the multipolar world order.[45]

Today, as a result of the Reform and Opening up policy initiated by Deng Xiaoping in 1978, the People's Republic of China has undergone enormous economic, military and technological development. China's GDP increased more than seventy times in 40 years, from USD 200 billion to USD 17,500.[46] Nowadays, China is often called as the workshop of the world, but at the same time, it is important to take into account that as a result of the many resources invested in research and development, China is already capable of producing high-tech products independently. The large-scale economic development was noticed by other states, including the United States, so it is no coincidence that in the early 2000s, the so-called Chinese threat theory appeared, according to which China pursues a world-conquering policy, the aim of which is to extend its own influence and power to as many parts of the world as possible, for example, with the tools of debt trap diplomacy.[47]

The Belt and Road Initiative, launched by President Xi Jinping in 2013 is most often associated with this theory, which is a huge-scale infrastructural investment and development program designed to build connections between Europe, Africa and Asia and asa result, to disconnent the European continent from the American continent economically, therefore it is not surprising that at the 2019 NATO summit in London the relationship with China was referred to as opportunities and challenges. The report prepared by the group NATO 2030: United for a New Era 2020 led by NATO Secretary General Jens Stoltenberg clearly characterizes it as a threat to democratic states.[48]

## NATO'S RESPONSES TO THE CHALLENGES - CONCLUSION

In the decade following the 2010 strategic concept, the most visible change in NATO's operation is the gradual strengthening of the collective defense nature, as well as the gradual deterioration of the dynamically changing international security environment in general. The annexation of Crimea in 2014 was a key element in these changes, which significantly increased the sense of threat in Europe, as a result of which the NATO summit in Wales in 2014 redirected the organization towards the tasks according to Article 5 of the Washington Treaty. Accordingly, NATO returned to regular military exercises, the cooperation of special operations forces and the federal level coordination of intelligence and surveillance came to fore. The Alliance also adopted the Readiness Action Plan (RAP), which focuses on the defense of the Alliance's eastern borders and which includes the installation of military equipment and bases.

As part of the plan, the number of NATO Response Forces was increased from 13,000 to 40,000 people (now the goal is to reach 300 000) [49], and a very rapid response force group of 4,000 people was also created. Last but not least, the power of Article 5 was extended to cyber defense, and the member states accepted the recommendation of a 2% approach to defense expenditure in proportion to GDP. [50]

At the next summit, in 2016, in Warsaw, the strengthening of collective defense continued and NATO deployed four battalion battle groups (4,000 people) in the territory of Poland and the Baltic States with a "forward rotational presence" and declared cyberspace as an operational area, and at the same time the Very Rapid Reaction Combined Forces were also increased to 15,000. Since 2016, unity and cooperation between member states has also become increasingly important, since it is difficult to react effectively to any threat without a unified collective action. An important element of this was the establishment of the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) in 2017, which is a result of NATO-EU cooperation and which institution's task is to analyse the incoming cyber attacks from Russia and the disinformation operations, as well as the development of common and effective responses to challenges.[51]

Last but not least, this article has arrived to reflect to the NATO Strategic Concept 2022, which can be seen as a result of the last deacede and an organized collection of the emerged threats and the possible reactions to them. The document states, that Euro-Atlantic security is undermined by instability and strategic competition, where the Russian's Federation war of aggression against Ukraine is the most threatening event, because it shatters the peace of the continent. Despite the fact, that Russia's actions are condemned, in the concept NATO states, that the organization does not seek the confrontation with Russia and is ready to talk to prevent escalation.[52] According to the escalation, though NATO collectively does not take part in the conflict, the members of the organization separately help Ukraine with humanitarian aid, armored vehicles, anti-tank weapons, ammuniton, mobile multiple rocket launcher systems and even main battle tanks, and as a result it is not surprising that the Russian and Chinese news are talking about a war between Russia and NATO.

According to the People's Republic od China (PRC) and the hybrid threats, they also appear in the new strategic document and in additon, these two challanges are strongly connected, since the concept refers to the hybrid and cyber threats as issues which also come from the direction of the PRC which is trying to expand its influence around the world and is trying to subvert the rules-based international order.[53]

Therefore, based on the trends of the 2010s and the 2022 Strategic Concept, NATO is increasingly returning to the collective defense needs that led to the creation of the organization, while at the same time it is trying to properly adapt to other new serious challenges, such as hybrid and cyber threats, energy security and security of supply, economic and technological competition with China, threats from Russia, and ever-increasing challenges such as pandemics and climate change. It should also be noted that NATO no longer concentrates only on defense, but it emphasizes the significance of the deterrence too.[54]

In conclusion, NATO is not in an easy situation since the security environment is constantly changing and it seems that the next decade will be tougher than the three decades after the dissoluiton of the Soviet Union and maybe even tougher than the Cold War.

## BIBLIOGRAPHY


[1] M. Ashley, “Churchill and History”, International Affairs, vol. 42, no. 1, pp. 89, 1966.
[2] President of the Russian Federation, “Address by the President of the Russian Federation,” The Kremlin, Moscow, Feb. 24, 2022. Available: http://en.kremlin.ru/events/president/news/67843. (Accessed Feb. 1, 2023).
[3] North Atlantic Treaty Organization, “The North Atlantic Treaty,” Washington, D.C., Apr. 4, 1949. Available: https://www.nato.int/cps/en/natolive/official_texts_17120.htm. (Accessed Feb. 21, 2023).
[4] North Atlantic Treaty Organization, “The Alliance’s Strategic Concept, 2010,” Available: https://www.nato.int/cps/en/natohq/topics_82705.htm. (Accessed Feb. 21, 2023).
[5] North Atlantic Treaty Organization, “NATO 2022 Strategic Concept,” Available: https://www.nato.int/strategic-concept/. (Accessed Feb. 21, 2023).
[6] Reuters, “Explainer: Why is Turkey blocking Sweden and Finland NATO membership?”, Available: https://www.reuters.com/world/why-is-turkey-blocking-swedish-finnish-nato-membership-2023-01-25/. (Accessed Feb. 16, 2023).
[7] North Atlantic Treaty Organization, “Why was NATO founded?”, Available: https://www.nato.int/wearenato/why-was-nato-founded.html. (Accessed Feb. 16, 2023).
[8] Winston Churchill, “Churchill’s Iron Curtain Speech”, Available: https://winstonchurchill.org/resources/speeches/1946-1963-elder-statesman/the-sinews-of-peace/. (Accessed Feb. 16, 2023).
[9] H. S. Truman, “Truman Doctrine,” Mar. 12, 1947. Available: https://avalon.law.yale.edu/20th_century/trudoc.asp. (Accessed Feb. 17, 2023).
[10] U.S. Senate, “Vandenberg resolution. U.S. Senate Resolution 239. 80th Congress, 2nd Session, 11th June 1948 (The Vandenberg Resolution)”, Available: https://www.nato.int/ebookshop/video/declassified/doc_files/Vandenberg%20resolution.pdf. (Accessed Feb. 17, 2023).
[11] North Atlantic Treaty Organization, “Origins: NATO Leaders”, Available: https://www.nato.int/cps/us/natohq/declassified_137930.htm. (Accessed Feb. 17, 2023).
[12] North Atlantic Treaty Organization, “The North Atlantic Treaty”, Washington, D.C., Apr. 4, 1949. Available: https://www.nato.int/cps/en/natohq/official_texts_17120.htm. (Accessed Feb. 21, 2023).
[13] United Nations, “Charter of the United Nations”, 1945.
[14] The North Atlantic Treaty. Washington D.C. - 4 April 1949.
[15] "Relations with partners across the globe", NATO, Feb. 17, 2023. Available: https://www.nato.int/cps/en/natohq/topics_49188.htm. (Accessed on: Feb. 20, 2023).
[16] Sun-Tzu, Art of War. Helikon, 2020.
[17] Strategic concepts", NATO, Feb. 20, 2023. Available: https://www.nato.int/cps/en/natohq/topics_56626.htm. (Accessed on: Feb. 20, 2023).
[18] I. Ahmad, "SCO summit reinforces global trend toward multipolarity," Arab News. Available: https://www.arabnews.com/node/2164911. (Accessed on: Feb. 20, 2023).

[19] U.S. Department of Defense, "America's Nuclear Triad", Available: https://www.defense.gov/Multimedia/Experience/Americas-Nuclear-Triad/. (Accessed on: Feb. 20, 2023).
[20] DC 6/1 The Strategic Concept for the Defense of the North Atlantic Area 1 December 1949. Available: https://www.nato.int/docu/stratdoc/eng/a491201a.pdf. (Accessed on: Feb. 20, 2023).
[21] "Dwight D. Eisenhower", The White House. Available: https://www.whitehouse.gov/about-the-white-house/presidents/dwight-d-eisenhower/. (Accessed on: Feb. 21, 2023).
[22] "Massive Retaliation", Britannica. Available: https://www.britannica.com/topic/nuclear-strategy/Massive-retaliation. (Accessed on: Feb. 21, 2023).
[23] MC 14/2 Overall Strategic Concept for the Defence of the NATO Area, 23. May 1957. Available: https://www.nato.int/docu/stratdoc/eng/a570523a.pdf. (Accessed on: Feb. 21, 2023).
[24] The North Atlantic Treaty. Washington D.C. - 4 April 1949. Available: https://www.nato.int/cps/en/natohq/official_texts_17120.htm. (Accessed on: Feb. 21, 2023).
[25] D. S. McDonough, "Nuclear Superiority or Mutually Assured Deterrence: The Development of the US Nuclear Deterrent", Canadian Journal of Political Science, vol. 60, no. 3, pp. 811-823, 2005.
[26] "Harmel Report", NATO. Available: https://www.nato.int/cps/en/natohq/topics_67927.htm. (Accessed on: Feb. 22, 2023).
[27] MC 14/3 Overall Strategic Concept for the Defence of the NATO Area, 16. January 1968. Available: https://www.nato.int/docu/stratdoc/eng/a680116a.pdf. (Accessed on: Feb. 22, 2023).
[28] F. Gazdag, "A magyar külpolitika 1989-2014", Nemzeti Közszolgálati Egyetem, 2014.
[29] North Atlantic Treaty Organization, "The Alliance's Strategic Concept, 2010", Available: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf. (Accessed: Feb. 22, 2023).
[30] North Atlantic Treaty Organization, "The Alliance's Strategic Concept, 1999", Available: https://www.nato.int/cps/en/natolive/official_texts_27433.htm. (Accessed: Feb. 22, 2023).
[31] L. R. Pfaltzgraff Jr., "NATO's Future Role: An American View", Proceedings of the Academy of Political Science, vol. 38, no. 1, pp. 176-186, 1991.
[32] North Atlantic Treaty Organization, "The Alliance's Strategic Concept, 1999."
[33] North Atlantic Treaty Organization, "The Alliance's Strategic Concept, 2010."
[34] Zs. Haig, Információs műveletek a kibertérben, Budapest: Dialóg Campus Kiadó, 2018.
[35] J. Tomolya, "A Geraszimov-cikk katonapolitikai háttere", DOI 10.17047/HADTUD.2019.29.1-2.74.
[36] Y. Hofstetter, „Láthatatlan háború – Avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását", Budapes, Corvina Kiadó, 2020.
[37] M. T. Klare, "China Reacts Aggressively to Pelosi's Taiwan Visit", Arms Control Association, 2022. Available: https://www.armscontrol.org/act/2022-09/news/china-reacts-aggressively-pelosis-taiwan-visit. (Accessed: Feb. 23, 2023).

[38] The State Council, "The People's Republic of China: China releases white paper on Taiwan question, reunification in new era", Available: https://english.www.gov.cn/archive/whitepaper/202208/10/content_WS62f34f46c6d02e533532f0ac.html. (Accessed: Feb. 23, 2023).
[39] P. Tálas, "A varsói NATO-csúcs legfontosabb döntéseiről", Nemzet és Biztonság, vol. 9, no. 2, pp. 97-101, 2016.
[40] Y. Hofstetter, „Láthatatlan háború – Avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását", Budapest, Corvina Kiadó, 2020.
[41] V. Putin, "Address by the President of the Russian Federation", The Kremlin, Moscow, Feb. 24, 2022. Available: http://en.kremlin.ru/events/president/news/67843. (Accessed: Feb. 25, 20239.
[42] United Nations Charter. Available: https://www.un.org/en/about-us/un-charter/full-text (Accessed: Feb. 25, 2023).
[43] Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX). Available: http://hrlibrary.umn.edu/instree/GAres3314.html (Accessed: Feb. 25, 2023).
[44] Relations with Russia. NATO. Available: https://www.nato.int/cps/en/natohq/topics_50090.htm (Accessed: Feb. 26, 2023).
[45] The People's Republic of China's 14th Five-Year Plan. Available: https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm. (Accessed: Feb. 25, 2023).
[46] GDP - China. The World Bank. Available: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN. (Accessed: Feb. 25, 2023).
[47] K. Wang, "China: Is it burdening poor countries with unsustainable debt?", BBC, Nov. 30, 2021. Available: https://www.bbc.com/news/59585507. (Accessed: Feb. 25, 2023).
[48] "NATO 2030: United for a new era" Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf. (Accessed: Feb. 25, 2023).
[49] "NATO to hike number of soldiers on high alert from 40,000 to 300,000, says Stoltenberg", Euronews, Jun. 27, 2022. Available: https://www.euronews.com/2022/06/27/nato-to-hike-number-of-soldiers-on-high-alert-from-40000-to-300000-says-stoltenberg. (Accessed: Feb. 25, 2023).
[50] Z. Szenes, "Előre a múltba", A NATO Wales után", Külügyi Szemle, vol. 13, no. 3, pp. 3-26, Fall 2014.
[51] "What is Hybrid CoE?", Hybrid CoE. Available: https://www.hybridcoe.fi/who-what-and-how/. (Accessed: Feb. 26, 2023).
[52] NATO 2022 Strategic Concept. Available: https://www.nato.int/strategic-concept/. (Accessed: Feb. 25, 2023).
[53] NATO 2022 Strategic Concept. Available: https://www.nato.int/strategic-concept/. (Accessed: Feb. 25, 2023).

# NEW CHALLENGES OF IR4 AND IR5: SOFT SKILLS AND CYBERSECURITY AWARENESS IN THE AGE OF DIGITAL TRANSFORMATION

## SYSTEMATIC REVIEW

# AZ IR4 ÉS IR5 ÚJ KIHÍVÁSAI: PUHA KÉSZSÉGEK ÉS KIBERBIZTONSÁGI TUDATOSSÁG A DIGITÁLIS ÁTALAKULÁS KORÁBAN

## SZISZTEMATIKUS SZAKIRODALOMELEMZÉS

MÓDNÉ TAKÁCS Judit[1] – POGÁTSNIK Monika[2]

**Abstract**

This systematic review aims to examine the reassessment of the crucial role of human participation within cyberspace, given the increasing importance of industries 4.0 and 5.0. Literature is lacking on the role of cyberspace, cyberawareness and soft skills, their interdependencies and the implications and consequences of developing them. This review outlines empirical research on soft skills and cybersecurity awareness in relation to industry transformations. The screening criteria were used to select 32 articles out of 5921. The study highlights the growing importance of combining technical and soft skills, including digital literacy, emotional intelligence, empathy and adaptability, for engineers and IT specialists working in this industry. Enhancing soft skills and cybersecurity awareness is essential for successful adaptation and maintaining competitiveness.

**Keywords**

industry 4.0, industry 5.0, cybersecurity awareness, soft skills, human centricity

**Absztrakt**

Kutatásunkban a szisztematikus szakirodalomelemzés módszerét alkalmazva megvizsgáltuk az ember szerepének újraértékelését a kibertérben az ipar 4.0 és 5.0 korában. A kibertér, a kibertudatosság és a puha készségek szerepéről, egymásra gyakorolt hatásukról, valamint ezek fejlesztésének eredményeiről kevés a szakirodalom. Az áttekintés célja, hogy ismertesse a puha készségekkel és a kiberbiztonsági tudatossággal kapcsolatos empirikus kutatásokat az ipari változások mentén. A szűrési kritériumok alapján 32 tanulmány került kiválasztásra 5921 cikkből. Elemzésünk a digitális írástudás, az érzelmi intelligencia, az empátia, az alkalmazkodóképesség, valamint a technikai és a puha készségek kombinációjának növekvő jelentőségét emeli ki a mérnökök és az informatikai szakemberek munkájában. A sikeres alkalmazkodás és versenyképesség fenntartásához elengedhetetlen a puha készségek és a kiberbiztonsági tudatosság fejlesztése.

**Kulcsszavak**

ipar 4.0, ipar 5.0, kiberbiztonsági tudatosság, puha készségek, emberközpontúság

[1] modne.t.judit@amk.uni-obuda.hu | ORCID: 0000-0001-8463-4032 | assistant lecturer, Obuda University Alba Regia Technical Faculty | PhD student, Obuda University Doctoral School for Safety and Security Sciences | tanársegéd, Óbudai Egyetem Alba Regia Műszaki Kar | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] pogatsnik.monika@amk.uni-obuda.hu | ORCID: 0000-0002-2698-7291 | associate professor, Obuda University Alba Regia Technical Faculty | egyetemi docens, Óbudai Egyetem Alba Regia Műszaki Kar

## BEVEZETÉS

Az ipar 4.0 és 5.0 jelentősen megváltoztatta az ipari környezetben zajló munkavégzést és az ehhez kapcsolódó szükségleteket. Az automatizálási folyamatok, a felhőtechnológiák széleskörű használata és a digitalizáció a munkafolyamatok szerves részévé váltak. Az ipar fejlődésével párhuzamos a kibertérben zajló munkavégzés került előtérbe került, hiszen a munkavégzés helye a digitális térbe helyeződött át. Ezen folyamatok együttesen változtatták meg a munkavállalóktól elvárt készségek és attitűdök körét [1]-[3]. Az emberi jelenlét sok szempontból vizsgálható a felsorolt változások vonatkozásában. A humán jelenlét kritikus szerepet játszik a kiberkörnyezetben folyó biztonságos tevékenységek kontextusában. A digitalizáció növekedése és az automatizáció terjedése mellett a közelmúlt változásai és környezeti hatásai miatt egyre inkább szükség van a humán jelenlét, az elvárt kompetenciák és készségek újraértékelésére, fejlesztésére és elemzésére.[4], [5]

Ennek a tanulmánynak célja, hogy feltárja az emberi és gépi részvétel konvergenciájának hatását az ipar 4.0 és 5.0 területén a munkaerőpiacra és a munkaerő-képzésre. Kiemelt figyelmet szentelve a megváltozott munkakörnyezetben és munkakapcsolatokban tapasztalható hatékony, emberközpontú feladatellátásnak, tanulmányozzuk a puha készségek jelentőségét és a kiberbiztonsági tudatosság fontosságát a biztonságcentrikus munkavégzéshez. [6].

### Kutatási kérdések

A tanulmány célja, hogy a növekvő jelentőségű ipar 4.0 és 5.0 kontextusában újraértékelje az emberi részvétel kritikus szerepét a kibertérben zajló munkafolyamatokban. A vizsgálat középpontjában a változások, kihívások és munkaerőpiaci lehetőségek állnak, megvizsgálva a kibertér, a kibertudatos viselkedés és a puha készségek közötti összefüggéseket.

Ezen szisztematikus áttekintés a következő kérdésekre összpontosít:

- K1: *Melyek jelenleg a leginkább preferált puha készségek a mérnökök körében, és hogyan változnak ezek az Ipar 4.0 és az Ipar 5.0 kontextusában?*
- K2: *Tekintettel a kibertér kihívásaira, milyen szintű kiberbiztonsági tudatossággal kell rendelkezniük az ipar 4.0 és az ipar 5.0 világában dolgozó mérnököknek?*
- K3: *Milyen puha készségekkel kapcsolatos hiányosságok lettek azonosítva a kibertérhez köthető munkakörökben?*

A tanulmány eredményeitől függően olyan változtatások és fejlesztések határozhatók meg, amelyek segítik az ipart és az oktatási rendszert abban, hogy megfeleljen az ipar 4.0 és 5.0 kihívásainak a fenntartható gazdasági fejlődés és versenyképesség érdekében.

## A SZAKIRODALOM ÁTTEKINTÉSE

### A kiberbiztonsági tudatosság jelentősége a kibertéri munkafolyamatokban

Mivel az IIoT-hálózatokban rengeteg intelligens eszköz kapcsolódik különféle gépekhez, robotokhoz, okoseszközökhöz, számítógépekhez és emberekhez, így a kiberbiztonság alapvető kérdésnek számít a 21. századi szervezetek és egyének szemszögéből [6]. Ebben az összetett és összekapcsolt ipari környezetben a kiberbiztonsági tudatosság elengedhetetlen feltétele a kiberbiztonsági incidensek és az érzékeny adatok megsértésének meg-

előzéséhez vagy minimalizálásához, valamint ahhoz, hogy a vállalatok ellenállóbbak legyenek a kibertámadásokkal szemben. A COVID-19 világjárvány okozta változások és a távmunka egyre gyakoribbá válása kiemelten fontossá tette a megfelelő szintű kiberbiztonsági készségek és attitűdök fejlesztését. A szükséges ismereteket a felnövekvő generációnak megfelelő módon kell átadni, és a biztonságtudatosság kialakítását már az általános iskola korai szakaszában el kell kezdeni, valamint a középfokú- és felsőoktatási intézményekben folyamatosan fejleszteni és növelni kell. A kiberbiztonsági készségek fejlesztése az Európai Bizottság átfogó digitális készségfejlesztési programjának is részét képezik. A Horizon 2020, a Horizon Európa és a Digitális Európa program keretében már most is különféle programok valósulnak meg az oktatás és az emberi tényező tudatosítása céljából. Az Európai Bizottság számos területen támogatja ezeket a digitális írástudással kapcsolatos erőfeszítéseket, többek között a kiberbiztonsági készségek képzésének koherens keretrendszerére irányuló felhívásokkal, különböző kísérleti projektekkel és folyamatban lévő kezdeményezésekkel.[7]

**A puha készségek jelenléte a kibertérbeli feladatok ellátáshoz**

Ahhoz, hogy a jövő szakemberei a tudásukat együttműködő és értékteremtő módon tudják használni, számos 4IR vagy Ipar 4.0 kulcskompetenciával, széleskörű készségekkel kell rendelkezniük [8]. Ide tartoznak többek között az olyan puha készségek, mint a kommunikáció, a kreativitás és a problémamegoldás. A 21. századi készségek a "puha" készségek kiegészülnek a "kemény" készségekkel.[9]

A kibertudatos viselkedés és a puha készségek komplex, együttes szerepével, párhuzamos fejlődésük hatásával és következményeivel, valamint szintjükkel egzakt, pontos mérésével a szakirodalom nem foglalkozik összefüggéseiben. Az sem tisztázott teljeskörűen, hogy a 21. századi munkavállalóknak milyen készségeket kell fejleszteniük ahhoz, hogy biztonságosan éljenek az információs szupersztrádán és alkalmazkodjanak a gyorsan változó körülményekhez, és hogy a különböző intelligens eszközökkel, a rendelkezésre álló technológiával és gépekkel való szoros kapcsolat hogyan befolyásolja majd ezt a folyamatot. Figyelembe kell venni, hogy milyen eszközök mérik a kívánt puha készségek és a kiberbiztonsági tudatosság fejlesztésének hatékonyságát, és hogy a különböző típusú képzéseknek van-e mérhető, tényleges fejlesztő hatásuk ebben a tanulási folyamatban. Ezen szisztematikus szakirodalomelemzés ezen hiányosság pótlására törekszik a posztindusztriális puha készségekkel és a kiberbiztonsági tudatossággal kapcsolatos empirikus kutatások adatait rendszerezve.

## A KUTATÁS MÓDSZERTANA

A kutatás során alkalmazott szisztematikus szakirodalomelemzés módszertana a PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) elveit követi. A kutatási kérdések megválaszolásához az 1. táblázatban feltüntetett PICO (Population Intervention Comparison Outcome) keret került kialakításra:

| Kutatási kérdés | P | I | C | O |
|---|---|---|---|---|
| K1 | mérnökök az ipar 4.0 és 5.0 területén | szükséges puha készségek | az ipar 4.0 és 5.0 különbségeinek összehasonlítása | a mérnökök körében leggyakrabban előforduló "puha készségek" azonosítása, az Ipar 4.0 és az Ipar 5.0 közötti különbségek meghatározásával. |
| K2 | mérnökök az ipar 4.0 és 5.0 területén | a kiberbiztonsági tudatosság jelenlegi elvárt szintje | az ipar 4.0 és 5.0 különbségeinek összehasonlítása | az ipar 4.0 és 5.0 mérnökei körében a kiberbiztonsági tudatosság jelenlegi elvárt szintjének meghatározása a kibertérrel kapcsolatos feladatok tekintetében |
| K3 | a kibertérben dolgozó mérnökök | puha készségek hiánya | az ipar 4.0 és 5.0 különbségeinek összehasonlítása | a kibertérhez kapcsolódó munkakörökben, az ipar 4.0 és az 5.0 mérnökeinek puha készségeinek hiánya terén mutatkozó különbségek azonosítása |

*1. Táblázat: A kutatási kérdés meghatározásához használt PICO-keretrendszer*

**A keresési stratégia és a kiválasztási folyamat**

A szakirodalom szisztematikus áttekintése érdekében átfogó keresést végeztünk a puha készségek, kiberbiztonság, oktatás, emberi aspektus és ipar 4.0/5.0 kulcsszavak különböző kombinációinak, szinonimáinak felhasználásával. A kereséshez Boolean-operátorokat használtunk, mint az ÉS és a VAGY műveletek, amelyekkel több adatbázisban, többek között a Scopus, a Web of Science és az IEEE Xplore adatbázisaiban kombináltuk a keresési kifejezéseket.

A következő angol szavakat tartalmazó keresőkombináció került felhasználásra, az angol nyelvű szakirodalmak szűréséhez: „cybersecurity" OR „information security" OR „cybersecurity awareness" OR „data security" OR „cyberspace" OR „cyber security awareness" OR „security awareness" OR „soft skill" OR „digital skill" AND „human factor" OR „engineer" OR „human" OR „engineering" OR „workforce" AND „industry 4.0" OR „industry 5.0". A kezdeti keresési halmaz összesen 5921 cikket tartalmazott. Az első szakaszban a szelekció a 2017 és 2022 közötti elmúlt hat évben megjelent, angol nyelven írt konferencia- és folyóiratcikkekre, valamint a lektorált tudományos cikkekre korlátozódott.

**A befogadási és kizárási kritériumok**

Az áttekintés céljához illeszkedően határoztuk meg a befogadási és kizárási kritériumokat. A szűrés pontos céljai, hogy azonosítani és összegezni tudjuk az ipar 4.0 és 5.0 hatásait az emberi tényezőre, hogy felmérjük a kibertér fontosságát és ezen belül a veszélyekre való hatékony reagálás képességének fontosságát, illetve hogy azonosítsuk a szükséges puha készségeket.

A kizárási kritériumok a következők voltak. A nyelvi eltérések kockázatának csökkentése érdekében a keresést az angol nyelven megjelent, lektorált tanulmányokra korlátoztuk. Azon cikkek, melyek nem önálló kutatásról számolnak be, mint például a szerkesztői levelek, szerkesztői cikkek, kommentárok és áttekintések, szintén kizárásra kerültek. Azon tanulmányok, amelyek nem a műszaki pályákra, szakterületekre vagy a humán oldalra összpontosítottak, kizárásra kerültek. Végezetül céljaink között szerepelt, hogy áttekintésünk során magas módszertani normákat alkalmazzunk, így bizonyos típusú cikkek, például könyvek, könyvkivonatok és nem eredeti kutatást reprezentáló tanulmányok szintén kizárásra kerültek.

Egy tanulmány befogadási kritériumai a következők:

- angol nyelven megjelent, és lektorált
- eredeti kutatásról számol be a műszaki pályához köthetően, de kizárva a szisztematikus szakirodalomelemzéseket és metaanalíziseket
- kvantitatív vagy kvalitatív adatokat szolgáltatnak a 21. századi puha készségek mérésével, szintjével vagy a kiberbiztonsági tudatosság mérésével, fejlesztésével kapcsolatosan
- az emberi tényező szerepére fókuszál
- információt nyújtanak a digitalizálás, felhőalapú szolgálatások, kibertérben zajló munkavégzéshez köthető elvárásokkal, puha készségekkel kapcsolatban

A módszertani követelményeknek és minőségi előírásoknak megfelelő, releváns tanulmányok áttekintésünkbe való bevonásának biztosítása érdekében dolgoztuk ki ezeket a kritériumokat, melyek biztosítják, hogy áttekintésünk releváns értekezéseket tartalmazzon.

**A szűrési és adatkiválasztási folyamat**

A szisztematikus felülvizsgálat a PRISMA irányelveket követte. A releváns elektronikus adatbázisokban (IEEE Xplore, Scopus, Web of Science) átfogó keresést végeztünk a korábban megadott kulcsszavak kombinációjának felhasználásával.

Az azonosított cikkek összegyűjtése után a duplikációkat és a bekerülési kritériumoknak nem megfelelő tanulmányok eltávolításra kerültek. A fennmaradó értekezések címét és kivonatát két bíráló egymástól függetlenül ellenőrizte, majd a teljes szövegű cikkek alkalmasságát értékelték. Ezt követte az adatkivonatolás és a minőségértékelés egy meghatározott kritériumok szerinti adatbázis felépítésének segítségével. Az adatok elemzéséhez narratív szintetizáló megközelítést alkalmaztunk.

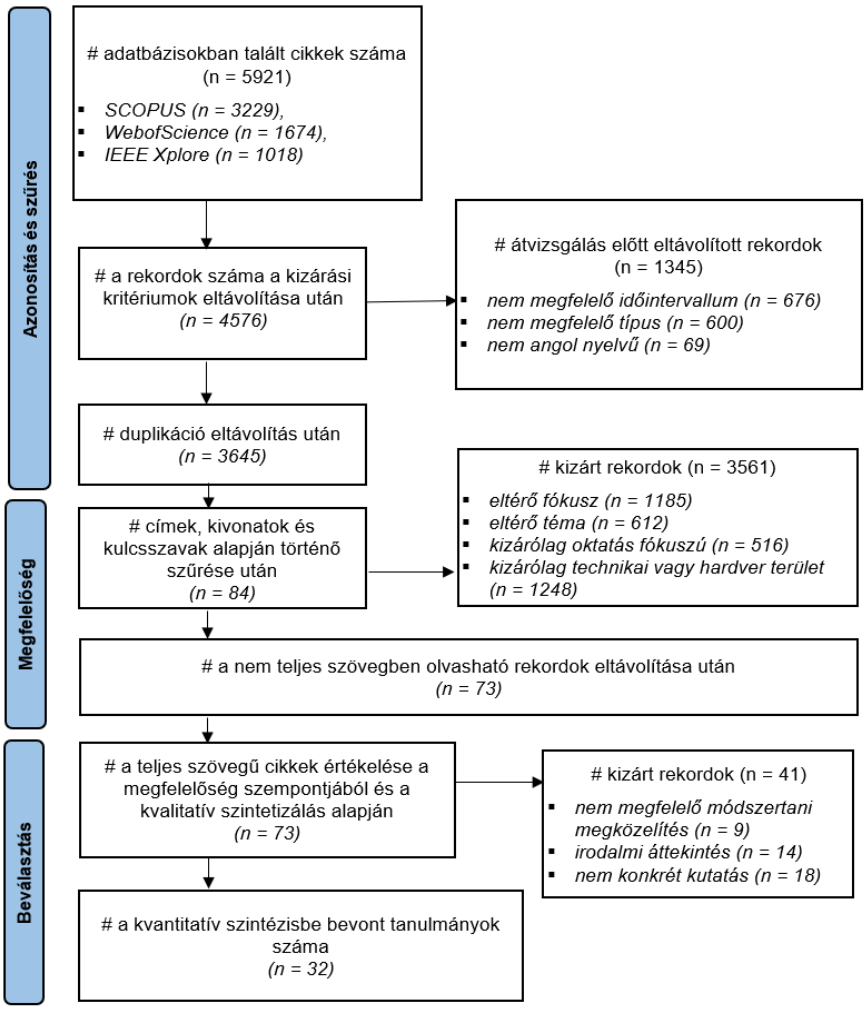
A szűrési folyamat a következő volt:

- azon cikkek eltávolítása, melyek az év, nyelv, típus szerint nem felelnek meg a kritériumoknak
- a duplikált tanulmányok eltávolítása
- a befogadási/kizárási kritériumoknak nem megfelelő cikkek eltávolítása cím és absztrakt alapján
- a nem teljes szöveggel elérhető értekezések eltávolítása
- a teljes terjedelmű cikkek átvizsgálása, befogadási kritériumoknak való megfelelőség vizsgálata
- az adatok kinyerése a véglegesen kiszűrt elemzésekből a kutatási kérdések által meghatározott kategóriákba

A keresés eredetileg 5921 cikket eredményezett. 676 tanulmány nem felelt meg a megadott időintervallumnak, 600 kizárásra került a típusa miatt, és 69 nem angol nyelven íródott, így ezek kizására kerültek. A Zotero és a Rayyan alkalmazás segítségével összesen 931 duplikátumot távolítottunk el. Ennek eredményeként 3645 rekordot kaptunk.

A címek és összefoglalók áttekintése 84 cikkre csökkentette a kritériumoknak megfelelő elemzések számát. Annak megállapítása érdekében, hogy a kiválasztott tanulmányok valóban illeszkednek a kutatás célkitűzéseihez, mindkét szerző elvégezte a cikkek elemzését.

A végső teljes áttekintésből kizárásra kerültek azok a cikkek, amelyek nem rendelkeztek teljes hozzáféréssel, amelyekből hiányoztak az elsődleges kutatási adatok, amelyek csak szakirodalmi adatokra támaszkodtak, vagy amelyek nem voltak relevánsak a célcsoport szempontjából. Végeredményben 32 cikk került be a végső áttekintésbe. A szűrési folyamat, a kiválasztás, illetve a kizárások okai az 1. ábrán láthatók részletezve.




*1. Ábra: A tanulmányok kiválasztásának folyamatábrája a PRISMA-irányelvek szerint (Forrás: saját szerkesztés)*

### Adatelemzési és szintetizálási módszerek

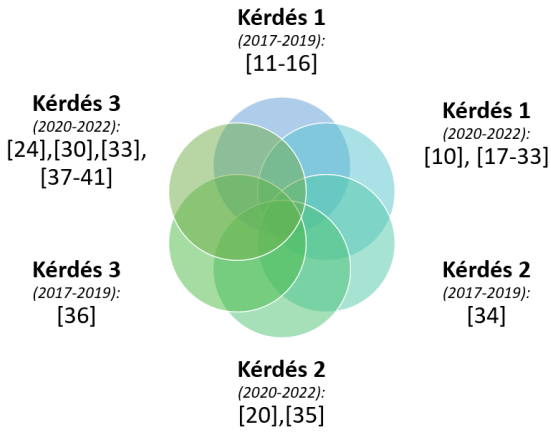
A cikk kategóriákba sorolásához minőségi tartalomelemzési módszereket alkalmaztunk, amelyek segítségével osztályoztuk a cikkekben található kutatási kérdés szempontjából releváns információkat, valamint kinyertük az adatokat a PICO-keretben meghatározott kritériumok alapján. Az adatok elemzéséhez narratív szintézis alapú megközelítésre került sor. Az adatok feldolgozásához a következő csoportosítási kritériumokat alkalmaztuk: A 2017-2019 közötti, a COVID előtti időszak, majd az ezt követő három év, 2022-ig bezáróan. Az adatgyűjtés során olyan általános információk kerültek felhasználásra, mint: a kutatási módszer, a populáció mérete, vizsgált szakterület, földrajzi elhelyezkedés és a használt mérőeszköz típusa. A kutatás célkitűzéseinek megfelelően kiterjesztettük az adatelemzési csoportokat további kategóriákkal, amelyek közé tartozak a szükséges puha készségek, a kutatási eredmények relevanciája az ipari 4.0 vagy 5.0 szempontjából, a kiberbiztonsági tudatosság szintjének mérése, valamint a puha készséghiányok azonosítása.

## EREDMÉNYEK

Az alábbi szekcióban bemutatjuk a kutatási kérdések alapján összegyűjtött releváns adatokat, melyeket a kutatási kérdések mentén csoportosítjuk és prezentáljuk.

### Az elemzésbe bevont tanulmányok áttekintése

A vizsgálat során összesen 32 tanulmány részletes elemzésére került sor, ebből N=23 cikk eredményei az 1. kutatási kérdésre összpontosítanak. Kutatási módszerek szerint összegezve az értekezéseket, 15 kvantitatív, 11 kvalitatív és 6 vegyes módszert alkalmazott a vizsgálat során. A cikkek 25%-a 2017-2019-es időszakból kerültek kiválogatásra, ami a világjárvány előtti időszakot jelenti. A fennmaradó 24 publikáció, a vizsgált tanulmányok 75%-a pandémiát követő időszakból került be az elemzésbe. A bemutatott válogatási folyamat eredményeként az ipar 5.0 vonatkozásában csak egy publikáció került kiválasztásra, így az ipar 4.0 és 5.0 valós méréseken alapuló összehasonlítására tett erőfeszítések nem jártak sikerrel. Ennek következtében az eredmények főként az ipar 4.0 kontextusában kerülnek prezentálásra. A 2. ábra a kutatási kérdések alapján csoportosított tanulmányok hivatkozási listáját szemlélteti.




*2. Ábra: Az elemzésbe bevont tanulmányok kutatási kérdések szerint csoportosítva (Forrás: saját szerkesztés)*

Az elemzésekben megfigyelt populációk túlnyomórészt európai eredetűek, közülük Kelet- és Nyugat-Európa képviselteti leginkább magát. Törökország és Oroszország hidat képez Európa és Ázsia között, ugyanakkor Ázsia reprezentációja alacsonyabb. Észak-Amerika az USA-t és Mexikót, Dél-Amerika pedig Brazília képviseli. A tanulmányokban megjelennek az iparág képviselői és az oktatás szereplői egyaránt. Vizsgált alanyai között diákok, oktatók, szakemberek, vezetők, mérnökök, HR szakemberek, biztonsági szakemberek, IT szakemberek, menedzserek, oktatók és mentorok szerepelnek.

**Az ipar 4.0 változást eredményezett a puha készségek terén**

A felhasznált irodalmi források mindegyike hangsúlyozza a puha készségek fontosságát az ipar 4.0 és az ipar 5.0 környezetben való sikeres helytálláshoz. A hiányolt puha készségek közül kiemelkednek a kommunikáció, a csapatmunka, az érzelmi intelligencia és az alkalmazkodóképesség. A munka természetének átalakulása folyamatban van, így a munkavállalóknak technikai és pszichoszociális készségeinek fejlesztése egyaránt szükséges. Az oktatás alapvető fontosságú a technológiai változásokra való felkészüléshez, és az alacsonyan képzett munkavállalók átképzése indokolt a munkavállalók marginalizálódásának elkerülése érdekében. A mesterséges intelligencia és a dolgok internete, amelyek egyszerre jelentenek kihívásokat és lehetőségeket, emberközpontú megközelítést igényelnek. A vizsgált tanulmányok különböző készségekre és kompetenciákra összpontosítanak, konkrét kereteket és modelleket javasolnak az oktatás és képzés javítására, és empirikus bizonyítékokkal szolgálnak a készséghiányról, és az ágazatra gyakorolt hatásáról.

Az elvárt alapkompetenciák közé tartoznak többek között az önmenedzsment, csapatmunka, kreativitás, kommunikáció, digitális készségek, probléma-megoldás, alkalmazkodóképesség, kritikus gondolkodás, érzelmi intelligencia és innováció. Kiemelt kategóriába sorolhatók a tanulási, és interperszonális készségek, motivációs készségek, élethosszig tartó tanulás, stresszkezelés és kezdeményezőkészség. Ezek a puha és személyes készségek elengedhetetlenek a sikerhez, mindennapi élethez és számos különböző területen és iparágban.

Tehát az 1. kutatási kérdésre válaszolva a kommunikáció, a csapatmunka, a problémamegoldás, a kreativitás, az alkalmazkodóképesség, az innováció, a vezetői képességek és a digitális írástudás a mai mérnökök körében a leggyakrabban elvárt "puha készségek". A munkaerőpiac olyan mérnökök iránt érdeklődik, akik rendelkeznek megfelelő szociális, technikai és műszaki készségekkel, beleértve a digitális kompetenciát, a funkcionális üzleti készségeket és a stratégiai készségeket. Az alkalmazottaknak ezekre a kulcsfontosságú területekre kell összpontosítaniuk a versenyképes és korszerű munkakörnyezetben való sikeres részvétel érdekében. A technológia gyors ütemű és folyamatosan változó természetéhez való alkalmazkodás érdekében elengedhetetlen készségek az önállóság, proaktivitás és rugalmasság.

Az ipar 5.0, amelyet az ember és a gép integrációja jellemez a termelési folyamatban, megköveteli a mérnököktől, hogy ötvözzék a műszaki és a szociális készségeket. Alapos technológiai ismeretekre van szükségük, ugyanakkor a gépekkel való interakcióra és interdiszciplináris csapatokban való együttműködésre is képesnek kell lenniük. Emellett egyre fontosabbá válnak az olyan puha készségek, mint az érzelmi intelligencia, a kreativitás, az empátia és az alkalmazkodóképesség.

A 2. táblázat a vizsgált tanulmányokban meghatározott szociális készségeket összegzi, a tanulmányok hivatkozási számának jelölésével, az elvárt puha készségek szerint kategorizálva.

| **Publikációk hivatkozással** | **Elvárt puha készségek** | |
|---|---|---|
| | ***Kategória*** | ***Készségek*** |
| [10-15], [18-20],[22], [23],[25], [29-32] | Kommunikációs és interperszonális készségek | asszertivitás, empátia, interperszonális és kommunikációs készségek, csapatmunka, érzelmi intelligencia, hierarchia tiszteletben tartása, együttműködés, szociális készségek és tudatosság. |
| [10-13],[15], [18],[19],[22] [24],[25],[27] [29-32] | Személyes készségek | önbizalom, függetlenség, önmenedzselés, alkalmazkodóképesség, reziliencia, proaktivitás, motiváció, élethosszig tartó tanulás, kiégés megelőzése, agilitás, önirányítás, felelősségtudat, munkavédelem, stresszkezelés |
| [12],[16],[17] [21],[23],[30] [33] | Digitális és informatikai készségek | digitális írástudás, információs készségek, műszaki és IKT készségek, digitális kommunikáció, folyamatok megértése és optimalizálása, berendezések üzemeltetése, biztonsági készségek |
| [11-15],[20], [22],[23],[25] [26],[28],[29] [31],[32] | Szervezési és irányítási készségek | projektmenedzsment, vezetői készségek, szervezeti kultúra, időgazdálkodás |

*2. Táblázat: A puha készségek kategorizált listája a szakirodalmi jelöléssel együtt*

## A kiberbiztonsági szemléletmód az ipar 4.0 és 5.0 világában

A [20] tanulmány elemzi a technológiai trendek hatását a munkahelyekre és a készségek változására. Olyan modellt javasol a munkavállalók készségeinek fejlesztésére és a készséghiányok leküzdésére mely a meglévő képzési programokon keresztül segíthet a munkaerőpiaci kihívásokra reagálni és a munkaerő készségszintjét javítani. A középpontban a technológia munkára gyakorolt hatásának elemzése és a munkaerő alkalmazkodóképessége áll.

A [34] értekezés a formális szabályozások és szankciók hatásainak elemzését mutatja be. Az értékelés és az ellenőrzés olyan szabályozási mechanizmusok, amelyek kiemelkedő szerepet játszanak a biztonsági eljárások betartásának előmozdításában. Az eredmények alapján felismerhető, hogy ezek a mechanizmusok nélkülözhetetlenek a hatékony és megbízható biztonsági rendszerek kialakításához és fenntartásához.

Az informatika oktatásának szerepével, a megfelelő módszerek kiválasztásával a [35] cikk foglalkozik. Egy olyan megközelítést javasol, amellyel leküzdhetők a szoftverfejlesztés tanításának nehézségei. Mindegyik tanulmány empirikus jellegű, és különböző módszertanokat és modelleket javasol a konkrét kérdések megválaszolására.

A [20] és [34] tanulmányok az externális tényezők hatását vizsgálják a munkavállalói magatartásra, bár eltérő szempontok szerint: az első tanulmány a technológiai trendekre és készségfejlesztésre, míg a második tanulmány az információbiztonsággal kapcsolatos formális ellenőrzésekre és szankciókra összpontosít. Azonban a [35] tanulmány a tanulási módszerek fejlesztésére fókuszál, ami szintén fontos tényező a munkavállalói magatartás alakulásában.

Az eredmények azonban csak érintik, de nem nyújtanak közvetlen választ az ipar 4.0 és az ipar 5.0 mérnökei esetében felmerülő tudatos kiberbiztonsági magatartásra vonatkozó kérdésre. Az értekezésben említett három publikáció nem szolgáltat kellő mennyiségű és minőségű információt a kiberbiztonsági tudatosság jelenleg várható szintjéről. Bár a formális ellenőrzések és szankciók hozzájárulhatnak az információbiztonsági gyakorlatok betartásához, nem szolgáltatnak konkrét információt a kiberbiztonsági tudatosság általánosan elvárt mértékéről.

**Készséghiány a kibertérrel összefüggő ipar 4.0-s szakmákban**

A [24][30],[33],[37],[38] tanulmányokban kiemelik a megfelelő digitális írástudás hiányát és a folyamatos készségfejlesztés jelentőségét. A kritikus/analitikus gondolkodás [24],[30],[41], a tervezési és szervezési készségek [24],[41], az új helyzetekhez való alkalmazkodóképesség, a reziliencia [24],[37] és a kiberbiztonsági és az információbiztonsági készségek fontossága [30],[33],[37],[39-41] szintén hiányolt és az elvárt készségek csoportjába tartoznak. Az ipar 4.0 megvalósítása során a munkavállalók félelme és a technológiával szembeni ellenállás jelentős kihívást jelent [37]. Ennek következtében elengedhetetlen a megfelelő képzés biztosítása, amely kompenzálja a hiányzó készségeket. A [24], [30] és [41] cikkek a puha készségek hiányát vizsgálják, ideértve a szervezési és csapatmunkával kapcsolatos készségeket, valamint a szociális és kommunikációs készségek fontosságát az informatikai szakemberek körében, különös tekintettel a friss diplomások munkaerőpiacra való belépésekor jelentkező kritikus kérdésekre. Az tapasztalatok azt mutatják, hogy ezek a szakemberek gyakran nem tudják alkalmazni elméleti tudásukat valós élethelyzetekben. Az önbizalom fejlesztése és a mentori támogatás, a folyamatos munkahelyi tanulás, az önálló tanulás képessége, a kritikus kérdésfeltevés és a negatív/pozitív visszajelzések elfogadásának képessége alapvető készségként jelenik meg. Végezetül a vizsgált tanulmányok hangsúlyozzák a minőségi információforrások kiválasztásának fontosságát, beleértve az információgyűjtés és -értékelés minőségi szempontjainak ismeretét, az információk elemzésének és szintézisének képességét, a jelentéskészítés és hivatkozáskészítés képességét, valamint az adatbiztonsági tudatosság meglétét e feladatokkal kapcsolatban. [24],[30],[36],[41]

Mivel nem állnak rendelkezésre olyan publikációk, amelyek közvetlenül összehasonlítanák az ipar 4.0 és az ipar 5.0 kontextusában a mérnökök puha készségei közötti különbséget, a 3. kutatási kérdésre nem adható megalapozott és teljes körű válasz. Azonban a publikációk kiemelik az IT- és mérnöki szakemberek digitális és kiberkészségek terén tapasztalható hiányosságait, ideértve a digitális írástudást, a kritikus gondolkodást és az al-

kalmazkodási készségeket. Ezeket a készséghiányokat folyamatos készségfejlesztés, munkahelyi tanulás és mentori támogatás révén kell kezelni. Azonban ahhoz, hogy a puha készségek hiányosságait az ipar 4.0 és 5.0 vonatkozásában össze tudjuk hasonlítani, pontosabb és naprakészebb adatokra van szükségünk.

## ÖSSZEFOGLALÁS ÉS KONKLÚZIÓ

A kutatás a kibertérre összpontosítva vizsgálja az Ipar 4.0 és az Ipar 5.0 ember-gép együttműködésének munkaerőpiacra és -képzésre gyakorolt hatásait. Az N=5921 értekezésből N=32 tanulmányt részletesen áttekintettük a szakirodalom szisztematikus átvizsgálása céljából. Az elemzésbe bevont cikkek többsége az első kutatási célkitűzésre összpontosít, nevezetesen milyen puha készségekre van ma a legnagyobb szükség a mérnökök esetében, és ezek hogyan változnak az ipar 4.0 és az ipar 5.0 kontextusában. A hiányosságok megszüntetéséhez elengedhetetlen a folyamatos készségfejlesztés, a munkahelyi tanulás és a mentorálás. Az ipar 4.0 és 5.0 szempontjából létfontosságú az emberi részvétel és a kibertér közötti kapcsolat mélyebb megértése.

A jövőbeli kutatási irány általánosságban a kibertér és az emberi részvétel közötti összetett kapcsolat mélyebb megértésére összpontosít, különös tekintettel a munkaerő-képzésre. A kutatás célja lehet a kibertérben tevékenykedő szakemberek és az általuk végzett munka közötti dinamikák és kölcsönhatások feltárása, valamint az ehhez kapcsolódó kihívások és lehetőségek azonosítása. A kiberbiztonsági tudatossággal és a puha készségekkel kapcsolatos további kutatások segíthetnek az ipar 4.0 és 5.0 által előidézett változások és kihívások kezelésében, és elősegíthetik a kibertérben foglalkoztatottak fenntartható és eredményes fejlődését.

## FELHASZNÁLT IRODALOM

[1] Dimitris, M., Angelopoulos, J., and Panopoulos, N., “A Literature Review of the Challenges and Opportunities of the Transition from Industry 4.0 to Society 5.0” Energies 15, 2022, no. 17: 6276. https://doi.org/10.3390/en15176276

[2] Hozdić, E., and Butala, P., “Concept of Socio-Cyber-Physical Work Systems for Industry 4.0”, Tehnički vjesnik, 27(2), 2020, pp. 399-410. https://doi.org/10.17559/TV-20170803142215

[3] B. Beszédes, K. Széll, and G. Györök, “A Highly Reliable, Modular, Redundant and Self-Monitoring PSU Architecture.,” Acta Polytechnica Hungarica, vol. 17, 2019, pp. 233–249

[4] Clim, A., “Cyber security beyond the Industry 4.0 era. A short review on a few technological promises.” Informatica Economica 23.2: 34-44., 2019, [online] available: http://revistaie.ase.ro/content/90/04%20-%20clim.pdf

[5] Corallo, A., Lazoi, M., & Lezzi, M., “Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts.” Computers in industry, 114, 2020, https://doi.org/10.1016/j.compind.2019.103165

[6] Corallo, A. et al., “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review.” Computers in Industry, 137, 103614., 2022, https://doi.org/10.1016/j.compind.2022.103614

[7] European Commission, "Cybersecurity Policies" Shaping Europe's Digital Future, 2023, [online] available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7xll8 (*utolsó megtekintés: 2023. március 19.*)
[8] Hernandez-de-Menendez, M. et al.,"Competencies for industry 4.0." International Journal on Interactive Design and Manufacturing (IJIDeM), 14, 2020, pp 1511-1524. https://doi.org/10.1007/s12008-020-00716-2
[9] Chaka, C., "Skills, competencies and literacies attributed to 4IR/Industry 4.0: Scoping review." IFLA journal, 46(4), 2020, pp 369-399. https://doi.org/10.1177/0340035219896376
[10] S. T. S. Chin, "Influence of emotional intelligence on the workforce for industry 5.0", Ibima Bus. Rev., vol. 2021, 2021, doi: 10.5171/2021.882278.
[11] G. Cotet et al., "Assessment procedure for the soft skills requested by Industry 4.0", presented at the 8th International Conference on Manufacturing Science and Education (MSE 2017) – Trends in new industrial revolution, vol. 121. 2017, doi: 10.1051/matecconf/201712107005.
[12] J.-F. Martínez-Cerdá et al., "Opening the black-box in lifelong E-learning for employability: A framework for a Socio-Technical E-learning Employability System of Measurement (STELEM)", Sustainability, vol. 10, no. 4, 2018, doi: 10.3390/su10041014.
[13] V. Siddoo, J. Sawattawee, W. Janchai, and O. Thinnukool, "An exploratory study of digital workforce competency in Thailand", Heliyon, vol. 5, no. 5, 2019, doi: 10.1016/j.heliyon.2019.e01723.
[14] U. Snis et al., "Contextualizing competence and learning for Industry 4.0", presented at the 13TH International Technology, Education and Development Conference (INTED2019), 2019, pp. 6923–6931. doi: 10.21125/inted.2019.1679.
[15] B. Lenarcic, "Rethinking competencies ot the European information-communication sector's workforce in the context of industry 4.0: The case of Slovenia", Sociologija, vol. 61, no. 4, 2019, pp. 585–598, doi: 10.2298/SOC1904585L.
[16] A. Ismail and R. Hassan, "Technical Competencies in Digital Technology towards Industrial Revolution 4.0", Journal of Technical Education and Training, vol. 11, no. 3, 2019, pp. 56–62, doi: 10.30880/jtet.2019.11.03.008.
[17] N. Ada, D. Ilic, and M. Sagnak, "A Framework for New Workforce Skills in the Era of Industry 4.0", International journal of mathematical engineering and management sciences, vol. 6, no. 3, 2021, pp. 771–786, doi: 10.33889/IJMEMS.2021.6.3.046.
[18] B. Kowal, D. Wlodarz, E. Brzychczy, and A. Klepka, "Analysis of Employees' Competencies in the Context of Industry 4.0", Energies, vol. 15, no. 19, 2022, doi: 10.3390/en15197142.
[19] G. Cotet, N. Carutasu, and F. Chiscop, "Industry 4.0 Diagnosis from an iMillennial Educational Perspective", Education Sciences, vol. 10, no. 1, 2020, doi: 10.3390/educsci10010021.
[20] J. Pontes et al., "Relationship between Trends, Job Profiles, Skills and Training Programs in the Factory of the Future", presented at the 22nd IEEE International Conference on Industrial Technology, ICIT 2021, 2021, pp. 1240–1245. doi: 10.1109/ICIT46573.2021.9453584.

[21] N. Obermayer et al., "Overcoming the Challenges of Digitalisation in Hungarian Manufacturing Companies", presented at the 23rd European Conference on Knowledge Management, ECKM 2022, vol. 23, 2022, pp. 845–851. doi: 10.34190/eckm.23.2.454.
[22] M. McPhillips and M. Licznerska, "Open innovation competence for a future-proof workforce: a comparative study from four European universities", J. Theor. Appl. Electron. Commer. Res., vol. 16, no. 6, 2021, pp. 2442–2457, doi: 10.3390/jtaer16060134.
[23] G. Rodriguez-Abitia et al., "Competencies of Information Technology Professionals in Society 5.0", Rev. Iberoam. Technol. Aprendizaje, vol. 17, no. 4, 2022, pp. 343–350, doi: 10.1109/RITA.2022.3217136.
[24] P. Leitão et al., "Analysis of the Workforce Skills for the Factories of the Future", presented at the 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS), vol. 1, 2020, pp. 353–358. doi: 10.1109/ICPS48405.2020.9274757.
[25] V. Goulart, L. Liboni, and L. Cezarino, "Balancing skills in the digital transformation era: The future of jobs and the role of higher education", Industry and Higher Education, vol. 36, no. 2, 2022, pp. 118–127, doi: 10.1177/09504222211029796.
[26] Z. Mingaleva and N. Vukovic, "Development of Engineering Students Competencies Based on Cognitive Technologies in Conditions of Industry 4.0", International Journal of Cognitive Research in Science Engineering and Education, vol. 8, 2020, pp. 93–102, doi: 10.23947/2334-8496-2020-8-SI-93-101.
[27] S. Veljkovic et al., "Emotional Intelligence of Engineering Students as Basis for More Successful Learning Process for Industry 4.0", Mathematics, vol. 8, no. 8, 2020, doi: 10.3390/math8081321.
[28] M. Pena-Jimenez, A. Battistelli, C. Odoardi, and M. Antino, "Exploring skill requirements for the Industry 4.0: A worker-oriented approach", Anales de psicologia, vol. 37, no. 3, 2021, pp. 577–588, doi: 10.6018/analesps.444311.
[29] N. Malik et al., "Impact of artificial intelligence on employees working in industry 4.0 led organizations", International Journal of Manpower, vol. 43, no. 2, 2022, pp. 334–354, doi: 10.1108/IJM-03-2021-0173.
[30] W. Puriwat and S. Tripopsakul, "Preparing for Industry 4.0 - Will youths have enough essential skills?: An Evidence from Thailand", International Journal of Instruction, vol. 13, no. 3, 2020, pp. 89–104, doi: 10.29333/iji.2020.1337a.
[31] M. Hirudayaraj et al., "Soft skills for entry-level engineers: What employers want", Educ. Sci., vol. 11, no. 10, 2021, doi: 10.3390/educsci11100641.
[32] S. Hartanto et al., "Work skills factor for mechanical engineering students in vocational high school", presented at the TVET towards industrial revolution 4.0, 2020, pp. 70–79.
[33] N. Soukupová, M. Adamová, and R. Krninská, "Industry 4.0: an Employee Perception (Case of the Czech Republic)", Acta Universitatis Agriculturae Et Silviculturae Mendelianae Brunensis, vol. 68, no. 3, 2020, pp. 637–644, doi: 10.11118/actaun202068030637.
[34] P. Ifinedo, et al., "Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions", presented at the Americans Conference on Information Systems: A Tradition of Innovation, AMCIS 2017, vol. 2017., 2017.

[35] G. Sharkov et al., “Multidisciplinary Approach to Industry Standards in the IT Higher Education Programs”, presented at the 2022 Information Systems and Grid Technologies, ISGT 2022, vol. 3191, 2022, pp. 51–62. [Online]. available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137175083&partnerID=40&md5=d62f8ec2fd505f9436ba205777a951b3

[36] L. Moldovan, L. Moldovan, and A. Gligor, “State-of-the-art Analysis on the Knowledge and Skills Gaps on the Topic of Industry 4.0 and the Requirements for Work-based Learning”, presented at the 12th International Conference Interdisciplinarity in Engineering, vol. 32, 2019, pp. 294–301. doi: 10.1016/j.promfg.2019.02.217.

[37] N. Obermayer, T. Csizmadia, and D. Hargitai, “Influence of Industry 4.0 technologies on corporate operation and performance management from human aspects”, Meditari accountancy research, vol. 30, no. 4, 2022, pp. 1027–1049, doi: 10.1108/MEDAR-02-2021-1214.

[38] N. Obermayer, T. Csizmadia, and Z. Banasz, “Companies on Thin Ice Due to Digital Transformation: The Role of Digital Skills and Human Characteristics”, International and Multidisciplinary Journal of Social Sciences, vol. 11, no. 3, 2022, pp. 88–118, doi: 10.17583/rimcis.10641.

[39] S. Von Solms and L. A. Futcher, “Adaption of a Secure Software Development Methodology for Secure Engineering Design”, IEEE Access, vol. 8, 2020, pp. 125630–125637, doi: 10.1109/ACCESS.2020.3007355.

[40] J. Sanchez et al., “An Integral Pedagogical Strategy for Teaching and Learning IoT Cybersecurity”, Sensors, vol. 20, no. 14, 2020, doi: 10.3390/s20143970.

# DANGERS OF SMART DEVICES | AZ OKOSESZKÖZÖK VESZÉLYEI

MANDIĆ Dorottya[1]

**Abstract**

Smart devices have become part of our everyday life. We can hardly imagine our daily lives without our smart devices. However, you can hear more and more that the use of smart devices can be dangerous. Many of the users buy the given smart device with only basic knowledge of how to use it safely these devices. In addition, manufacturers often prioritize profit over safety. This study shows, some of the dangers that smart devices can cause, and which are the most popular smart devices.

**Keywords**

smart devices, Internet of Things, dangers, security, IoT

**Absztrakt**

Az okoseszközök a mindennapi életünk részévé váltak. Szinte már el sem tudjuk képzelni a mindennapi életünket az okoseszközeink nélkül. Egyre többet lehet hallani arról, hogy az okoseszközök használata veszélyekkel járhat. Ezen kívül a felhasználók sokan úgy vásárolják meg az okoseszközöket, hogy még csak alapvető ismeretekkel sem rendelkeznek arról, hogy hogyan tudnák biztonságosan használni. A gyártók is sokszor előtérbe helyezik a haszon szerzést a biztonság helyett. A tanulmány bemutatja az egyes veszélyeket, melyeket az okoseszközök használata okozhat, valamint, hogy melyek a legnépszerűbb okoseszközök.

**Kulcsszavak**

okoseszközök, dolgok internete, veszélyek, biztonság, IoT

[1] mandic.dorottya@uni-obuda.hu | ORCID: 0000-0002-3384-5590 | PhD Student, Óbuda University Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETŐ

A „dolgok internete vagy angolul az Internet of Things (IoT)" kifejezést egyre többet lehet hallani. [40] Az IoT eszközöknek a száma rohamosan nő világszerte, és jelenleg megközelítőleg 15 milliárd IoT eszköz van jelen, ami várhatóan 2030-ra elfogja érni a 29 milliárd IoT eszközt. Az IoT eszközöknek a száma évről évre növekedni fog, és 2030-ra várhatóan Kínában lesz a legtöbb IoT eszköz. [1] Az IoT eszközöket már számos területen használják, és egyre több hétköznapi eszköz és tárgy is csatlakozik az internetre. [2] A felhasználók körében az okoseszközök egyre népszerűbbek. A Huawei Technologies Hungary felmérése szerint a magyar felhasználók körében az okoseszközök rendkívül népszerűek, és egyre többen használják az okoseszközeiket például a sportoláshoz vagy az egészségügyi funkciók méréséhez. [3] A felmérés szerint az emberek 60%-a például az eszközök által mért értékek alapján orvoshoz fordulna. [5] Az eNet 2018-ban végzet kutatása szerint például minden tizedik felnőtt internetező Magyarországon használ már okosórát vagy okoskarkötőt. [6] Az INNObyte 2021-ben végzett kutatása szerint a felhasználók egyre többen használnak okoseszközöket az otthonaikban. [4] Egyre többet lehet hallani arról is, hogy mennyire sérülékenyek az IoT eszközök biztonsági szempontból, és hogy a gyártók sokszor előtérbe helyezik a haszon szerzést, és a gyors megjelenítést a biztonság helyett. A Gemalto biztonsági vállat 2017-es felmérése szerint, az IoT eszköz gyártók, és szolgáltatók a költségvetésükből csak a 11%-át költik az IoT eszközök biztonságára. Ezen kívül a felhasználók 90%-a nem bízik az okoseszközök biztonságában. Az egyik fő aggodalom, hogy a hackerek átvehetik az irányítást az eszközeik felett. A felmérésben résztvevők mindössze 14%-a válaszolta, hogy megfelelően tájékozódott az IoT eszközök biztonságát illetően. [7] Az okoseszközöknek a használata számos előnnyel jár a mindennapi életben, hiszen segítik a mindennapi tevékenységeink elvégzését, az egészségünket is figyelemmel tudjuk kísérni a használatuk által, otthonunkat is kényelmesebbé, jobbá és biztonságosabbá tehetjük, ez mellett még számos előnye van annak, ha okoseszközöket használunk. A gyártók felelőssége fontos szerepet játszik az IoT eszközök biztonságában, de sajnos a biztonság sokszor háttérbe kerül. A felhasználóknak is fontos szerepük van az okoseszközök biztonságos használatában, viszont sokan még csak alapvető ismeretekkel sem rendelkeznek, hogy biztonságosan tudják használni ezeket az eszközöket. [9] Az IoT eszközökkel kapcsolatban az egyik aggodalmat az internetre csatlakoztatott eszközöknek a száma jelenti, valamint a sebezhetőség, amit a bűnözök kihasználhatnak. Ezen kívül az IoT eszközök hatalmas mennyiségű adatokat generálnak, ez által fennáll annak a veszélye is, hogy illetéktelen személyek hozzáférhetnek ezekhez az adatokhoz. [8]

### Okoseszközök népszerűsége

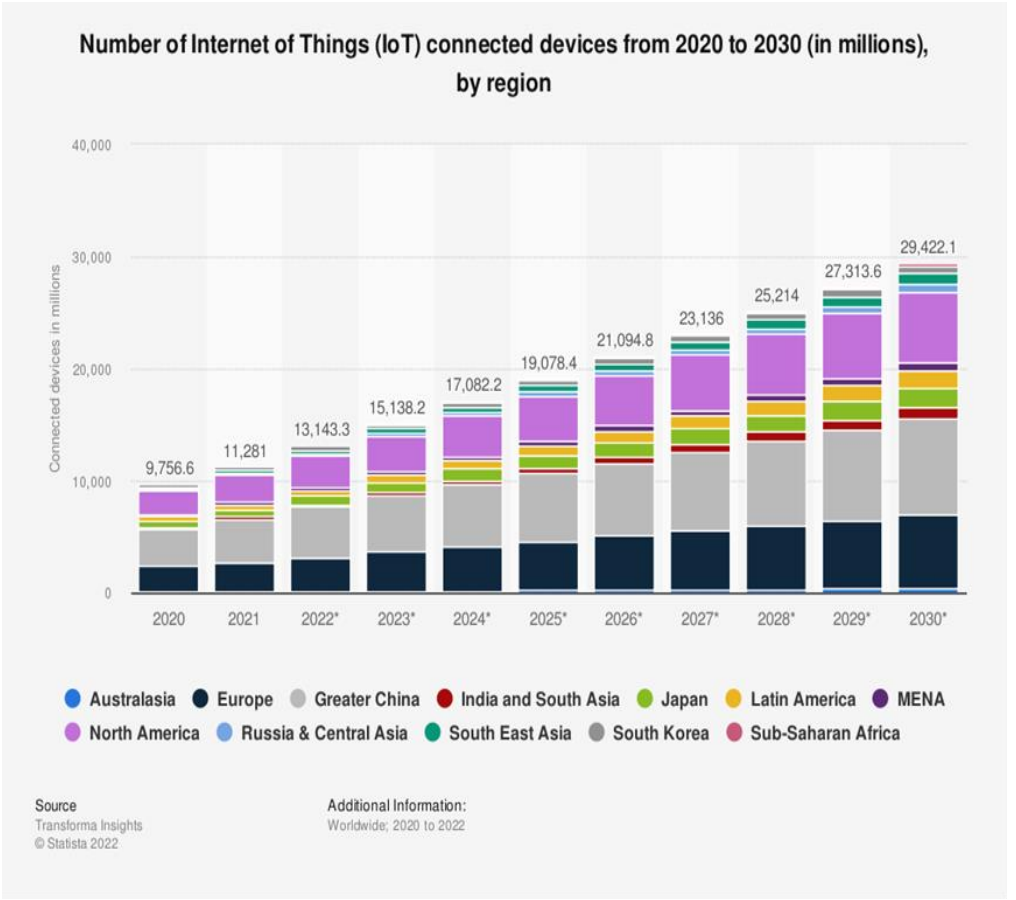
Manapság már szinte mindenki használ legalább egy okoseszközt például okostelefont. A Statista jelentése szerint 2019 és 2020 között jelentősen megnőt világszerte a csatlakoztatott hordozható eszközöknek a száma. [27] 2021-ben az eNet felmérése szerint Magyarországon 6,2 millióan használnak okostelefont. [10] Az okosóra is igen népszerű a felhasználók körében, hiszen lehetőség van az okosórán keresztül beszélni, üzeneteket küldeni és fogadni, a mozgást és a pulzust, valamint az alvás változásait is figyelemmel tudjuk kísérni. [11] A Huawei Technologies Hungary 2021-ben készített felmérést, melyben közel 8000 ezer válaszadó vett részt. A felmérésben azt vizsgálták, hogy mennyire népszerűek a különféle okoseszközök a magyarok körében, és hogy vásárláskor, melyek a legfontosabb

szempontok, amit figyelemmel vesznek, illetve, hogy milyen funkcióra használják az okoseszközöket. A válaszok alapján „63%-a visel okosórát vagy okoskarkötőt, 54%-a rendelkezik vezeték nélküli fülhallgatóval, 12%-a rendelkezik okosmérleggel vagy vérnyomásmérővel, és 15%-a válaszolta, hogy nem használ semmilyen okoseszközt.” A válaszok alapján, ami a vásárlást illeti a legfontosabb szempontok közé tartozik a hosszú üzemidő, ár, és a kényelem. [14]

*1. Ábra: Okoseszközök. (forrás:https://www.jtsec.es/iot-cybersecurity )*

A Samsung is végzett kutatást 2021-ben az Impetus Research által, melyben 815 válaszadó vett részt 18 és 64 év között. A felmérésben a magyar emberek otthonaikban használt okoseszközeik használatát vizsgálták. A felmérés szerint a járvány ideje alatt sokan vásároltak új okoseszközöket, és legtöbben a válaszadók közül okostelefont vásároltak. [15] Az INNObyte 2021-es felmérése szerint a válaszadók 83%-a rendelkezik otthonában okoseszközzel. A válaszadók 32%-a válaszolta azt, hogy azért vásárolt okoseszközt, mert fontos számára a kényelem, 17%-a szórakozás miatt vásárolt okoseszközt, és a 14%-a az energiamegtakarítás véget. A válaszadók 93%-a szerint előnyös, ha otthonában vannak okoseszközök, 82%-a szerint kényelmes a használatuk, és megkönnyítik a mindennapi életet az okoseszközök használata, 49%-a pedig azt válaszolta, hogy időmegtakarítást ért el az okoseszközök használata által. Azok a válaszadók, akik azt válaszolták, hogy nem rendelkeznek okoseszközökkel anyagi, valamint biztonsági okokkal indokolták. Egyes felhasználók például veszélyt látnak abban, hogy otthonaikban okoseszközöket használjanak. [4] 2022-ben a Deloitte végzett felmérést a digitális fogyasztói trendekről, melyben 36 ezer felhasználó vett részt világszerte, és 1000 Magyarországon. A 18 évestől az 54 éves kor-

osztály a legnagyobb érdeklődést az okostelefonok iránt mutatta. [12] A Reviews.org felmérése, mely szintén 2022-ben készült a 18 éves vagy ennél idősebb amerikaiak válaszai alapján a legnépszerűbb okoseszközök a személyes használatra az okostelefon, okosóra, és a tablet. Az otthonukban használt okoseszközök közül pedig a legnépszerűbbek például a hangszórók, tévék, hűtők, okoscsengők, biztonságkamerák és zárak. [13] A Digital Trends 2023-ban a legjobb otthoni okoseszközök közé sorolta a következőket ezekből néhányat megemlítenék például a hangasszisztens, biztonsági kamera, termosztát, robotporszívó. [17] A Statista szerint az IoT eszközöknek a száma várhatóan 2030-ban Kínában lesz a legnagyobb, majd ezt fogja követni Európa és Észak Amerika. [18]




*2. Ábra: Az IoT eszközök száma területek szerint 2020-tól 2030-ig.*
*(forrás:https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/ )*

## Okoseszközök veszélyei

Az okoseszközök használatának számos előnye van, de ez még nem jelenti azt, hogy ezeknek az eszközöknek a használata biztonságos is. Az utóbbi időben egyre többet lehet hallani arról, hogy az okoseszközeinken keresztül például megfigyelhetik a szokásainkat, vagy ellophatják a személyes adatainkat. A tömeggyártásban alacsony költségvetés-

ből készült eszközök következménye lehet, hogy gyenge biztonsági megoldásokat tartalmaznak. [19] Az IoT eszközök az otthonokban adatokat gyűjthetnek arról, hogy például a felhasználók mikor tartózkodnak otthon, vagy hogy milyen fogyasztási szokásai vannak. [22] Az IoT eszközök sérülékenyek lehetnek, melyeket a támadók kihasználhatnak, és az utólagos javítást nem egyszerű elvégezni. [20] Az OWASP (Open Web Application Security Project) az IoT Sérülékenységek Projektje szerint a legfontosabb IoT sérülékenységek közül néhányat megemlítenék például gyenge jelszavak, gyenge titkosítás, hiányzó frissítési mechanizmus. [21] Az IoT eszközök esetében gyakori, hogy gyenge jelszavakat alkalmaznak, és nem mindegyik gyártó kötelezi például a felhasználót, hogy módosítsa a készülék alapértelmezett jelszavát. [30] Ezért fontos, hogy elvégezzük az alapvető biztonsági beállításokat, ami azt jelenti, hogy az alapértelmezett felhasználónevet, és jelszót meg kell változtatni. Ez azért fontos, mert a megvásárolt eszközök esetében ezek azonosak lehetnek. A felhasználónév, és a jelszó kiválasztásakor például fontos figyelembe venni, hogy olyat válasszunk, ami nem található ki könnyen. Ez mellett az is fontos, hogy tartalmazzon számokat, valamint speciális karaktereket, és a hosszúságra is fontos figyelni. [31] A NordVPN felmérést végzett hét országban az IoT eszközök biztonságát illetően. Az országok között szerepelt Németország, Egyesült Államok, Ausztrália, Kanada, Franciaország, Hollandia és Nagy Britannia. A legrosszabb helyre az országok közül az IoT biztonságát illetően Nagy Britannia került, mivel a felmérésből kiderült, hogy legkevesebb intézkedést az eszközeik biztonsága érdekében a vizsgált országok közül Nagy Britanniában teszik. A többi országhoz képest, Nagy Britanniában a válaszadók 95%-a válaszolta, hogy rendelkezik legalább egy okoseszközzel, és 24%-a azt válaszolta, hogy egyáltalán nem tesz semmilyen intézkedést az eszközök védelme érdekében. A hét ország közül a válaszok alapján a legkevesebb IoT eszközzel Franciaország rendelkezik. A felmérésben résztvevők 41.4%-a gondolja úgy, hogy a gyártóknak kellene felelőséget vállalnia a biztonságért, 55.9%-a szerint a felhasználók felelőssége lenne, még a válaszadók 45.3%-a úgy gondolja, hogy az internetszolgáltatók felelősége lenne. [35] [36] [37] 2013-ban egy LG okostévével rendelkező felhasználó fedezte fel, hogy az okostévéje adatokat gyűjt a nézési szokásairól, akkor is, ha ez a funkció ki van kapcsolva. A Samsung okostévénél történt már olyan esett, hogy az okostévé beszédfelismerő funkciója személyes beszélgetéseket rögzített. [26] Mivel az okostévé rendelkezhet beépített kamerával, mikrofonnal, valamint hangfelismeréssel, ez által megfigyelhetik a beszélgetéseinket, és felvétel is készülhet róla. [23] 2019-ben az FBI hatósági közleményt adott ki az okostévékkel kapcsolatban, melyben felhívták a figyelmet, hogy az okostévék gyártója vagy a telepített alkalmazások fejlesztői az okostévén keresztül megfigyelhetik a felhasználókat. A Samsung például jelezte a felhasználóknak, hogy kerüljék a személyes beszélgetéseket az okostévék előtt, ha nincs kikapcsolva a hangvezérlő funkció. A Northeastern University, valamint az Imperial College London szerint a gyártók, mint például a Samsung vagy az LG, illetve az Apple okostévéi a felhasználók bizonyos adatait kiadják harmadik félnek. A kiberbűnözők pedig a haszonszerzés céljából akár az okostévé kamerája és mikrofonja által felvételeket készíthet. [28] 2019-ben az Amazon Echo valamint a Google Home okosrendszerről derült ki, hogy adatvédelmi szempontból ezek az eszközök sokkal több adatot gyűjtenek össze, mint amire lett volna például engedélyük, hiszen olyan információkat is rögzítettek, melyeket a tulajdonos nem szeretett volna megosztani. A Philips Hue okosvillanykörtéről is kiderült, hogy könnyen feltörhető, és mivel Kínában készül-

nek, így nehéz elkerülni, hogy ne legyenek sérülékenyek. [23] Az Amazon Ring otthonokban használt biztonsági rendszerről például kiderült, hogy adatokat oszt meg a Google, valamint a Facebookkal. A Roomba robotporszívó igen népszerű a felhasználók körében, viszont a kutatók az feltételezik erről a robotporszívóról, hogy a Lidar technológiát használva térérzékeléshez kifejlesztett lézeres letapogatóval képes hangot érzékelni. [24] 2018-ban az ESET figyelmeztetést adott ki, hogy a Dongguan Diqee 360 robotporszívóban biztonsági hiányosságokat fedeztek fel a szakértők, és mivel rendelkezik 360 fokos kamerával, abban az esetben, ha a támadók feltörnék, teljes képet kapnának otthonunkról. [25] Egyes okoseszközök nem csak megkönnyítik a mindennapi életünket, de a biztonságunkról is gondoskodik, mint például a biztonsági kamera. A felhasználók körében igen népszerűek, hiszen a kamera segítségével megfigyelhetjük például az otthonunkat, akkor is, ha nem tartózkodunk otthon. Az olcsó IP kamerák, amik az otthonunk megfigyelésére szolgálnak sajnos az egyik legtöbbet feltört eszközök közé tartoznak. Volt már olyan esett, hogy egy nagyobb kínai gyártónak az eszköze képeket osztott meg idegen otthonokról a többi felhasználóval. [29] A Nemzeti Kibervédelmi Intézet 2023-ban közzétette, hogy sebezhetőségeket találtak az olasz, valamint a brit kutatók a népszerű TP-Link Tapo L530E okosizzóban. Ez az okosizzó igen népszerű, és megvásárolható például Amazonon is. [16]

## ÖSSZEGZÉS

Az okoseszközök egyre népszerűbbek a felhasználók körében, és egyre többen vásárolnak már ilyen eszközöket. Legtöbben a kényelem, a szórakozás, az időmegtakarítás vagy az otthonuk biztonsága, illetve az egészségi állapotuk nyomon követese miatt vásárol okoseszközt. A felhasználók többsége rendelkezik okoseszközzel, és hasznosnak tartja ezeknek az eszközöknek a használatát. Viszont vannak olyan felhasználók, akik veszélyt látnak az okoseszközök használatában, és nem bíznak a biztonságukban. A felhasználók közül, akik okoseszközöket használnak sokan nem rendelkeznek alapvető ismeretekkel sem, hogy biztonságosan tudják használni az okoseszközeiket vagy egyáltalán nem tesznek semmilyen intézkedést az eszközök védelme érdekében. A gyártók pedig sokszor nem helyezik előtérbe a biztonságot. A jövőben várhatóan még több hétköznapi eszköz és tárgy fog csatlakozni az internetre. 2022-ben az Európai Bizottság nyilvánosságra hozta a kiberrezilienciáról szóló törvényjavaslatot (Cyber Resilience Act). A törvényjavaslat kiberbiztonsági szabályokat vezetne be a digitális elemeket tartalmazó termékek gyártói, és fejlesztői számára, és lehetővé tenné, hogy a termékek vásárlói megfelelő tájékoztatást kapjanak az általuk vásárolt, és használt termékek kiberbiztonságáról. A törvényjavaslat szerint „a gyártóknak felelőséget kell majd vállalniuk a termékeik sérülékenységeiért a teljes életciklus alatt.” [32] [33] [34] [39] A törvényjavaslat „minden olyan termékre alkalmazandó lesz, amely közvetlenül vagy közvetve csatlakozik egy másik eszközhöz vagy hálózathoz.” A tagállamok 2023-ban „megállapodtak a digitális termékekre vonatkozó biztonsági követelményekre irányuló közös álláspontról.” [38]

## FELHASZNÁLT IRODALOM


[1] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 [Online]. Elérhető: https://www.statista.com/statistics/1183 457/iot-connected-devices-worldwide/ (Letöltve:2023.07.28)

[2] Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018.

[3] Kutatás: Már a magyarok kétharmada visel okoseszközt a csuklóján [Online]. Elérhető: https://consumer.huawei.com/hu/press/news/2021/news-210304/ (Letöltve:2023.07.28)

[4] Egyre többen használnak okoseszközöket otthonukban - INNObyte kutatás [Online]. Elérhető:https://innobyte.hu/egyre-tobben-hasznalnak-okoseszkozoket-otthonukban-innobyte-kutatas/ (Letöltve:2023.07.28)

[5] Az okoseszközök előnye a folyamatos egészségmonitoring [Online]. Elérhető: http://medicalonline.hu/informatika/cikk/az_okoseszkozok_elonye_a_folyamatos_egeszseg-monitoring (Letöltve:2023.07.30.)

[6] Egészségtudatosabbak az okosórák, és okoskarkötők hazai használói [Online]. Elérhető: https://enet.hu/egeszsegtudatosabbak-az-okosorak-es-okoskarkotok-hazai-hasznaloi/ (Letöltve:2023.07.30.)

[7] Gemalto survey confirms that consumers lack confidence in IoT device security [Online]. Elérhető: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/press-release/gemalto-survey-confirms-that-consumers-lack-confidence-in-iot-device-security- (Letöltve:2023.08.01.)

[8] Az IoT eszközök veszélyei [Online]. Elérhető: https://mernoknok.hu/az-iot-eszkozok-veszelyei/(Letöltve:2023.08.01.)

[9] Mandic Dorottya, Simon János: Biztonságossak-e az okosotthonokban használt okoseszközök? Biztonságtudományi Szemle, 4. évf. 4. szám 59-67 (2022)

[10] A plafont súrolja a hazai okostelefon használat [Online]. Elérhető: https://enet.hu/a-plafont-surolja-a-hazai-okostelefon-hasznalat/ (Letöltve:2023.08.03.)

[11] Okoseszközök térhódítása [Online]. Elérhető: https://www.smartos.hu/blog/okoseszkozok-terhoditasa-64 (Letöltve:2023.08.05.)

[12] Digitális Fogyasztói Trendek 2022 [Online]. Elérhető: https://www2.deloitte.com/content /dam/Deloitte/hu/Documents/technology/Digitalis_Fogyasztoi_Trendek_Felmeres_Magyarorszag_2022.pdf (Letöltve:2023.08.08.)

[13] The most popular Smart Home Devices 2022 [Online]. Elérhető: https://www.reviews.org/home-security/most-popular-smart-home-device-statistics/ (Letöltve:2023.08.08.)

[14] Kutatás már a magyarok kétharmada visel okoseszközt a csuklóján [Online]. Elérhető: https://huawei.hu/2021/03/04/kutatas-mar-a-magyarok-ketharmada-visel-okoseszkozt-a-csuklojan/ (Letöltve:2023.08.11.)

[15] Sok az új okoseszköz a magyar háztartásokban, de a bevásárlólista még nem üres [Online]. Elérhető:https://www.samsung.com/hu/news/local/sok-az-uj-okoseszkoz-a-magyar-haztartasokban-de-a-bevasarlolista-meg-nem-ures/ (Letöltve:2023.08.13.)

[16] A támadók TP-LINK okosizzókon keresztül képesek megszerezni jelszavainkat [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/a-tamadok-tp-link-okosizzokon-keresztul-kepesek-megszerezni-jelszavainkat/ (Letöltve:2023.08.25.)

[17] The best smart home devices for 2023 [Online]. Elérhető: https://www.dig italtrends.com/home/best-smart-home-devices/ (Letöltve:2023.08.26.)
[18] Number of Internet of Things (IoT) connected devices from 2020 to 2030 (in millions), by region, [Online]. Elérhető: https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/ (Letöltve:2023.08.26.)
[19] Dr. Albert Ágota, Üveges András József: Az IoT eszközök biztonsága a személyes adatok tükrében [Online]. Elérhető: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf (Letöltve:2023.08.27.)
[20] Mit tudnak rólunk okoseszközeink? [Online]. Elérhető: https://ikron.hu/okoseszkozok-veszelye/ (Letöltve:2023.08.27.)
[21] Kovács László: A kibertér védelme, Dialóg Campus Kiadó, Budapest, 2018
[22] Eszteri Dániel: Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás [Online]. Elérhető: http://real.mtak.hu/133906/1/eszteri.daniel.uj.technologiak.adatvedelem.pdf (Letöltve:2023.08.27.)
[23] Kémkedő eszközök [Online]. Elérhető: https://itlawpro.com/hu/adatvedelem/kemkedo-eszkozok (Letöltve:2023.08.28.)
[24] Az okoseszközök veszélyei a porszívó is kémkedik? [Online]. Elérhető: https://zero itlab.com/hu/blog/az-okos-eszkozok-veszelyei-porszivo-kemkedik (Letöltve:2023.08.28.)
[25] Veszélyben vannak a hálózatba kapcsolt eszközeink? [Online]. Elérhető: https://www.eset.com/hu/hirek/milyen-veszelyek-leselkednek-a-halozatba-kapcsolt-eszkozeinkre/ (Letöltve:2023.08.28.)
[26] Az okos eszközök veszélyei – Lehet, hogy a TV néz téged [Online]. Elérhető: https://crosssec.com/az-okos-eszkozok-veszelyei-lehet-hogy-a-tv-nez-teged/ (Letöltve:2023.08. 28.)
[27] Number of connected wearable devices worldwide from 2019 to 2022 [Online]. Elérhető: https://www.statista.com/statistics/487291/global-connected-wearable-devices/ Letöltve:2023.08.28.)
[28] Milyen tévéje van otthon? Figyelmeztetést adott ki az FBI [Online]. Elérhető: https://hvg.hu/tudomany/20191203_okos_tevekeszulek_lehallgatas_megfigyeles_fbi (Letöltve:2023.08.29.)
[29] Kényelmesek az okoskütyük - de elég biztonságosak is? [Online]. Elérhető: https://www.eset.com/hu/hirek/az-okoseszkozok-kenyelmesek-de-vajon-biztonsagosak-is-2020/ (Letöltve:2023.08.29.)
[30] Kanizsai Viktor: Tárgyak Internete-tárgyak bizonytalansága [Online]. Elérhető: http://www.vmtt.org.rs/mtn2016/503_513_Kanizsai.pdf (Letöltve:2023.08.29.)
[31] Tóth András: Új típusú kihívások az infokommunikációban, Ludovika Egyetemi Kiadó, Budapest, 2023
[32] Kanyarban az uniós IoT-védelmi jogszabály [Online]. Elérhető: https://www .hwsw.hu/hirek/65139/europaiunio-bizottsag-kiberbiztonsag-kiberreziliencia-tervezet.ht ml (Letöltve:2023.08.30.)
[33] State of the Union: EU Cyber Resilience Act - Questions & Answers [Online]. Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375(Letöltve:2023.0 5.29.)

[34] Új uniós szabályok teszik még biztonságosabbá a hardver- és szoftvertermékeket [Online]. Elérhető: https://infovilag.hu/uj-unios-szabalyok-teszik-meg-biztonsagosabba-a-hardver-es-szoftvertermekeket/ (Letöltve:2023.08.30.)
[35] A brit felhasználók negyede nem védi az okoseszközeit [Online]. Elérhető: https://iot-zona.hu/biztonsag/a-brit-felhasznalok-negyede-nem-vedi-az-okoseszkozeit (Letöltve:2023.08.30.)
[36] Research finds that 24% of Brits aren't securing their IoT devices [Online]. Elérhető: https://www.iottechnews.com/news/2021/jul/22/research-finds-that-24-of-brits-arent-securing-their-iot-devices/ (Letöltve:2023.08.30.)
[37] Almost 9/10 people have at least one IoT device [Online]. Elérhető: https://nordvpn.com/research-lab/iot-device-security/ (Letöltve:2023.08.30.)
[38] A kiberrezilienciáról szóló jogszabály: a tagállamok megállapodtak a digitális termékekre vonatkozó biztonsági követelményekre irányuló közös álláspontról [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/ (Letöltve:2023.08.31.)
[39] A kiberrezilienciáról szóló jogszabály [Online]. Elérhető: https://digital-strategy.ec.europa.eu/hu/library/cyber-resilience-act (Letöltve:2023.08.31.)
[40] Tárgyak internete [Online]. Elérhető: https://sealog.hu/tudastar/fogalomtar/targyak-internete (Letöltve:2023.09.03.)

# EVALUATING THE INTEROPERABILITY OF IOT DEVICES AND CLOUD ENVIRONMENTS IN INTELLIGENT BUILDING SYSTEMS

# AZ IOT-ESZKÖZÖK ÉS A FELHŐKÖRNYEZETEK INTEROPERABILITÁSÁNAK ÉRTÉKELÉSE INTELLIGENS ÉPÜLETRENDSZEREKBEN

SÁNDOR Barnabás[1] – RAJNAI Zoltán[2]

**Abstract**

Integrating IoT devices and cloud environments is critical to developing and designing intelligent building systems. However, ensuring interoperability poses significant challenges, including data security and standardized communication. This research assesses the interoperability of IoT devices and cloud environments in intelligent building systems. It includes a description of advanced security protocols, data protection safeguards, and standardized communication interfaces. Cloud computing for real-time processing and analysis of IoT data will be presented, facilitating intelligent decision-making and optimization of building functions.

**Keywords**

Smart Building, IoT Cloud Environment, Cybersecurity Framework, Building Management, Data Security and Privacy

**Absztrakt**

Az IoT eszközöknek és a felhő-környezeteknek az integrálása kulcsfontosságú az intelligens épület-rendszerek fejlesztéseés kialakítása szempontjából. Az interoperabilitás biztosítása azonban jelentős kihívásokat jelent, többek között az adatbiztonság és a szabványosított kommunikáció terén. Ez a kutatás az IoT-eszközök és a felhőkörnyezetek interoperabilitását értékeli az intelligens épületrendszerekben. Magában foglalja a fejlett biztonsági protokollokat, az adatvédelmet megőrző intézkedéseket és a szabványosított kommunikációs interfészek ismertetését. Bemutatásra kerül a felhőalapú számítástechnika az IoT-adatok valós idejű feldolgozásához és elemzéséhez, megkönnyítve az intelligens döntéshozatalt és az épületfunkciók optimalizálását.

**Kulcsszavak**

Intelligens épület, IoT felhőkörnyezet, Kiberbiztonsági keretrendszer, Épületüzemeltetés, Adatbiztonság

[1] sandor.barnabas@gmail.com | ORCID: 0000-0001-7133-8082 | PhD-student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | dean, professor, Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering| dékán, egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## BEVEZETÉS

Az IoT technológia úttörőként jelent meg, amely forradalmasította a mindennapi életünk számos aspektusát, beleértve az épületek üzemeltetését és felhasználását. Az intelligens épületrendszerek, amelyek számos IoT-eszközzel, például érzékelőkkel, működtető elemekkel és beágyazott rendszerekkel vannak felszerelve, megkönnyítik az adatok valós idejű gyűjtését, feldolgozását és elemzését, lehetővé téve az intelligens döntéshozatalt és az épületfunkciók optimalizálását. Ehhez elengedhetetlen, hogy a felhőkörnyezetek biztosítsák a szükséges infrastruktúrát az IoT-eszközök által generált hatalmas mennyiségű adat tárolásához, feldolgozásához és elemzéséhez, ezáltal fokozva az intelligens épületrendszerek képességeit.

Az IoT-eszközök és a felhőkörnyezetek intelligens épületrendszerekbe való integrálása összetett feladat, amely jelentős kihívásokat jelent informatikai, kiberbiztonsági és műszaki szempontból is. A legkritikusabb kihívás az interoperabilitás, az kiberbiztonság és az adatvédelem biztosítása. Az interoperabilitás létfontosságú a különböző IoT-eszközök és felhőkörnyezetek közötti zökkenőmentes kommunikáció és interakció lehetővé tételéhez. Ez teszi lehetővé az eszközök és rendszerek egységes működését az intelligens épületrendszerekben. Az adatbiztonság és a magánélet védelme szintén kulcsfontosságú, mivel az IoT-eszközök által gyűjtött és feldolgozott adatok érzékenyek. Az intelligens épületrendszerekbe vetett bizalom megteremtése megköveteli ezen adatok biztonságának és adatvédelmének biztosítását.

E kutatásnak célja volt az IoT-eszközök és a felhőkörnyezetek interoperabilitásának értékelése az intelligens épületrendszerekben, miközben az kiberbiztonság és az adatvédelem kritikus kihívásaira fókuszálni. Egy komplex rendszer foglalja a fejlett biztonsági protokollokat, a magánélet védelmét szolgáló mechanizmusokat és a szabványosított kommunikációs interfészeket. A tanulmány fókusza a felhőalapú számítástechnika az IoT-adatok valós idejű feldolgozása és elemzése, megkönnyítve az intelligens döntéshozatalt és az épületfunkciók optimalizálását.

## INTEROPERABILITÁSI KIHÍVÁSOK AZ INTELLIGENS ÉPÜLETRENDSZEREKBEN

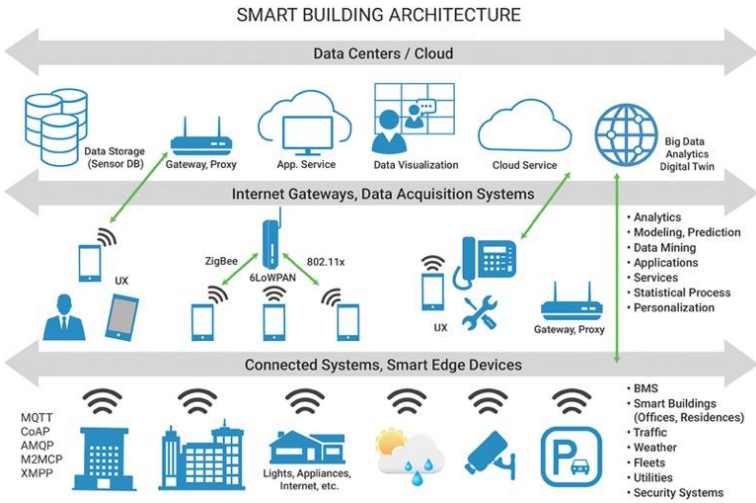
A dolgok internetétének megjelenése a különböző ágazatok kiterjedt integrációját eredményezte, ami az átalakító intelligens technológiák korszakát jelzi. Ennek a trendnek egyik jelentős haszonélvezője az építőipar. Ebben a részben Az intelligens épületek és az IoT kapcsolatának kölcsönhatását vizsgáltuk. Az intelligens épületek a modern építési gyakorlatok megtestesítői, amelyek fejlett technológiákat használnak az energiahatékonyság, a kényelem és az épület általános irányításának javítására. Működésükben központi szerepet játszik az IoT - egy olyan innovatív technológia, amely megkönnyíti az összekapcsolt eszközök közötti adatcserét. [1]

Az IoT integrálása az intelligens épületekbe a technológia és a szerkezeti tervezés érdekes keverékét kínálja, olyan intelligens szerkezeteket hozva létre, amelyek önállóan alkalmazkodnak a környezeti feltételekhez és a felhasználói igényekhez. Célünk ebben a részben megvilágítaani ezeket a fogalmakat, részletes betekintést nyújt az intelligens épületek és az IoT meghatározásába, szinergikus működésükbe, valamint a mai digitális korban rejlő forradalmi lehetőségekbe.

Az átjárhatóság az intelligens épületrendszerek egyik legfontosabb szempontja, amely lehetővé teszi a különböző eszközök és rendszerek zökkenőmentes együttműködését. Az intelligens épületrendszerek interoperabilitásának megvalósítása azonban számos kihívást jelent.

**Eszközök az intelligens épületeken belül**

Az intelligens épületrendszerekben különböző eszközöket, például érzékelőket, (fény, $CO_2$, levegőminőség), működtetőket (ablaknyitó) és vezérlőket használnak, és az egyes eszközök különböző kommunikációs protokollokat, adatformátumokat és interfészeket használhatnak. ***(1. Ábra)*** Ez a heterogenitás megnehezíti a különböző eszközök és rendszerek egységes és működőképes épületirányítási rendszerbe történő integrálását. Emellett számos gyártó saját megoldásokat kínál az intelligens épületrendszerekhez, amelyek nem feltétlenül kompatibilisek más gyártók eszközeivel és rendszereivel. Ez a gyártóspecifikus megközelítés akadályozza az interoperabilitást, mivel a gyártóhoz való kötődéshez vezet, és csökkenti az épületirányítási rendszer rugalmasságát. [2]




*1. Ábra: Okos Épület IoT architecktúra, powersystemsdesign.com*

**Felhőkörnyezetek az intelligens épületekben**

A felhőkörnyezetek kulcsfontosságúak az intelligens épületrendszerekben, mivel platformot biztosítanak az adatok tárolásához, feldolgozásához és elemzéséhez. Az IoT-eszközök felhőkörnyezetekkel való integrálása azonban számos kihívást jelent, beleértve az kiberbiztonságot, az adatvédelmet és az interoperabilitást. A felhőszolgáltatók különböző adatformátumokat, API-kat és kommunikációs protokollokat használhatnak, ami kihívás elé állítja az IoT-eszközök integrálását a felhőkörnyezetekkel. Az IoT-eszközök és a felhőkörnyezetek közötti adattovábbítás során jogi, biztonsági és adatvédelmi aggályok is felmerülhetnek. [3]

**Az IoT-eszközök és a felhőkörnyezetek integrációjának kihívásai**

Az IoT-eszközök és a felhőkörnyezetek intelligens épületrendszerekbe történő integrálása több problémát vet fel. Első sorban az intelligens épületrendszerek kommunikációs protokolljai és interfészei nincsenek szabványosítva. Bár több szabványügyi szervezet,

például a Nemzetközi Szabványügyi Szervezet (ISO), a Nemzetközi Elektrotechnikai Bizottság (IEC) és az épületautomatizálási és vezérlőhálózatok (BACnet) szabványokat dolgozott ki az épületautomatizálási rendszerek kommunikációjára, ezek a szabványok nincsenek általánosan elfogadva. Másodsorban a biztonság az átjárhatóság másik jelentős problémája. A különböző eszközök és rendszerek integrálása biztonsági résekkel járhat, mivel az egyes eszközök és rendszerek eltérő biztonsági jellemzőkkel és sebezhetőségekkel rendelkezhetnek.

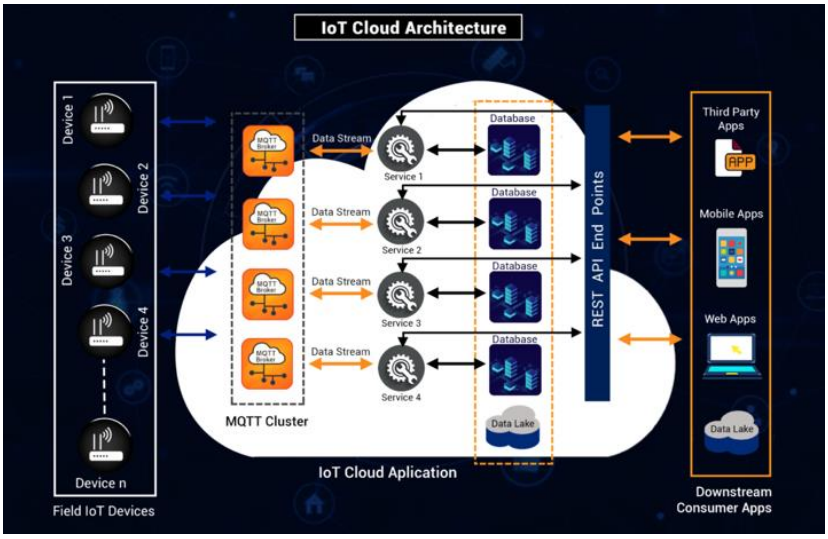
2022-ben az Európai Unióban 2022/2555 irányelvként megjelent a NIS2, melynek célja a kiberbiztonság növelése az alapvető szolgáltatók körében, a kiberbiztonság ésszerűsítése szigorúbb biztonsági követelmények és a jogsértésekért kiszabható szankciók révén, valamint az EU kibertámadásokkal szembeni felkészültségének javítása. Ebbe beletartoznak az IoT eszközök is. [4]

E kihívások kezelése érdekében ajánlott szabványosított kommunikációs protokollok és interfészek, például a BACnet, a KNX vagy a Zigbee használata, amelyek közös platformot biztosítanak a különböző eszközök és rendszerek kommunikációjához és integrálásához. Emellett fontos figyelembe venni a különböző eszközök és rendszerek integrációjának biztonsági vonatkozásait, és megfelelő biztonsági intézkedéseket kell végrehajtani az épületirányítási rendszer biztonságának és integritásának biztosítása érdekében.

## AZ IOT-FELHŐKÖRNYEZET VÉDELME AZ INTELLIGENS ÉPÜLETEKBEN

Az IoT elterjedése forradalmasította az épületüzemeltetést, így a hagyományos épületeket intelligens, energiahatékony és felhasználóbarát környezetté alakította át. Az egymással összekapcsolt IoT-eszközökkel felszerelt intelligens épületek megkönnyítik a különböző épületfunkciók, például a világítás, fűtés, szellőzés, légkondicionálás (HVAC), biztonság és energiagazdálkodás valós idejű felügyeletét, vezérlését, így az energiahatékonyság optimalizálását. [5] A felhőkörnyezetek és az intelligens épületekben lévő IoT-eszközök integrálása lehetővé teszi az ezen eszközök által generált hatalmas mennyiségű adat tárolását, feldolgozását és elemzését, ezáltal javítva az épületirányítási rendszerek képességeit. [6]

Az IoT-eszközök és a felhőkörnyezetek intelligens épületekbe történő integrálása azonban jelentős kihívásokat jelent a kiberbiztonság, jog és a műszaki megvalósítások terén. Az IoT-eszközök által gyűjtött és feldolgozott adatok érzékeny jellege miatt széleskörű intézkedésekre van szükség a titkosság, integritás és rendelkezésre állás (CIA-követelmények) biztosítása érdekében. [7] A ***2. Ábrán*** látható, hogy az egyes rendszerek közötti kommunikácó és szeparáció mekkora szerepet játszik a kiberbiztonág területén. Továbbá az intelligens épületekben a különböző eszközök és rendszerek interoperabilitása aggályokat vet fel a kommunikációs interfészek és protokollok szabványosításával kapcsolatban.




*2. Ábra: IoT Felhő architecktóra, www.embitel.com*

E kihívások kezelése érdekében fejlett biztonsági protokollok, adatvédelem, megőrző mechanizmusokat és szabványosított kommunikációs interfészeket kerülnek bemutatásra. Továbbá kiemelésker került az adatbiztonság és az adatvédelem kritikus szerepe az intelligens épületrendszerekbe vetett bizalom kiépítésében, és kiemeli a szabványosított kommunikáció fontosságát a hatékony épületirányítás szempontjából.

## Protokollok

Az IoT eszközök és az okosépületek felhőkörnyezetének integrálása adatbiztonsági szempontból megfelelő adatátviteli és titkosítási protokollokat követel meg. Tekintettel arra, hogy a feldolgozott és tárolt adatok megfeleljenek a CIA-követelményeinek. Az adatbiztonság kiemelkedő fontosságú az intelligens épületrendszerekben, mivel az IoT-eszközök által gyűjtött és feldolgozott adatok olyan érzékeny információkat tartalmazhatnak, mint például a foglaltsági minták, az energiafogyasztás és a biztonsági kamerák felvételei, felhasználók biometrikus adatai. [8] Továbbá az intelligens épületekben a különböző eszközök és rendszerek interoperabilitása aggályokat vet fel a kommunikációs interfészek és protokollok szabványosításával kapcsolatban.

- **Titkosítási protokollok**

A titkosítás az adatbiztonsági protokollok alapvető eleme. Magában foglalja az egyszerű szövegű adatok rejtjelezett szöveggé alakítását egy kriptográfiai kulcs segítségével, így azok az illetéktelen felhasználók számára értelmezhetetlenné válnak [9]. Az IoT-eszközök és a felhőkörnyezetek között továbbított adatok védelmére különböző titkosítási algoritmusok, például az Advanced Encryption Standard (AES), a Rivest Cipher (RC4) és az Data Encryption Standard (DES) alkalmazhatók. [10]

Az AES egy szimmetrikus titkosítási algoritmus, amely ugyanazt a kulcsot használja a titkosításhoz és a visszafejtéshez. Magas biztonsági szintje és számítási hatékonysága miatt széles körben használják különböző alkalmazásokban. [11] Az RC4 egy olyan folyamkódolás, amely pszeudo-véletlen bitekből álló kulcsfolyamot generál, amelyet aztán

a rejtjelezett szöveg előállítása érdekében XOR-olnak az egyszerű szöveggel. Az RC4-ről azonban kiderült, hogy számos sebezhetőséggel rendelkezik, és már nem tekinthető biztonságosnak. [12] A DES egy blokkos titkosítás, amely fix méretű blokkokban titkosítja az adatokat, de szintén nem tekinthető biztonságosnak a kis kulcsméret és a brute-force támadásokra való fogékonysága miatt. [13]

Ezért az intelligens épületekben az IoT-eszközök és a felhőkörnyezetek között továbbított adatok titkosítására az AES ajánlott. Az AES nagy biztonságot nyújt és számítási szempontból hatékony, így alkalmas az erőforrás-korlátozott IoT-eszközökhöz.

- **Hitelesítési protokollok**

A hitelesítés az adatbiztonsági protokollok másik kritikus eleme. Ez magában foglalja a felhasználó, az eszköz vagy a rendszer személyazonosságának ellenőrzését, mielőtt hozzáférést biztosítana egy erőforráshoz vagy szolgáltatáshoz. [14] Az intelligens épületek IoT-felhőkörnyezetének biztosítására különböző hitelesítési protokollok, például a PAP (Password Authentication Protocol), a CHAP (Challenge Handshake Authentication Protocol) és az EAP (Extensible Authentication Protocol) alkalmazhatók. [15]

A PAP egy egyszerű hitelesítési protokoll, amely a felhasználónevet és a jelszót egyszerű szövegben küldi a hálózaton keresztül. A PAP azonban a lehallgatási támadásokra való érzékenysége miatt nem tekinthető biztonságosnak. [15] A CHAP egy biztonságosabb hitelesítési protokoll, amely háromirányú kézfogást és kihívás-válasz mechanizmust tartalmaz. A kiszolgáló kihívást küld az ügyfélnek, aki egy egyirányú hash-függvény és egy megosztott titok segítségével kiszámított értékkel válaszol. [16] Az EAP egy rugalmas hitelesítési keretrendszer, amely különböző hitelesítési módszereket támogat, például token-kártyákat, intelligens kártyákat és digitális tanúsítványokat. [17]

Az EAP használata ajánlott az IoT-eszközök és a felhőkörnyezetek hitelesítésére az intelligens épületekben. Az EAP nagy biztonságot és rugalmasságot nyújt, így különböző alkalmazásokhoz és eszközökhöz alkalmas.

- **IoT-specifikus protokollok**

Az IoT-eszközök egyedi jellemzői, például az erőforráskorlátok, az időszakos kapcsolódás és a valós idejű követelmények speciális, az IoT-környezetre szabott biztonsági protokollokat tesznek szükségessé. Különböző IoT-specifikus biztonsági protokollokat fejlesztettek ki az IoT-eszközök és az intelligens épületekben lévő felhőkörnyezetekkel való kommunikációjuk biztosításának kihívásaira. [18]

**Lightweight Cryptography**

A „könnyű kriptográfia” a kriptográfia egy olyan ága, amelyet erőforrás-korlátozott eszközök, például IoT-eszközök számára terveztek. A hagyományos kriptográfiai algoritmusok, például az AES, túl számításigényesek lehetnek egyes IoT-eszközök számára, ami megnövekedett energiafogyasztáshoz és késleltetéshez vezet. [19] Könnyű kriptográfiai algoritmusokat, például a PRESENT és a SIMON-t úgy fejlesztették ki, hogy a hagyományos algoritmusokhoz hasonló szintű biztonságot nyújtsanak, de csökkentett számítási követelményekkel. [20]

A PRESENT egy erőforrás-korlátozott eszközökre tervezett, könnyű blokkos titkosítás. Blokkmérete 64 bit és 80 és 128 bit kulcsméretet támogat. A SIMON a Nemzeti Biz-

tonsági Ügynökség (NSA) által tervezett könnyűsúlyú blokkos titkosítások családja. Különböző blokkméreteket és kulcsméreteket támogat, így különböző alkalmazásokhoz alkalmas. [21]

**Biztonságos kommunikációs protokollok**

A biztonságos kommunikációs protokollok elengedhetetlenek az IoT-eszközök és a felhőkörnyezetek között továbbított adatok titkosságának, integritásának és rendelkezésre állásának biztosításához. Az IoT-eszközök számára különböző biztonságos kommunikációs protokollokat fejlesztettek ki, például a Datagram Transport Layer Security (DTLS), a Constrained Application Protocol (CoAP) és a Message Queuing Telemetry Transport (MQTT). [22]

A DTLS a Transport Layer Security (TLS) protokoll egy adatcsomag-alapú kommunikációra tervezett változata. A TLS-szel azonos szintű biztonságot nyújt, de alkalmas a IoT eszközöket tartalmazó alkalmazásokban általánosan használt User Datagram Protocol (UDP) protokollal való használatra. [22] A CoAP egy speciális webes átviteli protokoll korlátozott csomópontok és hálózatok számára. Könnyű és hatékony mechanizmust biztosít az IoT-eszközök és a felhőkörnyezetek közötti kommunikációhoz. Az MQTT egy könnyű üzenetküldési protokoll, amelyet kis érzékelők és mobil eszközök számára terveztek. Megbízható és hatékony mechanizmust biztosít az IoT-eszközök és a felhőkörnyezetek közötti kommunikációhoz.

Az intelligens épületek IoT-felhőkörnyezetének biztonságossá tételéhez könnyű kriptográfiai algoritmusok, például a PRESENT vagy a SIMON, valamint biztonságos kommunikációs protokollok, például a DTLS, a CoAP vagy az MQTT használata ajánlott. Ezek a protokollok magas szintű biztonságot nyújtanak, miközben alkalmasak az erőforrás-korlátozott IoT-eszközökhöz.

**Adatvédelmi mechanizmusok**

Az adatvédelem kiemelkedő fontosságú napjainkban, tekintettel arra, hogy az intelligens épületekben az IoT-eszközök által generált és feldolgozott adatok olyan érzékeny információkat tartalmaznak, mint a foglaltsági minták, az energiafogyasztás és a biztonsági kamerák felvételei. [23] Ezen adatok adatvédelmének biztosítása kulcsfontosságú az intelligens épületrendszerekbe vetett bizalom kiépítéséhez.

- **Az adatok anonimizálása**

Az adatok anonimizálásának célja a személyazonosításra alkalmas információk (PII) eltávolítására használnak az adathalmazokból, megnehezítve a rosszindulatú szereplők számára az adatok konkrét személyekhez való hozzárendelését. [24] Különböző adatanonimizálási technikákat, például a k-anonimitást, az L-diverzitást és a T-closeness technikát fejlesztettek ki a magánélet különböző szintű védelmének biztosítására. [25]

A K-anonimitás biztosítja, hogy az anonimizált adathalmaz minden egyes rekordja megkülönböztethetetlen legalább k-1 másik rekordtól bizonyos azonosító attribútumok tekintetében. [24] Az L-diverzitás kiterjeszti a k-anonimitást annak biztosításával, hogy az azonos azonosító attribútumokkal rendelkező rekordok minden egyes csoportja legalább l "jól reprezentált" értékkel rendelkezik az érzékeny attribútumok tekintetében. [25] A T-

closeness biztosítja, hogy egy érzékeny attribútum eloszlása az azonos azonosító attribútumokkal rendelkező rekordok bármely csoportjában közel áll a teljes adathalmazban való eloszláshoz. [26]

Ezen adatanonimizálási technikák kombinálása ajánlott az intelligens épületekben található IoT-eszközök által gyűjtött és feldolgozott adatok adatvédelmének biztosítása érdekében. Például a k-anonimitás, majd az L-diverzitás és a T-closeness alkalmazása magas szintű adatvédelmet biztosíthat, miközben megőrzi az adatok hasznosságát.

- **Biztonságos többszereplős számítás (SMPC)**

Az SMPC egy olyan kriptográfiai technika, amely lehetővé teszi, hogy több fél közösen számítson ki egy függvényt a bemeneteiken, miközben a bemeneteket titokban tartja.[27] Az SMPC különösen hasznos az intelligens épületek adatelemzésének adatvédelmére, ahol több érdekelt félnek, például az épület tulajdonosainak, bérlőinek és szolgáltatóinak együtt kell működniük az adatelemzésben anélkül, hogy felfednék egymás előtt a privát adataikat. [28]

Különböző SMPC protokollokat, például a Garbled Circuits protokollt és a Secret Sharing protokollt fejlesztettek ki, hogy különböző szintű biztonságot és hatékonyságot biztosítsanak. [27][29] A Garbled Circuits protokoll a kiszámítandó függvény torzított változatának létrehozását és a felek közötti torzított értékek cseréjét foglalja magában [27]. A Secret Sharing protokoll a bemeneteket részekre osztja és szétosztja a felek között, akik ezután részeredményeket számolnak ki a részükön, és ezeket kombinálva kapják meg a végeredményt. [29]

Az SMPC használata ajánlott az intelligens épületek adatainak adatvédelmet biztosító elemzésére. Az SMPC lehetővé teszi, hogy több érdekelt fél együttműködjön az adatelemzésben anélkül, hogy felfedné magánadatait, ezáltal növelve az intelligens épületrendszerek adatvédelmét és megbízhatóságát.

**Szabványosított kommunikáció az épületüzemeltetés számára**

A hatékony kommunikáció az épületirányítási rendszerek kritikus eleme, különösen az intelligens épületekben, amelyek számos IoT-eszközre támaszkodnak különböző funkciók, például az energiagazdálkodás, a biztonság és az épületet használók kényelme szempontjából. A szabványosított kommunikációs protokollok és interfészek elengedhetetlenek az épületirányítási rendszerek átjárhatóságának, biztonságának és hatékonyságának biztosításához. [30] Tekintettel arra, hogy más-más hatótávolságon és frekvencián működnek. ***(3. Ábra)*** Így a biztonságuk is más felkészültséget igénye.

**Vezeték nélküli kommunikáció**

A vezeték nélküli kommunikáció egyre népszerűbbé válik az épületirányítási rendszerekben a rugalmassága, a könnyű telepíthetősége és a különböző IoT-eszközökkel való integrálhatósága miatt. Az intelligens épületekben általában több vezeték nélküli kommunikációs technológiát használnak, köztük a Wi-Fi, a Bluetooth, a Zigbee, a LoRa és a KNX RF technológiákat.

- **Wi-Fi**

A Wi-Fi egy széles körben használt vezeték nélküli kommunikációs technológia, amely nagy sebességű internet- és hálózati kapcsolatokat biztosít. Általánosan használják

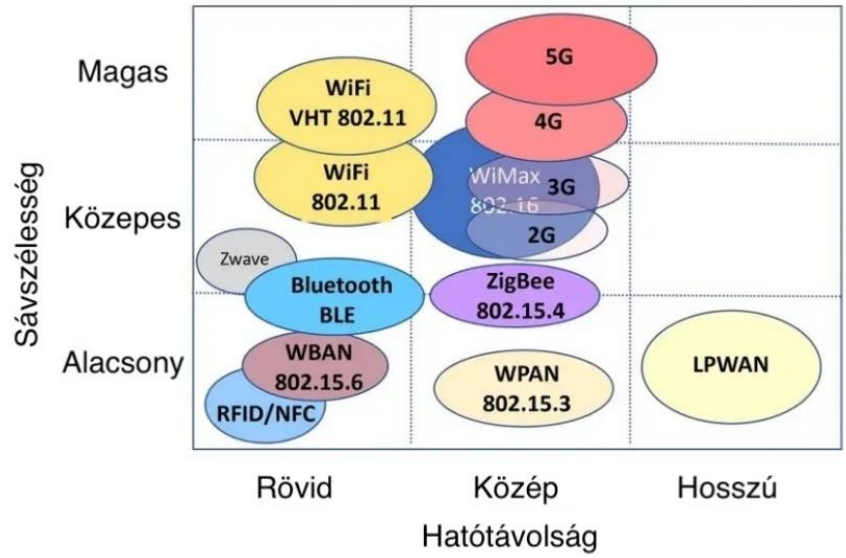
az intelligens épületekben a különböző IoT-eszközök, például érzékelők, működtetők és vezérlők épületirányítási rendszerhez való csatlakoztatására. [31]

- **Bluetooth**

A Bluetooth egy kis hatótávolságú vezeték nélküli kommunikációs technológia, amely kis területen, jellemzően legfeljebb 10 méteres körzetben csatlakoztatja az eszközöket. Általában az intelligens épületekben használják olyan eszközök, mint a termosztátok, világításvezérlők és biztonsági kamerák csatlakoztatására az épületirányítási rendszerhez. [32]

- **Zigbee**

A Zigbee egy alacsony fogyasztású, alacsony adatátviteli sebességű vezeték nélküli kommunikációs technológia, amelyet az eszközök hálós hálózatba kapcsolására terveztek. Általában intelligens épületekben használják érzékelők, működtetők és vezérlők hálós hálózatba kapcsolására, ami redundanciát biztosít és növeli a kommunikáció megbízhatóságát.[30]




*3. Ábra: Vezeték nélküli kapcsolatok összehasonlítása, saját készítésű*

- **LoRa**

A LoRa (Long Range) egy nagy hatótávolságú, kis teljesítményű vezeték nélküli kommunikációs technológia, amelyet úgy terveztek, hogy nagy távolságokra, jellemzően akár 10 kilométeres távolságokra is összekapcsolja az eszközöket. Általában intelligens épületekben használják egymástól távol lévő eszközök, például kültéri érzékelők és működtetők összekapcsolására. [33]

- **KNX RF**

A KNX RF (Radio Frequency) az épületautomatizáláshoz használt KNX protokollcsalád részét képező vezeték nélküli kommunikációs szabvány. Az épületautomatizálási

rendszerben lévő eszközök rádiófrekvenciás kommunikációval történő összekapcsolására szolgál. A KNX RF szabványosított kommunikációs interfészt biztosít az épületautomatizálási rendszer különböző eszközei, például érzékelők, működtetők és vezérlők számára. [34]

A vezeték nélküli kommunikációs technológiák döntő szerepet játszanak az épületirányítási rendszerek átjárhatóságában, biztonságában és hatékonyságában. Az intelligens épület egyedi követelményeitől, például a hatótávolságtól, az adatátviteli sebességtől és az energiafogyasztástól függően ajánlott e technológiák kombinációját használni.

**Kommunikációs védelem**

A kiberbiztonság az épületirányítási rendszerek kommunikációjának másik kritikus szempontja. A szabványosított kommunikációs protokollok gyakran tartalmaznak olyan biztonsági funkciókat, mint a titkosítás, a hitelesítés és az integritás ellenőrzése, amelyek biztosítják az átvitt adatok titkosságát, hitelességét és integritását. [3].

Az épületirányítási rendszerek kommunikációs biztonságának biztosítása érdekében ajánlott a beépített biztonsági funkciókkal rendelkező szabványosított kommunikációs protokollok használata. Ez segít megvédeni a továbbított adatokat a jogosulatlan hozzáféréstől, módosítástól vagy nyilvánosságra hozataltól, ezáltal növelve az épületirányítási rendszer biztonságát és megbízhatóságát.

**Kommunikáció hatékonysága**

A hatékonyság szintén lényeges szempont az épületirányítási rendszerek kommunikációjában. A szabványosított kommunikációs protokollok gyakran tartalmaznak adattömörítést, hibaérzékelést és -javítást, valamint a szolgáltatásminőség (QoS) kezelését a hatékony kommunikáció biztosítása érdekében. [32]

A BACnet szabvány például számos szolgáltatást tartalmaz, például a ReadPropertyMultiple szolgáltatást és a WritePropertyMultiple szolgáltatást, amelyek lehetővé teszik egy BACnet objektum több tulajdonságának egyetlen kéréssel történő olvasását és írását, ezáltal csökkentve a kommunikációs többletköltséget. [35]

A hatékony kommunikáció biztosítása érdekében az épületirányítási rendszerekben ajánlott a beépített hatékonysági jellemzőkkel rendelkező szabványosított kommunikációs protokollok használata. Ez segít csökkenteni a kommunikációs többletköltséget, ezáltal javítva az épületfelügyeleti rendszer teljesítményét és reakciókészségét.

## AZ ADATBIZTONSÁG ÉS AZ ÉPÜLETÜZEMELTETÉS ÉRTÉKELÉSE

Az adatbiztonság kritikus fontosságú az épületirányítási rendszerek számára, különösen az intelligens épületekben, amelyek számos IoT-eszközre támaszkodnak különböző funkciók, például az energiagazdálkodás, a biztonság és a kényelem szempontjából. Az épületirányítási rendszerek adatbiztonságának értékelésére összpontosítása a cél ezen fejezetben.

**Értékelési kritériumok és mérőszámok**

Az épületirányítási rendszerek adatbiztonságának értékelése különböző kritériumok és mérőszámok értékelését foglalja magában. Ezek a következők lehetnek:

- **Bizalmasság:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatok csak az arra jogosultak számára legyenek hozzáférhetők. Ez magában foglalja a titkosítási algoritmusok és biztonságos kommunikációs protokollok végrehajtását az adatokhoz való jogosulatlan hozzáférés megakadályozása érdekében.
- **Sértetlenség:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatokat az átvitel során ne hamisítsák meg vagy ne változtassák meg. Ez magában foglalja az ellenőrző összegek és digitális aláírások végrehajtását az adatok integritásának.
- **Rendelkezzésre állás:** Annak biztosítása, hogy az IoT-eszközök és az épületirányítási rendszer között továbbított adatok szükség esetén rendelkezésre álljanak. Ez magában foglalja a redundancia és a failover mechanizmusok megvalósítását az adatok folyamatos rendelkezésre állásának biztosítása.
- **Hitelesítés:** Csak engedélyezett eszközök és rendszerek kommunikálhatnak az épületirányítási rendszerrel. Ez magában foglalja a hitelesítési mechanizmusok, például jelszavak, digitális tanúsítványok és biometrikus adatok bevezetését az eszközök és rendszerek személyazonosságának ellenőrzésére.
- **Engedélyezés**: Annak biztosítása, hogy csak az engedélyezett eszközök és rendszerek férhessenek hozzá az épületirányítási rendszer adataihoz és módosíthassák azokat. Ez magában foglalja a hozzáférés-szabályozási mechanizmusok, például a hozzáférés-szabályozási listák és a szerepkör-alapú hozzáférés-szabályozás megvalósítását, hogy az eszközökhöz és rendszerekhez rendelt jogosultságok alapján korlátozzák az adatokhoz való hozzáférést.
- **Letagadásmentesség:** Annak biztosítása, hogy az üzenet küldője ne tudja letagadni az üzenet elküldését, a címzett pedig ne tudja letagadni az üzenet fogadását. Ez magában foglalja a digitális aláírások és időbélyegzők alkalmazását az adatok eredetének és kézhezvételének bizonyítására.
- **Rugalmasság:** Annak biztosítása, hogy az épületirányítási rendszer gyorsan helyre tudjon állni bármilyen biztonsági incidensből, és továbbra is megfelelően működjön. Ez magában foglalja az incidensekre való reagálási eljárások, valamint a biztonsági mentési és helyreállítási mechanizmusok végrehajtását, hogy a rendszer a biztonsági incidens után visszaálljon a normál állapotba.
- **Ellenőrizhetőség:** Annak biztosítása, hogy az épületirányítási rendszerben minden tevékenységet naplóznak és ellenőrizhetővé tesznek. Ez magában foglalja a naplózási mechanizmusok és ellenőrzési nyomvonalak bevezetését a rendszerben végzett valamennyi tevékenység rögzítése és a végrehajtott tevékenységek elszámoltathatóságának biztosítása érdekében.

**Sérülékenységvizsgálat és eredmények**

Az épületirányítási rendszerek kiber,- és adatbiztonságának értékeléséhez sérülékenységvizsgálatot kell lefolytatni a végrehajtott biztonsági intézkedések hatékonyságának értékelésére. Ezek a kísérletek magukban foglalhatják különböző kibertámadások - például adatlefoglalás, adatmanipuláció és szolgáltatásmegtagadási támadások - szimulálását, és az épületirányítási rendszer e támadásokra adott válaszának értékelését.

### Értelmezés és következtetések

A vizsgálatok eredményei értelmezhetők az épületirányítási rendszerben végrehajtott biztonsági intézkedések hatékonyságának meghatározása érdekében. Tegyük fel, hogy az épületirányítási rendszer sikeresen megakadályozza a szimulált kibertámadásokat, és biztosítja az adatok titkosságát, sértetlenségét és rendelkezésre állását. Ebben az esetben megállapítható, hogy a bevezetett biztonsági intézkedések hatékonyak. Ha azonban az épületirányítási rendszer nem tudja megakadályozni a szimulált kibertámadásokat, vagy bármilyen sebezhetőséget azonosítanak, az azt jelenti, hogy a potenciális biztonsági kockázatokkal foglalkozni kell. E megállapítások következményei között szerepelhet a végrehajtott biztonsági intézkedések felülvizsgálatának, további biztonsági ellenőrzések végrehajtásának vagy az épületirányítási rendszer újratervezésének szükségessége a biztonság fokozása érdekében.

## KÖVETKEZTETÉSEK ÉS JÖVŐBELI IRÁNYOK

Az IoT-eszközök és a felhőkörnyezetek integrálása az intelligens épületekben számos kihívást jelent, többek között az adatbiztonság, az adatvédelem és az interoperabilitás terén. Ez a publikáció feltárta ezeket a kihívásokat, és lehetséges megoldásokat javasolt. Az épületirányítási rendszerek adatbiztonságának értékelése különböző kritériumok értékelését foglalja magában, beleértve a bizalmasságot, az integritást, a rendelkezésre állást, a hitelesítést, a felhatalmazást, a letagadásmentességet, a rugalmasságot és az ellenőrizhetőséget. A titkosítási algoritmusok, biztonságos kommunikációs protokollok, ellenőrző összegek, digitális aláírások, hozzáférés-szabályozási mechanizmusok, incidensekre reagáló eljárások és naplózási mechanizmusok megvalósítása elengedhetetlen az épületirányítási rendszer biztonságának és integritásának biztosításához.

Az intelligens épületirányítási rendszerek másik jelentős kihívása az interoperabilitás. A különböző eszközök, például érzékelők, működtetők és vezérlők különböző kommunikációs protokollokat, adatformátumokat és interfészeket használhatnak, ami kihívássá teszi integrálásukat egy egységes és működőképes épületirányítási rendszerbe. Biztonsági és adatvédelmi aggályok is felmerülhetnek az IoT-eszközök és a felhőkörnyezetek közötti adattovábbítás során. E kihívások kezelése érdekében ajánlott szabványosított kommunikációs protokollok és interfészek, például BACnet, KNX vagy Zigbee használata, valamint megfelelő biztonsági intézkedések végrehajtása az épületirányítási rendszer biztonságának és integritásának biztosítása érdekében.

Kutatásunkat folytatva a cél egy átfogó és kiterjedt auditálható kiberbiztonsági keretrendszer kidolgozása az okos épületek auditálhatósága szempontjából, ahol a fő fókusz az IoT rendszerekre irányul. Ezzel is segítve a tervezőket, kivitelezőket, döntéshozókat és auditorokat, hogy egy meghatározott irányvonal mentén tudjanak megfelelő döntésket hozni egy intelligen épület IoT kiberbiztonsága kapcsán.

Összefoglalva, az intelligens épületrendszerek adatbiztonságának és átjárhatóságának biztosítása alapvető fontosságú az épületirányítási rendszerek sikeres megvalósításához és működtetéséhez. A szabványosított kommunikációs protokollok és interfészek, valamint a megfelelő biztonsági intézkedések bevezetése megoldhatja ezeket a kihívásokat, és biztosíthatja az intelligens épületrendszerek biztonságos és hatékony működését. A jövőbeni kutatásoknak a fejlettebb biztonsági protokollok és kommunikációs interfészek fejlesztésére

kell összpontosítaniuk, hogy kezelni tudják az intelligens épületrendszerek fejlődő biztonsági fenyegetéseit és interoperabilitási kihívásait.

## FELHASZNÁLT IRODALOM[3]


[1] R. A. Abdelouahid, O. Debauche, és A. Marzak, „Internet of things: a new Interoperable IoT platform. Application to a smart building”, *Procedia Comput. Sci.*, köt. 191, o. 511–517, 2021.

[2] W. Granzer, F. Praus, és W. Kastner, „Security in building automation systems”, *IEEE Trans. Ind. Electron.*, köt. 57, sz. 11, o. 3622–3630, 2009.

[3] B. Sándor és Z. Rajnai, „Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View”, *Interdiscip. Descr. Complex Syst. INDECS*, köt. 21, sz. 2, o. 141–147, 2023.

[4] „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE”, 2022. december 14. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX%3A32022L2555 (elérés 2023. szeptember 1.).

[5] V. M. Rohokale, N. R. Prasad, és R. Prasad, „A cooperative Internet of Things (IoT) for rural healthcare monitoring and control”, in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, febr. 2011, o. 1–6. doi: 10.1109/WIRELESSVITAE.2011.5940920.

[6] A. Botta, W. De Donato, V. Persico, és A. Pescapé, „Integration of cloud computing and internet of things: a survey”, *Future Gener. Comput. Syst.*, köt. 56, o. 684–700, 2016.

[7] F. Vahid és T. D. Givargis, *Embedded system design: a unified hardware/software introduction*. John Wiley & Sons, 2001.

[8] L. Cui, G. Xie, Y. Qu, L. Gao, és Y. Yang, „Security and privacy in smart cities: Challenges and opportunities”, *IEEE Access*, köt. 6, o. 46134–46145, 2018.

[9] W. Stallings, „CRYPTOGRAPHY AND NETWORKSECURITY PRINCIPLES ANDPRACTICE”, 2011.

[10] A. Dorri, S. S. Kanhere, R. Jurdak, és P. Gauravaram, „Blockchain for IoT security and privacy: The case study of a smart home”, előadás 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, o. 618–623.

[11] D. S. Abd Elminaam, H. M. Abdual-Kader, és M. M. Hadhoud, „Evaluating The Performance of Symmetric Encryption Algorithms.”, *Int J Netw Secur*, köt. 10, sz. 3, o. 216–222, 2010.

[12] N. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, és J. C. Schuldt, „On the security of {RC4} in {TLS}”, előadás 22nd USENIX Security Symposium (USENIX Security 13), 2013, o. 305–320.

[13] D. Coppersmith, „The Data Encryption Standard (DES) and its strength against at

[14] A. Juels, „Minimalist cryptography for low-cost RFID tags”, előadás Security in Communication Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers 4, Springer, 2005, o. 149–164.

[15] T. Dierks és E. Rescorla, „The transport layer security (TLS) protocol version 1.2”, 2070–1721, 2008.
[16] W. Simpson, „PPP challenge handshake authentication protocol (CHAP)”, 2070–1721, 1996.
[17] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, és H. Levkowetz, „Extensible authentication protocol (EAP)”, 2070–1721, 2004.
[18] J. Granjal, E. Monteiro, és J. Sá Silva, „Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 3, o. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
[19] A. Menezes, P. Sarkar, és S. Singh, „Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography”, előadás International Conference on Cryptology in Malaysia, Springer, 2016, o. 83–108.
[20] A. Bogdanov *és mtsai.*, „PRESENT: An ultra-lightweight block cipher”, előadás Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9, Springer, 2007, o. 450–466.
[21] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, és L. Wingers, „The SIMON and SPECK families of lightweight block ciphers”, *Cryptol. Eprint Arch.*, 2013.
[22] E. Rescorla és N. Modadugu, „Datagram transport layer security version 1.2”, 2070–1721, 2012.
[23] R. Yu, G. Xue, V. T. Kilari, és X. Zhang, „Deploying robust security in internet of things”, előadás 2018 IEEE Conference on Communications and Network Security (CNS), IEEE, 2018, o. 1–9.
[24] L. Sweeney, „k-anonymity: A model for protecting privacy”, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, köt. 10, sz. 05, o. 557–570, 2002.
[25] A. Machanavajjhala, D. Kifer, J. Gehrke, és M. Venkitasubramaniam, „l-diversity: Privacy beyond k-anonymity”, *ACM Trans. Knowl. Discov. Data TKDD*, köt. 1, sz. 1, o. 3-es, 2007.
[26] N. Li, T. Li, és S. Venkatasubramanian, „t-closeness: Privacy beyond k-anonymity and l-diversity”, előadás 2007 IEEE 23rd international conference on data engineering, IEEE, 2006, o. 106–115.
[27] A. C. Yao, „Protocols for secure computations”, előadás 23rd annual symposium on foundations of computer science (sfcs 1982), IEEE, 1982, o. 160–164.
[28] D. Bogdanov, S. Laur, és J. Willemson, „Sharemind: A framework for fast privacy-preserving computations”, előadás Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings 13, Springer, 2008, o. 192–206.
[29] A. Shamir, „How to share a secret”, *Commun. ACM*, köt. 22, sz. 11, o. 612–613, 1979.
[30] W. Granzer és W. Kastner, „Security analysis of open building automation systems”, előadás Computer Safety, Reliability, and Security: 29th International Conference, SAFECOMP 2010, Vienna, Austria, September 14-17, 2010. Proceedings 29, Springer, 2010, o. 303–316.
[31] J. Han, C.-S. Choi, W.-K. Park, I. Lee, és S.-H. Kim, „Smart home energy management system including renewable energy based on ZigBee and PLC”, *IEEE Trans. Consum. Electron.*, köt. 60, sz. 2, o. 198–202, 2014.

[32] W. Kastner, G. Neugschwandtner, S. Soucek, és H. M. Newman, „Communication systems for building automation and control”, *Proc. IEEE*, köt. 93, sz. 6, o. 1178–1203, 2005.
[33] L. Trinh, V. X. Bui, F. Ferrero, T. Nguyen, és M. Le, „Signal propagation of LoRa technology using for smart building applications”, előadás 2017 IEEE Conference on Antenna Measurements & Applications (CAMA), IEEE, 2017, o. 381–384.
[34] A. S. Shah, H. Nasir, M. Fayaz, A. Lajis, és A. Shah, „A review on energy consumption optimization techniques in IoT based smart building environments”, *Information*, köt. 10, sz. 3, o. 108, 2019.
[35] A. Fernbach, W. Granzer, és W. Kastner, „Interoperability at the management level of building automation systems: A case study for BACnet and OPC UA”, előadás ETFA2011, IEEE, 2011, o. 1–8.

# THE SIGNIFICANCE OF CASH AND ITS SUPPLY IN HUNGARY AND IRELAND

# A KÉSZPÉNZ-ELLÁTÁS JELENTŐSÉGE ÉS BIZTOSÍTÁSA MAGYARORSZÁGON ÉS ÍRORSZÁGBAN

SOMOGYI TAMÁS[1]

**Abstract**

Cash, that has some thousand-year long history and serves the purpose of transaction and saving, is still significant in the era of electronic payment. And undoubtedly essential for those who do not use digital banking services. In the EU, making the choice between cash or electronic payment solution is a fundamental right. Therefore, beside the digital financial solutions, the supply of cash is also to be considered essential service. However, few studies addressed the security issues of cash supply. The purpose of this paper is to investigate the significance of cash and to explore the way cash supply is maintaned in Hungary and the eurozone member Ireland. Research data has been drawn from three sources: publicly available documents, relevant literature and sector-specific regulations were examined. Moreover, some observations will be provided at the end.

**Keywords**

Cash, Hungary, Ireland, European Union

**Absztrakt**

Az évezredes múltra visszatekintő készpénz az elektronikus fizetés korában sem veszített jelentőségéből: továbbra is szolgál tranzakciós célokat és vagyontartási célokat. És vitathatatlanul létfontosságú az elektronikus pénzügyi szolgáltatásokat nem használók számára. Az Európai Unió alapelvként tekint a szabad választás lehetőségére a készpénz és az elektronikus fizetési megoldások között. Következésképpen az elektronikus pénzügyi szolgáltatások mellett a készpénz-ellátás is létfontosságú rendszernek tekinthető. Azonban ennek a területnek a biztonsági kérdései kevés figyelemben részesültek a korábbi kutatások során. Cikkemben a pénzügyágazat nyilvános adataira építve áttekintem a készpénz jelentőségét, majd pedig elemzem a készpénz-ellátás biztosítását Magyarországon és az euroövezeti Írországban a vonatkozó jogszabályok és releváns szakirodalom alapján. Végül megállapításokat teszek a készpénz-ellátás aktuális helyzetéről.

**Kulcsszavak**

Készpénz, Magyarország, Írország, Európai Unió

[1] somogyi.tamas@phd.uni-obuda.hu | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Kétségtelen, hogy a piacgazdaságban kulcsszerepet játszik a pénz. Ebből fakad a pénzhasználatot lehetővé tévő és a pénzkereslet kielégítését biztosító infrastruktúra jelentősége. Az általánosan elfogadott meghatározás szerint az infrastruktúra létesítmények, intézmények, eszközök és személyek olyan összekapcsolódása, mely lehetővé teszi anyagi javak termelését és fogyasztását a gazdaság minden területén, valamint hozzájárul a hatékony működéshez, és fejlődéshez [1]. Ahogyan a 2012. évi CLXVI. törvény 1. § j) pontja megfogalmazza, az infrastruktúra egyes elemei létfontosságúak, mivel „*elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna*“. Ezen törvény létfontosságúnak nevezi a pénzügy ágazaton belül a készpénzellátást is (lásd fenti törvény 1. § j) pontja hivatkozta 1. számú melléklet) [2].

Kimutatható, hogy a pénzügyi szolgáltatások terén is megfigyelhető digitalizáció adta fejlődés [3] változást hozott a lakosság fizetési szokásaiban [4]. Ráadásul az egész társadalmat érintő koronavírus-járvány alatti védekező intézkedések csökkentették a készpénzes tranzakciókat [5], így felerősödött a készpénz-mentesítés kérdéskörének kutatása [6]. Igaz, a készpénz-kímélő fizetés jelensége országonként változó mértékű [7], és gazdasági szempontból összességében nézve kevéssé jelentős változást eredményezett a készpénz-forgalomban [8]. Érdekességként említhető, hogy egy, a pénzügyi tudatosságot is figyelembe vevő japán kutatás szerint az eltérő pénzügyi ismeretekkel rendelkező társadalmi csoportok között sem azonosítható jelentős eltérés a készpénzkeresletet nézve [9]. Bár lehetséges eltérés országonként, az kijelenthető, hogy a készpénzellátás biztosítása mai is jelentős feladat, a készpénzellátást biztosító infrastruktúra elemei pedig valóban létfontosságúak. Az Európai Központi Bank (ECB) *The Eurosystem's retail payments strategy* című dokumentuma bár üdvözli a készpénz-kímélő fizetést, a készpénz-ellátást is a lakossági fizetési stratégia részének tekinti az euróövezetben [10]. Ezen felül az ún. *uniós lakossági pénzforgalmi stratégia* a teljes EU-ra nézve stratégiai intézkedésnek tekinti a központi banki pénz rendelkezésre állásának biztosítását (a készpénz-kímélő fizetési megoldások és azonnali átutalás biztosítása mellett) [11]. Ahogyan az Európai Központi Bank megfogalmazta, az euroövezet garantálja a készpénzhez való hozzáférés lehetőségét azért, hogy mindenki szabadon eldönthesse, hogyan teljesíti napi fizetési kötelezettségeit: készpénzben vagy elektronikusan [12].

A készpénzellátást is magában foglaló létfontosságú infrastruktúra védelme államilag szabályozott és irányított [13], hiszen az folyamatos kihívást jelent: elegendő gondolni a napjainkban egyre nagyobb mértéket öltő kiberfenyegetettségre [14], [15], vagy a Kárpát-medencét is érintő klímaváltozás okozta extrém természeti jelenségekre [16] vagy akár egy nagy hatású terrortámadás veszélyére [17]. Ezen néhány példa is alátámasztja a létfontosságú infrastruktúra magas szintű, államilag összefogott védelmének fontosságát [18] és tudományos kutatásának indokoltságát.

A következőkben áttekintem a készpénz-ellátás jelentőségét, valamint biztosításának aktuális kérdéseit hazánkban és egy euróövezeti tagállamban, Írországban.

## A KÉSZPÉNZ ÉS JELENTŐSÉGE

A pénz célja kettős: egyfelől tranzakciós célt szolgál, másfelől vagyontartási céllal bír. Ez utóbbi hazánkban leginkább a nagyobb címletű bankjegyekre igaz, míg általában a kisebb címleteket tranzakcióra használjuk [19]. A készpénz iránti igény kielégítését, vagyis az elengedő pénz rendelkezésre állását a jegybankok monetáris politikája biztosítja [20]. A jegybank, vagyis központi bank, ágazat-specifikus hatóságként a stabilitás megőrzésének céljával felügyeli és szabályozza a pénzügyi ágazatot, valamint rendelkezik a pénzteremtés jogával [21]. Hazánkban a jegybank szerepét a Magyar Nemzeti Bank (MNB) tölti be, míg az euroövezetben az Európai Központi Bank (ECB) és a tagállami központi bankok együttesen.

A Bevezetésben már említésre került, hogy a digitalizáció és innováció terjedése mellett továbbra is jelentős a készpénz-forgalom. A készpénz-használat előnyei közé sorolhatóak:

- technikai infrastruktúra nélküli azonnali fizetést tesz lehetővé;
- magánszemélyek közvetlenül tarthatják maguknál;
- anonim módon használható;
- kiskereskedelmi ügyletekben az elfogadása az irányadó.

A készpénz-használat jelentőségét növeli továbbá, hogy az elektronikus pénzügyi szolgáltatásokkal nem rendelkezők számára a készpénz használata létfontosságú. Ezen társadalmi csoport méretét jól láttatja a Világbank adataira épülő 1. Táblázat.

| | **Magyarország** | **Magas jövedelmű országok csoportjának átlaga (hazánk és Írország is itt)** |
|---|---|---|
| rendelkezik bankszámlával | 88,2% | 96,4% |
| az elmúlt egy évben fizetett digitálisan | 81,4% | 92,4% |
| államtól pénzt kapott bankszámlára az elmúlt egy évben | 37,3% | 43,2% |
| bankszámlán tartalékol pénzt | 75,2% | 84,5% |

*1. Táblázat Elektronikus pénzügyi szolgáltatások a 15 évesnél idősebb korosztályban, [22] alapján*

A Magyar Nemzeti Bank éves jelentései alapján 2021. év végén a forgalomban lévő készpénzállomány 7675,2 milliárd Forint [23], míg 2022. év végén 8226,1 milliárd Forint volt [24]. Elmondható, hogy a koronavírus-járvány hullámai alatti ingadozást leszámítva a hazai készpénzállományt lassuló ütemű bővülés jellemzi. Magyarországon a pénzforgalmi szolgáltatóknál (elsősorban a postahivatalokban) a készpénzbefizetések száma enyhén csökken, de értéke növekszik (2. Táblázat). Bár a magyar lakosság 80%-a tartja magát nyitottnak az elektronikus fizetési lehetőségekre és használt már készpénz-kímélő fizetési eszközt az MNB felmérése alapján [25], fenti adatok alapján a készpénzforgalom hazánkban jelentősnek mondható.

| Készpénzbefizetés | 2021. I. negyedév | 2022. I. negyedév | 2023. I. negyedév |
|---|---|---|---|
| darab | 3 077 818 | 2 940 954 | 2 930 444 |
| millió Forint | 2 055 877 | 2 350 106 | 2 567 734 |

*2. Táblázat A hazai pénzforgalmi szolgáltatók pénztáraiban lebonyolított készpénz-befizetési tranzakciók száma és értéke, [26] alapján*

A készpénzzel lebonyolított tranzakciók száma az Európai Unió szintjén nézve is jelentős: a kis értékű fizetések többségében továbbra is készpénzt használnak, ezért az Európai Bizottság kulcskérdésnek tekinti a készpénz rendelkezésre állásának biztosítását [11]. Csak az euróövezetet tekintve is jól látható a készpénz fontossága. Az Európai Központ Bank egy 2022. évi tanulmánya szerint az euróövezetben bár csökken a készpénz-használat, az 50 EUR alatti fizetések többségét készpénzben bonyolítják le [27]. Ezen felül ezen tanulmány a fizetési szokások tekintetében a 2019. és 2022. közötti időszakban a következő változást is megállapította. A megkérdezettek 54%-a nem változtatta meg a készpénz-használati szokásait, 32%-a kevesebb alkalommal fizet készpénzzel, míg 14%-a több alkalommal használ készpénzt.

Az ECB egy másik tanulmánya a készpénz-használat mögött több lehetséges okot is feltételez [28]:

- az idősebb korosztály alacsony jövedelmű és alacsony iskolázottságú része erősen valószínű, hogy nem vesz igénybe banki szolgáltatást (“cash-only population”);
- korrelál a digitális világban való magasabb fokú jártasság és az elektronikus fizetési módok használata - más szavakkal, a digitális ismeretek hiánya megakadályozhat egyeseket az elektronikus fizetési módok használatában;
- a fizetésüket készpénzben felvevők nagyobb valószínűséggel nem vesznek igénybe banki szolgáltatásokat (“unbanked”).

Habár egy-egy konkrét esetben a fizetési mód megválasztását több tényező is befolyásolhatja (például az összeg nagysága, a teljes bevételen belül a készpénzben felvett jövedelem nagysága, vagy a kereskedő preferenciája), az kijelenthető, hogy a társadalom számottevő része bizonyos tranzakciók esetében a készpénzt részesíti előnyben vagy kizárólag csak készpénzt használ. Azt is hangsúlyozni szükséges, hogy a kevesebb pénzügyi ismerettel rendelkezők számára egy felelőtlen pénzügyi döntés (például helytelenül megválasztott bankszámlacsomag) anyagi veszteséggel járhat, mélyítheti a társadalmi leszakadást és végső soron a teljes gazdaság számára káros lehet [29].

Felmerül a kérdés, hogyan viszonyulnak a készpénzhez a készpénz-kímélő fizetési módokat preferáló emberek, milyen elvárás fogalmazódik meg a társadalomban? A fentebb már említett ECB tanulmány közli egy, a készpénzre vonatkozó euróövezeti felmérés eredményét [27]:

- az Euróövezetben a lakosság 60%-a fontosnak mondja a készpénzes fizetési lehetőséget, és csak a válaszadók 12%-a tartja kivezethetőnek a készpénzt;
- az 55 év feletti korosztály magasabb iskolázottságú tagjainak 64%-a számára fontos a készpénzes fizetési lehetőség, míg a 25 év alatti korosztálynak csak az 54%-a számára fontos;
- az Euróövezetben a válaszadók háromnegyede ATM -nél vesz fel készpénzt (és nem például bankfiók pénztárában).

Hazánkban egy témabeli tanulmány megállapítja, hogy a magyar lakosság közel fele a bankkártyás fizetést vagy az átutalást részesíti előnyben a készpénzzel szemben, és harmada, ha tehetné, csak elektronikusan fizetne [30].

Látható tehát, hogy a digitális pénzügyi szolgáltatások elterjedtek, és bár a készpénz-kímélő fizetési lehetőségek kényelmesek, sőt, például járvány időszakában javasoltnak is mondhatók, mégis, a pénzügyi ágazat infrastruktúrájától függenek. A Bevezetésben már említésre került, hogy hazánkban a pénzügyi ágazat infrastruktúrája részben létfontosságú, ennek megfelelően kiemelt védelmet élvez. Az kétségtelen azonban, hogy egyre nagyobb mértékű kihívás jellemzi a pénzügyágazat infrastruktúrájának a biztonságos üzemeltetését: elegendő megemlíteni a globális felmelegedés hatását az adatközpontokra [31] vagy a kibertámadás növekvő fenyegetettségét a bankszektorban [32]. Ráadásul, az éghajlatváltozás következményeként előforduló szélsőséges természeti jelenségek olyan katasztrófát is okozhatnak [33], amely egy adott területen használhatatlanná teszi a pénzügyi szolgáltatásokat is biztosító infrastruktúrát. A készpénz-kímélő fizetési szolgáltatásokat biztosító infrastruktúra sérülékeny, kiesése esetén a tranzakció lebonyolítása lehetetlenné válik. Ezen esetekben a készpénzes fizetési tranzakció tulajdonképpen egyfajta vészhelyzeti megoldásként is szolgálhat, hiszen bárhol, bármikor azonnal használható, és kétségtelenül egyszerűbb, mint a váltó vagy a csekk.

Érdemes külön megemlíteni, hogy a készpénz nemzeti szimbólumokat tartalmaz, így bizonyos módon része identitásunknak és kulturális örökségünknek. Ezen kívül a gyűjtők számára speciális értéket képviselnek mind a bankjegyek, mind pedig az érmék. Mindez pedig hozzájárul a készpénz iránti igényhez, így ezen a szempontokat is figyelembe kell venni.

Mindezek alátámasztják a készpénz-használat biztosításának a fontosságát és a készpénz-ellátás biztonságának jelentőségét. Ezen biztonságot garantálni tudja a szabályozott és felügyelt pénzügyágazat, azon belül pedig a készpénz-ellátást biztosító és létfontosságúként azonosított infrastruktúra. A készpénz-forgalom szabályozottságának és állami felügyeletének indokoltságát igazolja mindezen túlmenően a terrorizmus elleni küzdelem, továbbá a hamis bankjegyek kiszűrése a készpénz-forgalomhoz vitathatatlanul szükséges bizalom fenntartása érdekében. Igazolást nyert, hogy a nagyobb a terrorszervezetek a számukra szükséges pénz megszerzése érdekében többek között bankjegyeket hamisítanak [34], valamint megjelennek legálisan például a turizmus szektorban, így téve lehetővé a pénzmosást vagy készpénz határokon átívelő mozgását [35]. A készpénz birtokában pedig fegyverhez juthatnak [36], vagy erőszakos cselekményeiket finanszírozhatják.

Összefoglalva, bár látható a készpénz-kímélő fizetés térnyerése, vitathatatlan a készpénz-forgalom jelentősége, fontossága a társadalom és a gazdaság szempontjából hazánkban és az Európai Unióban egyaránt. A következőkben a készpénz-ellátás biztosításának főbb kérdéseit tekintjük át először Magyarországon, utána pedig az euroövezeti Írországban.

## A KÉSZPÉNZ-ELLÁTÁS BIZTOSÍTÁSA MAGYARORSZÁGON

Az előbb már említésre került a jegybank szerepe a készpénzellátás és a pénzügyágazat stabilitásának biztosítása érdekében. Ennek megfelelően a Magyar Nemzeti Bank figyelemmel követi a hazai készpénz-használatot és szükség esetén ágazat-specifikus ható-

ságként beavatkozik a pénzügyi tranzakciók megbízható és hatékony megvalósulása érdekében. Ennek egyik példájaként említhető az MNB rendszeres készpénzforgalmi hatósági ellenőrzése a hitelintézetek és pénzfeldolgozó szervezetek körében. Ezen vizsgálatok során helyszínen ellenőrzi a bankjegyvizsgáló gépek működését, a sérült és nehezen felismerhető bankjegyek kezelésének folyamatát [23]. Az MNB vonatkozó tevékenységére másik példa a 2021. szeptember 8-án a pénzforgalmi szolgáltatók számára kibocsátott vezetői körlevele [37]. Az MNB egy 2021-es felmérése megállapította az ATM gépek használatának és funkcióinak bővülésével együtt az ügyfélpanaszok számának a növekedését [23]. Erre válaszul a jegybank 2021. szeptember 8-án a pénzforgalmi szolgáltatók számára vezetői körlevelet adott ki, amelynek célja az automaták üzemeltetésére, az ügyfelek tájékoztatására, a fizetési műveleteket érintő ügyfélpanaszok kezelésére, elszámolására vonatkozó jogszabályi rendelkezések[2] egységes értelmezésének elősegítése.

A hazai készpénzellátás biztosítása elsősorban az ún. bankjegyrendeleten[3] alapul. Ez az 1/2023. (I. 17.) MNB rendelet tárgyalja a bankjegyek forgalmazásának szabályait és annak zavartalanságát célzó előírásokat, valamint foglalkozik a készpénz valódiságának és forgalomképességének kérdéseivel. Ezt két nagy témakört tekintjük át a következőkben.

A zavartalan készpénz-ellátás biztosításának fontos kérdése a készpénzhez való hozzáférés, mely a lakossági fogyasztók esetében elsősorban hitelintézeteken keresztül történik. Azon hitelintézetek, melyek lakossági fogyasztók részére fizetési számlát vezetnek és a fizetési kártyákat tekintve a piaci részesedésük legalább 1%, kötelesek ATM hálózatot üzemeltetni. A készpénzhez való hozzáférés országos biztosítása érdekében a készpénzfelvételi funkcióval rendelkező ATM automaták területi megoszlása is szabályozott (lásd 3. Táblázat), a hitelintézet kibocsátott fizetési kártyáinak darabszáma szerint. Amennyiben a kibocsátott fizetési kártyák száma meghaladja a 600,000 darabot, úgy a kibocsátó hitelintézet a vármegyeszékhelyen kívüli városok legalább 65%-ában köteles készpénzfelvételi funkcióval rendelkező készpénzes automatát üzemeltetni, 1 200 000 feletti kártyaszámnál pedig a vármegyeszékhelyen kívüli városok 80%-ában. Ez az előírás garantálja a megfelelő földrajzi lefedettséget. A hitelintézetek kötelesek a készpénzesautomata-hálózatuk területi és forgalmi alapú feltételeknek való megfelelését háromévente felmérni, és annak eredményét a nemzeti banknak megküldeni[4].A készpénzes automaták működésével kapcsolatban az elvárás az éves szinten minimum 98%-os rendelkezésre állás[5] (kivéve a vis maior helyzetet és a szezonális működést). A készpénzes automaták használatát a hitelintézetek telefonos ügyfélszolgálatukkal támogatják.

Felmerülhet a készpénzellátásban jelentős szerepet betöltő hazai ATM automaták és a mögöttes IT infrastruktúra biztonságának kérdése, ezért érdemes kitérni erre. Kijelenthető, hogy a magyar pénzügyi ágazat is kitett a pénzügyi szektort célzó kibertámadásoknak [38].

[2] 2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról

[3] 1/2023. (I. 17.) MNB rendelet a bankjegyek feldolgozásáról, forgalmazásáról, valamint hamisítás elleni védelmével kapcsolatos technikai feladatokról

[4] bankjegyrendelet 10.§ (1) és (7)

[5] bankjegyrendelet 14.§

| **Készpénzfelvételi funkcióval rendelkező betéti típusú fizetési kártyák teljes kibocsátott mennyisége, valamint a hitel típusú fizetési kártyák 50%-kal csökkentett kibocsátott mennyisége** | **min. ATM szám fővárosi kerületben** | **min. ATM szám vármegyeszékhelyen** | **min. ATM szám vármegye egyéb településein** |
|---|---|---|---|
| ≤600 000 | 2,5 | 2,5 | 3,5 |
| 600 001–1 200 000 | 5 | 5 | 15 |
| 1 200 001–2 400 000 | 7 | 7 | 28 |
| 2 400 001≤ | 12 | 15 | 60 |

*3. Táblázat hitelintézet által üzemeltetendő, készpénzfelvételi funkcióval rendelkező ATM automaták minimálisan elvárt darabszáma az 1/2023. (I. 17.) MNB rendelet 10.§ (1) bekezdése alapján*

Az informatikai rendszerek védelmének alapja az ágazatban vonatkozó 42/2015. (III. 12.) Kormányrendelet és a Magyar Nemzeti Bank az informatikai rendszer védelméről szóló 8/2020. (VI.22.) számú ajánlása, mely részletezi a jogszabályi minimum szintű elvárásokat és az előremutató gyakorlatot többek között az ATM automaták infrastruktúrájának védelme érdekében.

A készpénzellátás másik lényeges infrastrukturális feltétele a hitelintézetek fiókhálózatában elérhető pénztárak. Ugyanakkor a bankok már pénztár nélküli fiókot is üzemeltethetnek, azonban pénztár megszüntetése csak szabályozott módon történhet. Pénztár megszüntetésének feltétele a forgalom kimutatható csökkenése és a pénztári szolgáltatást igénybe vevő ügyfélkör számára a be- és kifizetést is biztosító készpénzes automaták elérhetősége. Az automaták elhelyezése vagy bankfiókban vagy a településen, kerületben csomópontban kell történjen, ahol orvosi ellátás, kiskereskedelmi üzlet, postai szolgáltatás, közösségi közlekedés vagy egyéb szolgáltatás is elérhető. Figyelembe kell venni ugyanakkor, hogy a készpénzes automaták nem biztosítják a készpénz-ellátás teljes körét: az érmék elfogadását és a sérült bankjegyek átváltását, tehát a pénztári szolgáltatás teljes mértékben nem szüntethető meg. A hitelintézetek pénztári szolgáltatása mellett a készpénz-ellátás fontos szereplője az országos lefedettséggel rendelkező posta. Mindez együtt biztosítja a lakosság készpénz-ellátását és a készpénzforgalom fennmaradását.

Az eddigiekben a készpénzhez való hozzáférés és a készpénz befizetésének infrastrukturális feltételeiről esett szó. E mellett a bankjegyrendelet másik nagy témaköre a valódiság és forgalomképesség biztosítása, mely kétségtelenül esszenciális a készpénz-használat fentebb említett céljainak elérése érdekében. Magyarországon pénzfeldolgozó és -forgalmazó bankjegyet abban az esetben forgathat vissza, ha megvizsgálta és azt valódinak és forgalomképesnek találta[6]. Természetesen valódisági és forgalomképességi vizsgálatot nem kell elvégezni a bankjegy kibocsátójától átvett bankjegyek esetében, vagy ha más pénzfeldolgozó, -forgalmazó igazoltan elvégezte a vizsgálatot. Ezen vizsgálatot az MNB jegyzék-

[6] bankjegyrendelet 3.§

ben szereplő típusú, az ott meghatározott hardver- és szoftververzióval rendelkező bankjegyvizsgáló géppel vagy kézi ellenőrzéssel kell elvégezni. Ez a szabályozott és előírt eljárás biztosítja a hamis bankjegyek kiszűrését és ezzel a készpénzforgalomban alapvető bizalom fenntartását.

Fentiekből látható, hogy a bankjegyrendelet célja készpénzellátás és -forgalom zavartalanságának biztosítása, mely a társadalom számára létfontosságú szolgáltatás. Ugyanakkor felmerülhet a kérdés, vajon rendkívüli helyzetben melyik az elsődleges a készpénzellátás folyamatossága és a biztonság közül? A bankjegyrendelet meghatározása szerint vis maior helyzet az „*elháríthatatlan, a bankjegyellátásban komoly fennakadást okozó természeti, infrastrukturális vagy társadalmi körülmény, amely az e rendeletben foglaltak teljesítését befolyásolja, illetve gátolja, így különösen a természeti katasztrófa, a terrorcselekmény, a sztrájk, a háború és a polgárháború*“[7]. Az előírt valódisági és forgalomképességi ellenőrzést vis maior helyzetben is el kell végezni, de megengedett a kézi ellenőrzés[8]. Rendkívüli helyzetben a készpénzes automaták üzemeltetése akár el is lehetetlenülhet, így az előírt 98%-os rendelkezésre állás biztosítása alól mentesül az automatát üzemeltető[9]. Amennyiben lehetséges, rendkívüli helyzetben (mely pénzügyi kockázatból eredő helyzet is lehet, például hitelintézetbe vetett bizalom megrendülése) a készpénzellátás zavartalanságának biztosítása érdekében az MNB gondoskodik az előzetesen kijelölt hitelintézeti és postai fiókokba készpénzt szállításáról. Ezek alapján kijelenthető, hogy a készpénzellátás folyamatossága még rendkívüli helyzetben is prioritást élvez a készpénz - előző fejezetben tárgyalt - jelentőségének megfelelően.

Összefoglalásként elmondható tehát, hogy a hazai szabályozás alapján a pénzügyi ágazat szereplői biztosítják a készpénz-ellátás folyamatosságát és biztonságát, valamint a készpénzforgalom zavartalan működését. A következő rész bemutatja a készpénzellátás és -forgalom aktuális kérdéseit egy EU-s, euroövezeti országban, Írországban.

## A KÉSZPÉNZ-ELLÁTÁS BIZTOSÍTÁSA ÍRORSZÁGBAN

A bevezető részben említettük, hogy az Európai Központi Bank a készpénz-ellátást is a lakossági fizetési stratégia részének tekinti az euróövezetben, így Írországban is. Érdemes megvizsgálni az ír készpénzellátás aktuális kérdéseit, majd a hazai helyzettel összehasonlítást tenni.

Az Ír Központi Bank (CBI) 2022. október 13-án tette közzé az ATM használat elemzésének eredményeit 2015-től, beleértve a koronavírus-járvány időszakát is [39]. Annak ellenére, hogy az elmúlt években Írországban megnövekedett a bankkártyás fizetések száma, az ATM hálózatnál lebonyolított készpénzes tranzakciók számossága összességében stabilnak mondható. A járványhelyzet előtt az átlagos készpénzfelvétel havonta 1,5 milliárd Euró értékű volt 2015. január és 2020. február között minden hónapban. A koronavírus-járvány miatti rendkívüli intézkedések hatására 2020. márciusától az ATM hálózat forgalma számottevő mértékben csökkent. Azonban 2022. júniusától a havi összes készpénzfelvétel már ismét átlagosan 1 milliárd Euró. Ezen adatok a járvány miatti lezárásoknak megfelelőek, hiszen a készpénzzel történő fizetés a karantén-időszakban nyilvánvalóan háttérbe

[7] bankjegyrendelet 2.§ 36.
[8] bankjegyrendelet 4.§ (6)
[9] bankjegyrendelet 14.§

szorult. Azonban fontos megállapítás a járványhelyzet elmúltával a készpénz iránti igény ismételt megjelenése. 2022. júniusában kb. 8 millió készpénzfelvételi tranzakciót bonyolítottak le az ír ATM hálózatban, miközben Írország lakossága 5 millió fő.

Egyértelmű tehát a készpénzhasználat iránti igény, mely kielégítéséről a CBI gondoskodik, mint központi bank. További feladata a használhatatlanná vált bankjegyek és érmék forgalomból történő kivonása. A CBI egy 2021-es jelentése szerint a készpénz iránti igény megmarad hosszú távon, vagyis mind a központi banknak, mind a pénzügyágazat tagjainak fel kell készülniük a készpénzforgalom hosszútávú biztosítására [40]. Ehhez kapcsolódik a bevezető részben már említett ECB stratégia is, mely az euroövezet alapvető felelősségeként határozza meg a készpénzellátás biztosítását és a készpénzes fizetési műveletek lehetőségének megtartását. Az ECB és az euroövezet központi bankjai ennek megfelelően kötelezően gondoskodnak arról, hogy

1. az euró bankjegyek és érmék folyamatosan a lakosság rendelkezésére álljanak a bankszektor szolgáltatásain keresztül;
2. a készpénz-felvétel és -befizetés, mint szolgáltatások, a lakosság rendelkezésére álljanak;
3. az euroövezetben a készpénz a kiskereskedelemben és magánügyletekben elfogadott legyen.

Írországban a készpénzellátás biztosításában az elmúlt években jelentősebb átrendeződést lehetett tapasztalni. A lakosság számára az elsődleges készpénz-forrást jelentő lakossági banki szolgáltatást nyújtó pénzintézetek ATM parkja 25%-kal csökkent az *Ulster Bank* kivonulásával, valamint a *Bank of Ireland* és *Allied Irish Bank* fiókbezárásaival. Ráadásul az írországi bankok az ATM hálózatuk nagyobb részének üzemeltetését átadták független szolgáltatóknak, így mostanra Írországban az ATM automaták kb. háromnegyedét független szolgáltatók üzemeltetik [41]. Írországban a lakosság kb. 90%-a nagyon könnyen vagy könnyen ér el ATM automatát [12], ugyanis lakásától 5 kilométeren belül található ATM.

A független szolgáltatók által üzemeltetett ATM eszközök nagy hányadának hátránya is megfogalmazható. Ezen független szolgáltatók nem tartoznak központi banki felügyelete alá, díjszabásuk, valamint automatáik száma és elhelyezése teljes mértékig tőlük függ [41]. Ez pedig a lakosság készpénzellátásának biztonságára nézve kockázatot hordoz magában. Díjak emelése vagy kevésbé használt ATM automata megszüntetése a lakosság készpénzhez jutását megnehezítheti vagy akár egyes településeken lehetetlenné is teheti.

Mindez emeli az ATM automaták mellett a lakosság készpénz-ellátásban fontos szerepet játszanak a bankfiókok pénztárainak jelentőségét, ahol lehetséges készpénz felvétele és -befizetése, illetve letétbe helyezése. Esetleges fiókbezárási döntés meghozatala esetén a CBI megköveteli az ügyfelek igényeinek előtérbe helyezését és a megfelelő tájékoztatásukat [41]. Ebből következik a készpénz-ellátás szempontjából az előnyük a független szolgáltatókkal szemben.

A bankfiókok mellett Írországban a postahivatalokban is lehetséges készpénzt felvenni és készpénzt számlára befizetni, az ország több, mint 900 pontján. Ezt a szolgáltatást a posta lakossági bankokkal kötött együttműködés keretében nyújtja, mint ügynök. Ebből fakadóan a CBI elvárásainak megfelelően a bankok a szerződésben megkövetelik a hatékony irányítást, a kockázatkezelést és az üzletmenet-folytonossági tervezést a postától. Ez

adja a posta előnyét a független ATM szolgáltatókkal szemben a készpénz-ellátás biztonsága szempontjából.

## KÖVETKEZTETÉSEK

Napjainkban elterjedtek az elektronikus fizetési módok, azonban, ahogyan láthattuk, a készpénz-forgalom továbbra is jelentős, ráadásul egyesek kizárólag készpénzes tranzakciókat bonyolítanak le. Ennek megfelelően mind az ECB, mind az MNB biztosítja a szükséges készpénzmennyiség elérhetőségét, valamint a választás lehetőségét a készpénz és az elektronikus fizetési eszközök között.

A készpénz-ellátás biztosítása két feladat elé állítja a központi bankokat és a pénzügyágazatot. Biztosítani kell a területi lefedettséget és a kapacitást. Az előbbi arra hivatott, hogy a lakosság számára elérhető közelségben rendelkezésre álljon készpénz-felvételi lehetőség. A területi lefedettség esetében külön meg kell említeni a turizmust, mely hozzájárul egy-egy terület készpénz-forgalmához, így szezonálisan megnövelheti a készpénz iránti igényt. Egy magyar felmérés szerint a felnőtt lakosság háromnegyede egy- vagy többnapos utazást tesz, mely része éttermi-, fürdőszolgáltatás igénybevétele, valamint szabadidős tevékenységek végzése [42]. A területi lefedettség tehát több szempontból is lényeges. Magyarországon a bankjegyrendelet meghatározza az ATM automaták minimális számát fővárosi kerületben, vármegyeszékhelyen és egyéb településeken. Írországban a lakosság nagy része számára 5 km-en belül elérhető ATM, azonban az ATM automaták háromnegyedét olyan független szolgáltatók üzemeltetik, amelyek nem tartoznak a CBI felügyelete alá, ezért stabil és hosszútávú működésük nem tartható biztosnak. A folyamatosan elérhető ATM automaták mellett a pénztárral rendelkező bankfiókok és a postahivatalok is részt vesznek a lakosság készpénz-ellátásában mind Írországban, mind Magyarországon. Ezek jelentőségét az adja, hogy mind a bankfiókok, mind a postahivatalok működése az állam illetékes szerveinek felügyelete alatt áll, szabályozott, a készpénz-ellátás jelentőségének megfelelően és nem kizárólag üzleti alapokon.

A területi lefedettség mellett a másik problémát a kapacitás jelenti. Nem elegendő pusztán az ATM automata vagy pénztár elérhetősége, a feltöltöttségét is biztosítani kell. A készpénz iránti igény időben változó lehet, szezonális turisztikai helyszíneken főszezonban. Ennek érdekében a CBI és az MNB is elvárja a bankoktól az ügyfélforgalom monitorozását és a lakosság igényének megfelelő reakciót. Vagyis, a kapacitásprobléma megfelelő kezelését előírják az illetékes felügyeleti szervek.

Fentiek alapján kijelenthető, hogy a hazai és az euroövezeti ír pénzügyágazat megfelelően biztosítja a lakosság készpénz-ellátását, mind a területi lefedettség, mind a kapacitás kérdésének kezeléséről gondoskodnak. Ezen felül a CBI és az MNB is gondoskodik a forgalomban lévő készpénz-állomány megfelelőségéről a hamis és a sérült bankjegyek forgalomból történő kivonásáról, azaz biztosítják a készpénz-forgalom működését, valamint az egész pénzügyágazat alapját képező bizalom fenntartását.

## ÖSSZEFOGLALÁS

Cikkemben áttekintettem a készpénz jelentőségét a társadalomban, és a pénzügyágazat aktuális adatai alapján bemutattam a lakoság készpénz iránti igényét, igazolva ezzel a készpénz létjogosultságát. Elemeztem a bankjegyek és érmék forgalmazásának szabályait,

annak zavartalanságát célzó előírásokat, valamint a készpénz forgalomképességét biztosító rendelkezéseket hazánk és egy euroövezeti tag, Írország példáján keresztül. Megállapítottam, hogy mindkét ország pénzügyágazata eltérő módon ugyan, de garantálja a lakosság megfelelő mennyiségű és forgalomképes készpénzzel történő ellátottságát, valamint az EU elveinek megfelelően a választás szabadságát a készpénz és az elektronikus fizetési módok között.

## FELHASZNÁLT IRODALOM


[1] Abonyiné P.J., *Infrastruktúra*, Dialóg Campus Kiadó, Budapest, 2007. ISBN 978-963-9310-77-3

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[3] Csiszárik-Kocsir Á. „The Present and Future of Banking and New Financial Players in the Digital Space of the 21st Century", *Acta Polytechnica Hungarica*, Vol 19, no 8, 2022.

[4] T. De Portu, „New trends in retail payments: How technological changes are reshaping the payments system. Introducing a proposal for a new pan-European instant payment system", *Latin American Journal of Central Banking*, Vol. 3, no 4, 2022.

[5] N. Jonker et al., „Pandemic payment patterns", *Journal of Banking & Finance*, Vol 143, October 2022

[6] Matolcsy Gy., „A magyar gazdaság, az MNB változó erőtere és annak okai", *Polgári Szemle*, 17. évf. 4-6. szám, 2021.

[7] R. Kotkowski, M. Polasik, „COVID-19 pandemic increases the divide between cash and cashless payment users in Europe", *Economics Letters*, 209 (2021)

[8] M. Braun et al., „The convenience of electronic payments and consumer cash demand", *Journal of Monetary Economics*, Vol 130, September 2022.

[9] H. Fujiki, „Cash demand and financial literacy: A case study using Japanese survey data", *Japan and the World Economy*, Vol 54, June 2020.

[10] European Central Bank, *The Eurosystem's retail payment strategy*. Online. Elérhető: https://www.ecb.europa.eu/pub/pdf/other/ecb.eurosystemretailpaymentsstrategy~5a74eb9ac1.en.pdf

[11] Európai Bizottság. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és szociális bizottságnak és a Régiók bizottságának az uniós lakossági pénzforgalmi stratégiáról. 2020. szeptember 24. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52020DC0592

[12] European Central Bank. Guaranteeing freedom of payment choice: access to cash in the euro area. Economic Bulletin. Issue 5, 2022. Elérhető: https://www.ecb.europa.eu/pub/economic-bulletin/html/eb202205.en.html

[13] Nagy R., Földi L. „A kritikus infrastruktúrák nemzeti programja", *Polgári Védelmi Szemle*, Vol 2, no 1. Elérhető: http://hdl.handle.net/20.500.12944/1088

[14] A.L.V. Ubaldo et al. „Information Security in the Banking Sector: A Systematic Literature Review on Current,Trends, Issues, and Challenges", *International Journal of Safety and Security Engineering*. Vol. 13, No. 1, 2023. https://doi.org/10.18280/ijsse.130111

[15] Gulyás O., Kiss G., „Impact of cyber-attacks on the financial institutions", *Procedia Computer Science*, Vol 219, 2023. https://doi.org/10.1016/j.procs.2023.01.267
[16] Somogyi T., „Természeti veszélyek és kezelésük a létfontosságú rendszerek és létesítmények védelmében", *Védelem Tudomány,* Vol 7, no 4, 2022. https://vedelemtudomany.hu/articles/VII/4/07-somogyi.pdf
[17] Nagy R., „A kritikus infrastruktúrák elleni lehetséges radiológiai terrortámadások", *Magyar Rendészet*. XVI. évf., 6. szám, 2016
[18] Nagy R., „A hazai katasztrófavédelmi feladatok és egyes globális hatások összefüggéseinek vizsgálatáról", *Hadtudományi Szemle*, Vol 2, no 4, 2009
[19] Végső T., „A magyarországi pénzkereslet változásának összehasonlító elemzése", *Hitelintézeti Szemle*, XIX. évf., 1. szám, 2020
[20] Fülöp K., *Bevezetés a közgazdaságtanba*, Dialóg Campus Kiadó, Budapest, 2019. ISBN 978-615-5945-31-1
[21] J. Goddard, J. Wilson, *Banking*, Oxford University Press, 2016. ISBN 978-0-19-968892-0
[22] World Bank, *The little data book on financial inclusion 2022*, Elérhető: https://openknowledge.worldbank.org/handle/10986/38148
[23] Magyar Nemzeti Bank, *Éves jelentés 2021*, ISSN 1585-4582 Elérhető: https://www.mnb.hu/kiadvanyok/jelentesek/eves-jelentesek
[24] Magyar Nemzeti Bank, *Éves jelentés 2022*, ISSN 1585-4582 Elérhető: https://www.mnb.hu/kiadvanyok/jelentesek/eves-jelentesek
[25] Magyar Nemzeti Bank, *Fizetési rendszer jelentés 2022*. https://www.mnb.hu/letoltes/fizete-si-rendszer-jelente-s-2022.pdf
[26] Magyar Nemzeti Bank. *Tájékoztató: Tovább bővül az elektronikus pénzforgalom*. Budapest, 2023. június 15., Elérhető: https://statisztika.mnb.hu/sw/static/file/Penzforgalmi_tablakeszlet_tajekoztato_20230615.pdf
[27] European Central Bank, *Study on the payment attitudes of consumers in the euro area (SPACE) 2022*, ISBN 978-92-899-5463-1 Elérhető: https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.space-report202212~783ffdf46e.en.pdf
[28] European Central Bank, „Consumer payment preferences in the Euro area", *ECB Working Paper Series*, No 2729, 2022 Elérhető: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2729~77a315ffeb.en.pdf
[29] Csiszárik-Kocsir Á., „Pénzügyi tudatosság a bankválasztásban - az ügyfélpreferenciák változása a pandémia hatására", *Polgári Szemle*, XVIII. évf. 1-3. szám, 2022.
[30] Deák V., Nemecskó I., Végső T., „A lakosság fele szívesebben fizet(ne) elektronikusan: Lakossági fizetési szokások 4. rész", 2022, Elérhető: https://www.mnb.hu/letoltes/lakossagi-fizetesi-szokasok-4-resz.pdf
[31] Somogyi T., Nagy R., „Some impacts of global warming on critical infrastructure protection - heat waves and the European financial sector", *Insights Into Regional Development*, Vol 4, no 4, 2022. https://doi.org/10.9770/IRD.2022.4.4(1)
[32] Gulyás O., Kiss G., „Kiberbiztonság 2021-ben a bankszektorban és a pénzügyi szervezeteknél", *Biztonságtudományi Szemle*, Vol 4, no 1, 2022
[33] Mezősi G., *Természeti veszélyek és hatásaik csökkentése*, Akadémiai Kiadó, Budapest, 2021. ISBN 978-963-454-692-4

[34] Besenyő J., Gulyás A., Trifunovic, D., „Hezbollah and the Internet in the Twenty-First Century", *International Journal of Intelligence and CounterIntelligence*. Vol 36, no 3, 2023. https://doi.org/10.1080/08850607.2022.2111999

[35] Besenyő J., Sólyomfi A.H., „The relationship between terrorism and tourism". In: (szerk.*) Selected Topics on Defence Economics and Terrorism*. Olcay, Ç., Sevilay, E. G. Ö., Bursa, Törökország, 2020

[36] Besenyő J., „Barry Buzan's securitization theory and the case of Iraqi Kurdish military action against ISIS in 2014", *Journal of Security and Sustainability Issues*, Vol 8, no 3, 2019

[37] Magyar Nemzeti Bank, *Vezetői körlevél a készpénz ki-, illetve befizetések lebonyolítására szolgáló automaták üzemeltetéséről, az automatákat érintő ügyfélpanaszok kezeléséről, valamint a fióki pénztárak megszüntetéséről, azok működésének korlátozásáról*, 2021. szeptember 8. Elérhető: https://www.mnb.hu/letoltes/vezetoikorlevel-atm-penztarnelkulifiok-alairt.pdf

[38] Somogyi T., Nagy R., „Cyber threats and security challenges in the Hungarian financial sector", *Contemporary Military Challenges*, Vol 24, No. 3, 2022

[39] Central Bank of Ireland, „ATM Cash Withdrawals Before, During and After the Covid-19 Pandemic", *Economic letter*, Vol 2022, no 6. Elérhető: https://www.centralbank.ie/docs/default-source/publications/economic-letters/atm-cash-withdrawals-before-during-after-covid-19-pandemic.pdf?sfvrsn=bf02951d_5

[40] Central Bank of Ireland, *Whither cash in payments?* 2021. január. Elérhető: https://www.centralbank.ie/docs/default-source/publications/quarterly-bulletins/quarterly-bulletin-signed-articles/whither-cash-in-payments.pdf?sfvrsn=5

[41] Central Bank of Ireland, *Access to cash*, 2022 június. Elérhető: https://assets.gov.ie/240775/0c505280-cd47-4592-9c12-4c8e50930ca2.pdf

[42] Rácz A., „A magyar lakosság utazási szokásai 2018 májusa és 2019 júniusa között", *Turizmus Bulletin*, Vol 20, no 2, 2020. https://doi.org/10.14267/TURBULL.2020v20n2.5

# EXTENSION TO THE SERIAL VECTOR FORMAT SPECIFICATION SUPPORTING TESTING OF ANALOG UNITS OF SAFETY-CRITICAL EMBEDDED SYSTEMS

# BIZTONSÁGKRITIKUS BEÁGYAZOTT RENDSZEREK ANALÓG RÉSZEGYSÉGEINEK VIZSGÁLATÁT TÁMOGATÓ BŐVÍTÉS A SOROS VEKTOROS FORMÁTUM SPECIFIKÁCIÓJÁHOZ

MOLNÁR Zsolt[1]

**Abstract**

In safety-critical embedded systems, the built-in self-test is an important tool to increase reliability. Embedded self-test solutions for digital circuits are much more sophisticated than for analog circuits. In this paper, my goal is to facilitate the built-in self-testing of analog circuit components and subcircuits using the solution described here. I am trying to achieve this by extending the SVF specification used for boundary scan testing of digital circuits. With the extended command set, it is possible to generate excitation current signals to measure the parameters of analog components or subcircuits, and to detect and measure the response voltages of the circuit.

**Keywords**

safety critical embedded system, built-in self-test, boundary scan, IEEE 1149, SVF, mixed signal testing

**Absztrakt**

A biztonságkritikus beágyazott rendszerekben a beépített önteszt fontos eszköz a megbízhatóság növelésére. A beépített önteszt megoldásai digitális áramköri egységekre sokkal kidolgozottabbak, mint az analóg áramkörökre. Jelen tanulmányomban célom, hogy az itt ismertetett megoldással segítsem az analóg áramköri részegységek beépített öntesztbe vonását. Ezt olyan módon igyekszem elérni, hogy a digitális áramkörök peremfigyeléses teszteléséhez használt SVF specifikációt kibővítem. A kibővített parancskészlettel lehetővé válik az analóg alkatrészek vagy részegységek paramétereinek méréséhez szükséges gerjesztő áramjelek előállítása, és az áramkör válaszfeszültségeinek érzékelése, megmérése.

**Kulcsszavak**

biztonságkritikus beágyazott rendszer, beépített önteszt, peremfigyelés, IEEE 1149, SVF, kevert jelű vizsgálat

[1] molnar.zsolt@kvk.uni-obuda.hu | ORCID: 0009-0000-8794-292X | assistant lecturer, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University | egyetemi tanársegéd, Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar

## BEVEZETÉS

A beágyazott rendszer egy speciális, előre meghatározott, optimalizált felépítésű, feladat vagy feladathalmaz ellátására létrehozott, intelligenciával ellátott rendszer. Alapja általában valamilyen processzor (mikrovezérlő, általános célú processzor, célprocesszor), vagy valódi párhuzamos működés megvalósítására képes eszköz (pl. FPGA). A rendszer működését – és részben üzembiztonságát is – nem csak a hardver határozza meg, hanem a működtető program is. Mivel a hardver feladat-orientált, így egyedi vagy speciális kiegészítő elemeket (perifériákat) igényel.

Szűkítve a beágyazott rendszerek körét, a biztonságkritikus beágyazott rendszerek esetében kiemelt szerepe van az üzembiztonságnak, ahol egy funkció vagy a teljes rendszer meghibásodása közvetlen és jelentős veszteséggel járhat. Ilyen jelentős veszteség lehet az emberi egészség vagy élet, a berendezés károsodása, vagy környezeti károk. Kritikus beágyazott rendszerekkel leginkább a járműipari (főként a vasúti és a légi), az ipari, az orvosi és katonai alkalmazásoknál találkozhatunk [3]. A kritikus beágyazott rendszereket elsődlegesen megbízhatóságra tervezik, így az olyan technikák és módszerek kutatása és kidolgozása során elért elméleti eredmények, amelyek alkalmasak a megbízhatóság növelésére, gyorsan gyakorlati hasznot hoznak. Az egyik ilyen megbízhatóságot növelő megoldás a beépített önteszt (built-in self-test).

A jelenlegi kritikus beágyazott rendszerekben általában létezik valamilyen szintű önteszt funkció. A beépített öntesztet vagy automatikusan, indításkor futtatja le a rendszer, vagy külön kérésre (parancsra). Ezt a típusú öntesztet, amely nem a normális üzem közben valósul meg, hanem üzemszünetben vagy bekapcsoláskor, nem-konkurens módszernek hívják, és meglehetősen elterjedt. Hibája, hogy a keletkező hibák bizonyos típusait nehéz vele azonosítani, detektálni. A konkurens önteszt, amely a normális üzem közben történik, sokkal kedvezőbb tulajdonságokkal rendelkezik a hiba-felfedési arány tekintetében, megvalósítása azonban számos problémát vet fel, és elterjedése is szűkkörű. Kutatási munkám során célom, hogy a konkurens önteszt eszköztárát növeljem, elsősorban a peremfigyelés (boundary-scan) alkalmazásával.

### A peremfigyeléses vizsgálat

A peremfigyelés alapgondolata, hogy az áramköröket egészében, vagy részegységeire bontva úgy vizsgálják, hogy a be- és kimeneti pontjai (fizikai kivezetései), és a magáramkör között egy-egy, a tesztelési feladatok elvégzésére alkalmas cellát (peremfigyelő cella) helyeznek el Ezek a cellák virtuális mérőtűként működnek, amelyeken keresztül gerjesztés vihető be, illetve a pontok logikai szintje mérhető. Ezek a cellák digitális rendszereknél sorosan felfűzve egy léptető regisztert alkotnak, amely rendelkezik párhuzamos írási és olvasási lehetőséggel is. A cellák soros beírásával (majd párhuzamos kiolvasásával) elvégezhető a tesztvektorok bevitele, majd párhuzamos beírással a válaszjelek mintavételezése, a soros kiolvasással pedig a tesztadatok kiléptetése történhet. Az alapszabványra (IEEE 1149.1) [1] épülő többi szabványban leírtak ennél összetetteb, speciális, illetve nem csak digitális (hanem kevert jelű, azaz analóg és digitális jeleket is használó) vizsgálatot is támogatnak (az erre vonatkozó szabvány száma: IEEE 1149.4 [2]). A peremfigyeléses vizsgálatról, annak alkalmazásáról számos könyv, tanulmány és cikk jelent meg [4] [5] [6].

A következőkben két korábbi kutatási eredményemet ismertetem röviden, mert ezek ismeretében könnyebben értelmezhető jelen tanulmányom. Mindkét téma a kevert jelű peremfigyeléshez kapcsolódik, ezen belül az analóg áramköri egységek tesztelését célozza.

**Korábbi eredményeim az analóg vizsgálatot támogató megoldások témájában**

Az analóg áramkörök beépített öntesztbe vonását támogató integrált áramkör témáját azért kezdtem kutatni, mert nincs olyan integrált áramkör a piacon, amely képes lenne beépített önteszt során biztosítani a méréshez szükséges erőforrásokat (áramgenerátor, feszültségmérő, helyi vezérlő és járulékos funkciók). Az általam körvonalazott integrált áramkör [7] képes lenne ezt az űrt betölteni: DC és AC áram gerjesztést létrehozni, DC és AC válaszfeszültséget mérni, elvégezni az eredmények képzéséhez szükséges számításokat, és az erőforrások vezérlését ellátni csupán az IEEE 1149.1 buszra csatlakozva. A működtetéséhez kidolgoztam a helyi parancsokat, azonban nincs meg az a felület a meglévő rendszerek felé, amely a digitális áramkörök vizsgálatához szükséges gerjesztő és válasz vektorokhoz hasonlóan alkalmas lenne analóg gerjesztések előállítására és a válaszok begyűjtésére.

A naplózás, az öntesztelés és a működés követése alkalmas arra, hogy bizonyos kiegészítő elemek és technikák alkalmazásával növeljék a rendszer működésének átláthatóságát és eredő biztonságát. Az általam felvázolt rendszer [8] képes arra, hogy az önteszt során

- helyettesítse az analóg és digitális információs peremfelületeken a normál üzemmódban várható jeleket, üzeneteket, parancsokat, kezelői beavatkozásokat előre meghatározott vizsgálati eseményekkel/jelekkel,
- regisztrálja azt, hogy milyen eseményekkel/jelekkel és mekkora időkéséssel válaszol a vizsgálati eseményekre a döntéshozó egység
- összehasonlítja a vizsgált rendszer válaszait a helyes (számított, vagy hibátlan egység működése közben felvett) válaszokkal, és dönt, hogy azok a megengedett hibahatáron belül rendben vannak-e

Ezen felül képes arra, hogy a naplózás során gyűjtse, tárolja és szükség esetén rendelkezésre bocsássa

- a célegységek információs peremfelületére érkező analóg vagy digitális jeleket, parancsokat, állapotjelzéseket és üzeneteket az eredeti (kódolatlan, esetleg hibás/sérült) formájukban
- a célegységek által hozott döntések hatására létrejövő, a célegységből kiküldött analóg vagy digitális jeleket, parancsokat, állapotjelzéseket és üzeneteket, a megvalósult formájukban és paramétereikkel (jelszint, időtartam)
- a kezelőszerveken keresztüli beavatkozásokat, konfigurálási tevékenységeket
- a célegységek tápellátásában, hőmérsékletében, ill. egyéb környezeti körülményeiben (páratartalom, rázkódás, stb.) bekövetkező lényeges változásokat
- az önellenőrző (öntesztelő) rendszer tevékenységeit és döntéseit
- az esemény-tárolókkal kapcsolatos eseményeket (olvasás, törlés).

Mivel ebben a beépített öntesztelést és naplózást végző rendszerben szükséges analóg gerjesztéseket előállítani, és analóg válaszjeleket mérni, itt is szükség van egy olyan, a

meglévő szabványokhoz illeszkedő eszközre, amely alkalmas lenne analóg gerjesztések előállítására és a válaszok begyűjtésére.

Sajnos eddig nem állt rendelkezésre ilyen eszköz vagy megoldás, ezért jutottam arra a kutatásaim során, hogy a digitális áramkörökhöz használt soros vektoros formátumot kísérlem meg kibővíteni erre a célra.

## A SOROS VEKTOROS FORMÁTUM ÉS JELENLEGI ALKALMAZÁSA

2023-ban szinte minden programozható logikai eszköz (FPGA és CPLD), de sok mikrovezérlő és FLASH memória is rendelkezik IEEE 1149.1 interfésszel. A soros vektoros formátumot (Serial Vector Format, SVF) azért fejlesztették ki, mert az IEEE 1149.1 szabvány használata gyorsan terjedt, és igény merült fel arra, hogy a tesztvektorokat könnyen lehessen reprezentálni és tárolni az (automatikus) tesztgeneráló szoftverekben, és egyszerűen lehessen használni a teszterekben. [9] Példának hozható a teszteléshez szükséges adatok JTAG interfészen való letöltése a tesztvezérlőről a tesztelendő áramkörbe. A specifikáció gyártófüggetlen, magas szintű IEEE 1149.1 buszműveleteket ad meg, amelyek általában léptetési műveletekből és az IEEE 1149.1-ben rögzített, a működést leíró állapotdiagram stabil állapotai közötti lépkedésből állnak. Az SVF fájl

- szöveges (ASCII) formátumú fájl, amely SVF utasítások halmazából áll
- egy sorban legfeljebb 256 karakter lehet, de egy SVF utasítás (statement) többsoros is lehet
- minden utasítás egy parancsból és a hozzá tartozó paraméterekből áll
- minden SVF utasítás pontosvesszővel zárul
- az SVF nem érzékeny a nagy- és kisbetűkre
- az SVF-fájlba megjegyzéseket lehet illeszteni a „!”, a „//” karakterek után
- az utasításon belüli adatok hexadecimális formában vannak rögzítve, és zárójelek között kell lenniük
- az adatok nem lehetnek hosszabbak, mint az adott peremfigyeléses lánc bithossza (de az MSB bevezető nullái nem számítanak bele a hosszba)
- a bitsorrend egyezik az IEEE 1149.1-ben rögzített bitsorrenddel. [10]

A fenti összegzés azért fontos, mert ezeket a szabályokat kellett figyelembe vennem a specifikáció kibővítéséhez. A specifikációban rögzített parancsokat az alábbi táblázatban mutatom be, amelyet azért közlök, hogy látható legyen, hogy a kiegészítő parancskészlet megfelelően illeszkedik a meglévő parancsokhoz. (A paraméterezés és a parancsok értelmezése a specifikációban [10] megtalálható.)

| SVF parancs | A parancs működése |
|---|---|
| ***ENDDR*** | Megadja az alapértelmezett záró állapotot adatregiszter (DR) figyelés (scan) műveletekhez. |
| ***ENDIR*** | Megadja az alapértelmezett záró állapotot adatregiszter (IR) figyelés (scan) műveletekhez. |
| ***FREQUENCY*** | Meghatározza az IEEE 1149.1 buszműveletek maximális tesztelési órajel frekvenciáját. Paraméter nélkül a rendszer maximális frekvenciájára állítja az órajelet. |

| SVF parancs | A parancs működése |
|---|---|
| ***HDR*** | Meghatározza a fejlécmintát (Header Data Register tartalmát), amely a későbbi DR figyelés (scan) műveletek elejére kerül. |
| ***HIR*** | Meghatározza a fejlécmintát (Header Instruction Register tartalmát), amely a későbbi IR figyelés műveletek elejére kerül. |
| ***PIO*** | Párhuzamos tesztmintát definiál. (A paraméterben: H/L – logikai 1/0 meghajtás, Z – nagyimpedanciás állapot, U/D – logikai 1/0 érzékelés, X – érzékelés, „don't care" állapot) |
| ***PIOMAP*** | Párhuzamos tesztminta esetén PIO oszlopokat rendel hozzá logikai kivezetésekhez. Megadja, hogy azok bemenetek vagy kimenetek. |
| ***RUNTEST*** | Futtatás állapotba kényszeríti az IEEE 1149.1 busz meghatározott számú órajelig vagy egy meghatározott időtartamra. |
| ***SDR*** | Az IEEE 1149.1 adatregiszterének (DR) kiolvasását végzi. |
| ***SIR*** | Az IEEE 1149.1 utasításregiszterének (IR) kiolvasását végzi. |
| ***STATE*** | Az IEEE 1149.1 buszt egy meghatározott stabil állapotba kényszeríti. |
| ***TDR*** | Meghatározza az DR figyelési (scan) műveletek végéhez csatolt kivezető mintát (Trailer Data Register). |
| ***TIR*** | Meghatározza az IR figyelési (scan) műveletek végéhez csatolt kivezető mintát (Trailer Instruction Register). |
| ***TRST*** | Az opcionális TRST vonalat vezérli. |

*1. Táblázat: Az SVF parancsok listája, saját szerkesztés [10] alapján*

## A SOROS VEKTOROS FORMÁTUM PARANCSRENDSZERÉNEK JAVASOLT KIEGÉSZÍTÉSE KEVERT JELŰ TESZTELÉSHEZ

A javaslat célja, hogy egy olyan kiegészítő parancskészlet kerüljön a specifikációban rögzített parancsrendszerbe, amellyel a megfelelő képességekkel ellátott tesztvezérlő képes analóg (áram) gerjesztőjelek előállítására, és analóg (feszültség) válaszjelek érzékelésére. Ez a javasolt kiegészítő parancskészlet egy lehetséges módszert kínál az előzőekben említett, kevert jelű peremfigyelést támogató áramkör működtetésére. A parancslista az ott leírt lehetőségeket nem fedi le teljesen, de véleményem szerint a két megoldás együtt használva egy gyakorlatban is működőképes, hatékony módszer alapjait teheti le. Ugyanez a parancslista integrálható a korábbi cikkemben [8] ismertetett naplózó és öntesztelő rendszerben is, amely az alapvető analóg vizsgálatokra megfelelő lehet. Mindkét itt említett alkalmazásban, és egyéb alkalmazásokban is elmondható, hogy a kiegészítő parancsok listája az SVF specifikáció és az alábbi logika szerint tovább bővíthető. A javasolt parancsrendszer-elemeket a következő táblázat tartalmazza.

| SVF parancs és paramétere(i) | A parancs működése |
|---|---|
| ***GDC*** (*dci*) | Áramgenerátorral *dci* nagyságú egyenáram létrehozása az AT1 vezetékrendszeren. (*dci* értékét µA-ben kell megadni) |
| ***GAC*** (*aci*) (*freq*) | Áramgenerátorral *aci* csúcsértékű, *freq* frekvenciájú, szinusz jelalakú áram létrehozása az AT1 vezetékrendszeren. (a*ci* értékét µA-ben, *freq* értékét Hz-ben kell megadni) |
| ***MDC*** (*vmean*) | Egyenfeszültség (egyszerű középérték) mérése az AT2 vezetékrendszeren, a mérési eredmény *vmean* változóba kerül. (*vmean* mV-ban kerül kiadásra) |
| ***MAC*** *(vpeak)* | Váltakozó feszültség csúcsértékének mérése az AT2 vezetékrendszeren, a mérési eredmény a *vpeak* változóba kerül. (*vpeak* mV-ban kerül kiadásra) |
| ***WAIT*** *(time)* | Várakozás a tesztprogram végrehajtásában *time* ideig. (*time* értékét µs-ban kell megadni) |

*2. Táblázat: Az SVF jelenlegi parancsrendszerének kibővítésére javasolt parancsok, saját szerkesztés*

## PÉLDÁK A JAVASOLT PARANCSRENDSZER-ELEMEK HASZNÁLATÁVAL TÖRTÉNŐ MÉRÉSEKRE

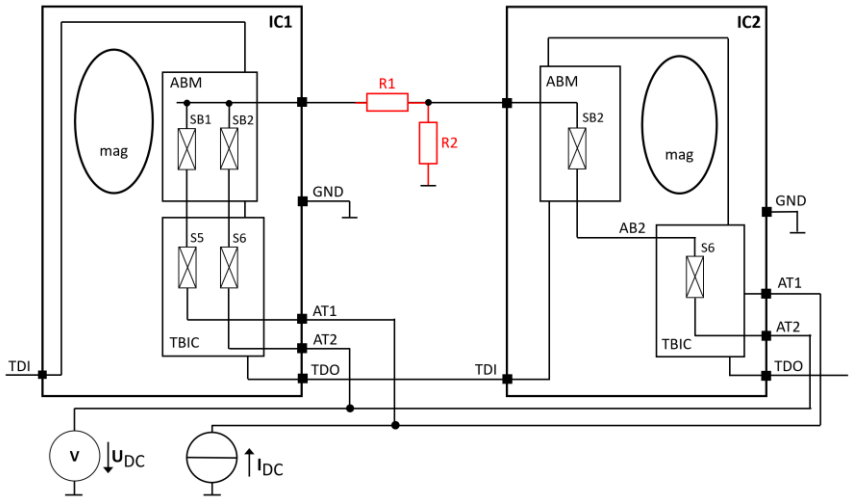
A következőkben az új parancsrendszer-elemek használatára kidolgozott számos példából két egyszerűbbet ismertetek. Ezek általános, de a valóságos áramkörökben is előforduló alapáramkörök paramétereinek mérését mutatják be. Terjedelmi okok miatt az alkalmazhatóság vizsgálatára kidolgozott számos példából csak hármat mutatok be. A példákat szemléltető ábrán csak a mérés szempontjából fontos részletek vannak kirajzolva, a kapcsolók közül is többnyire csak azok, amelyeket használok az adott mérésnél. Az alábbiakban ismertetett tesztprogramokban fel kell használni néhány, az IEEE 1149.4 szabványban definiált parancsot, ezek (és hexadecimális kódjuk) a következők:

| Parancs | A parancs kódja |
|---|---|
| ***BYPASS*** | *0xF* |
| ***EXTEST*** | *0x0* |
| ***SAMPLE/PRELOAD*** | *0xC* |
| ***PROBE*** | *0xA* |

*3. Táblázat: A felhasznált IEEE 1149.4 utasítások és kódjuk, saját szerkesztés [1] alapján*

**Feszültségosztó ellenállásainak meghatározása két integrált áramkör között**

A probléma vázlatát az 1. ábra mutatja.




*1. Ábra: Ellenállásosztó mérése két integrált áramkör között, saját szerkesztés*

Az ábrázolt részletben két integrált áramkör van (IC1 és IC2), és az SVF fájl megírásához feltételezem, hogy a peremfigyeléses láncban előttük és utánuk sincs másik integrált áramkör. A feladat a pirossal jelölt R1 és R2 ellenállások értékének meghatározása. Ez egy feszültségosztó, a meghajtás és az osztási pont analóg funkcionális pontra csatlakozik, az osztó alsó ellenállása pedig földre. IC1 és IC2 szimbólumán lévő kitöltött kis fekete négyzetek a kivezetések. A magáramkör az ABM[2]-eken keresztül csatlakozik ezekre a kivezetésekre. A feszültségosztó egy nagyon egyszerű analóg klaszternek tekinthető, ha a digitális klaszterek szemléletmódját kiterjesztem az analóg áramkörökre.

A méréshez szükséges SVF fájl, amely használja az új, javasolt parancsrendszer-elemeket is, a 2. ábrán látható. (A sorok elején található sorszámozás csupán az azonosítást szolgálja, szintaktikailag a program ebben a formában helytelen.)

A program 13…15. és 21…24. sorában alkalmazom az általam javasolt új parancsrendszer-elemeket. A fájlban hivatkozott, kapcsolókat vezérlő minták (p0, P0, p1, P1, p3 és P3) értékeit [1] 29. oldalán található Table 1 és 47. oldalán található Table 6 alapján határoztam meg. A mérés során tehát a gerjesztés hatására létrejövő feszültséget mérjük először az osztó két elemén együtt ($U_1$), majd csak R2-n ($U_2$). Mindkét mérési fázisban 3 vezetékes mérést valósít meg a program, ez kedvezően befolyásolja a mérés állandó hibáját. R1 és R2 a következőképpen számítható ki:

$$R_1 = \frac{U_1 - U_2}{100\ \mu A}$$

$$R_2 = \frac{U_2}{100\ \mu A}$$

[2] Analog Boundary Module, analóg peremfigyelő cella

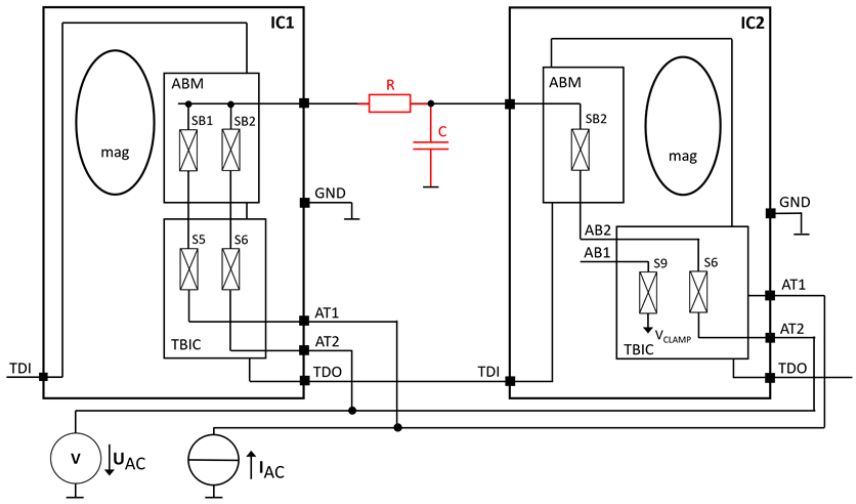
```
1.  TRST ON;                          // alaphelyzetbe állítás
2.  TRST OFF;
3.  ENDIR IDLE;                       // az utasítás-küldés végállapota: IDLE
4.  ENDDR IDLE;                       // az adatküldés végállapota: IDLE
5.  HDR 0;                            // TDO irányban IC2 után nincs több
6.                                    // alkatrész a BSC vonalon, nincs fejléc
7.  TDR 0;                            // TDI irányban IC1 előtt nincs több
8.                                    // alkatrész a BSC vonalon, nincs kivezető
9.  SDR 16 TDI (3300) SMASK (FFFF);   // IC1 ABM: p3 (SB1, SB2 bekapcsol)
10.                                   // IC1 TBIC: P3 (S5, S6 bekapcsol)
11.                                   // IC2 ABM: p0 (minden kikapcsol)
12.                                   // IC2 TBIC: P0 (minden kikapcsol)
13. GDC 100;                          // AT1-re 100 µA DC generálása
14. WAIT 20;                          // várakozás állandósulásra 20 µs
15. MDC U1;                           // AT2-n DC feszültség mérése
16.                                   // eredmény az U1 változóba
17. SDR 16 TDI (2211) SMASK (FFFF);   // IC1 ABM: p2 (SB1 bekapcsol)
18.                                   // IC1 TBIC: P2 (S5, S10 bekapcsol)
19.                                   // IC2 ABM: p1 (SB2 bekapcsol)
20.                                   // IC2 TBIC: P1 (S6, S9 bekapcsol)
21. WAIT 20;                          // várakozás állandósulásra, 20 µs
22. MDC U2;                           // AT2-n DC feszültség mérése
23.                                   // eredmény az U2 változóba
24. GDC 0;                            // áramgenerátor kikapcsolása
25. TRST ON;                          // alaphelyzetbe állítás
```

*2. Ábra: SVF fájl egy ellenállásosztó elemeinek megméréséhez, saját szerkesztés*

**RC tag elemeinek meghatározása két integrált áramkör funkcionális pontjai között**

A probléma vázlatát az alábbi ábra mutatja. Az ábrázolt részletben két integrált áramkör van (IC1 és IC2), és az SVF fájl megírásához feltételezem, hogy a peremfigyeléses láncban előttük és utánuk sincs másik integrált áramkör.

A feladat a pirossal jelölt R és C elemek értékének meghatározása. Ez egy olyan RC tag, amelynél a meghajtás és az R és C elemek közös pontja analóg funkcionális pontra csatlakozik, a kondenzátor másik kivezetése pedig földre. IC1 és IC2 szimbólumán lévő kitöltött kis fekete négyzetek a kivezetések. A magáramkör az ABM-eken keresztül csatlakozik ezekre a kivezetésekre. Ennél a mérésnél AC gerjesztésre van szükség, és a megjelenő feszültség is AC jellegű. Az ábrán rajztechnikai okokból IC1 S10 kapcsolója nincs feltüntetve, az a mérés második fázisában zavarjel csökkentési célt szolgál ($V_{CLAMP}$-ot kapcsolja AB2-re). Ugyanebből a célból a mérés második fázisában IC2 S9 kapcsolója AB1-re kapcsolja $V_{CLAMP}$-ot (ez a kapcsoló szerepel a rajzon).




*3. Ábra: RC tag elemeinek mérése két integrált áramkör között, saját szerkesztés*

A méréshez szükséges SVF fájl, amely használja az új, javasolt parancsrendszer-elemeket is, az alábbi ábrán látható. (A sorok elején található sorszámozás csupán az azonosítást szolgálja, szintaktikailag a program ebben a formában helytelen.)

```
1.  TRST ON;                              // alaphelyzetbe állítás
2.  TRST OFF;
3.  ENDIR IDLE;                           // az utasítás-küldés végállapota: IDLE
4.  ENDDR IDLE;                           // az adatküldés végállapota: IDLE
5.  HDR 0;                                // TDO irányban IC2 után nincs több
6.                                        // alkatrész a BSC vonalon, nincs fejléc
7.  TDR 0;                                // TDI irányban IC1 előtt nincs több
8.                                        // alkatrész a BSC vonalon, nincs kivezető
9.  SDR 16 TDI (3300) SMASK (FFFF); // IC1 ABM: p3 (SB1, SB2 bekapcsol)
10.                                       // IC1 TBIC: P3 (S5, S6 bekapcsol)
11.                                       // IC2 ABM: p0 (minden kikapcsol)
12.                                       // IC2 TBIC: P0 (minden kikapcsol)
13. GAC 100, f1;                          // AT1-re 100 µA csúcsértékű, f1 frekvenciájú
14.                                       // szinuszos áram generálása
15. WAIT 20;                              // várakozás állandósulásra, 20 µs
16. MAC U1;                               // AT2-n AC feszültség csúcsértékének mérése
17.                                       // eredmény az U1 változóba
18. SDR 16 TDI (2211) SMASK (FFFF); // IC1 ABM: p2 (SB1 bekapcsol)
19.                                       // IC1 TBIC: P2 (S5és S10 bekapcsol)
20.                                       // IC2 ABM: p1 (SB2 bekapcsol)
21.                                       // IC2 TBIC: P1 (S6 és S9 bekapcsol)
22. WAIT 20;                              // várakozás állandósulásra, 20 µs
23. MAC U2;                               // AT2-n AC feszültség csúcsértékének mérése
24.                                       // eredmény az U2 változóba
25. GAC 0;                                // AC áramgenerátor kikapcsolása
26. TRST ON;                              // alaphelyzetbe állítás
```

*4. Ábra: SVF fájl egy RC tag elemeinek megméréséhez, saját szerkesztés*

A fájlban hivatkozott, kapcsolókat vezérlő minták (p0, P0, p1, P1, p2, P2, p3 és P3) értékeit [1] 29. oldalán található Table 1 és 47. oldalán található Table 6 alapján határoztam meg. A mérés során tehát az AC gerjesztés hatására létrejövő feszültséget (annak csúcsértékét) mérjük először az RC tag bemenetén ($U_1$), majd csak C-n ($U_2$). Az alábbiakban általános esetre $f_1$ a gerjesztőáram frekvenciája, $I_1$ a gerjesztőáram csúcsértéke. $U_1$ és $U_2$ ismeretében a két elem, R és C értéke a következőképpen határozható meg[3] ($Z_1$ az RC tag impedanciája $f_1$ frekvencián, $\omega_0$ pedig a töréspponti körfrekvencia):

$$\omega_0 = \frac{1}{RC}$$

$$\omega_1 = 2 \cdot \pi \cdot f_1$$

$$\bar{Z}(\omega) = R + \frac{1}{j\omega C} = R\left(1 + \frac{1}{j\frac{\omega}{\omega_0}}\right)$$

$$|U_1| = I \cdot |\bar{Z}(\omega_1)| = I \cdot Z_1 \rightarrow Z_1 = \frac{U_1}{I}$$

$$|U_2| = I \cdot \frac{1}{\omega_1 \cdot C} \rightarrow C = \frac{I}{\omega_1 \cdot U_2}$$

$$Z_1 = |\bar{Z}(\omega_1)| = R \cdot \frac{\sqrt{\omega_0^2 + \omega_1^2}}{\omega_1} \rightarrow R = \frac{1}{\omega_1 \cdot C} \cdot \sqrt{\omega_1^2 \cdot C^2 \cdot Z_1^2 - 1}$$

**Általános négypólus (általános analóg klaszter) paramétereinek meghatározása és egyéb alkalmazások**

Korábbi cikkemben [11] elemzést végeztem, amelyben azt igyekeztem kutatni és igazolni, hogy a kevert jelű peremfigyelés módszerével elvégezhető-e egy általános négypólus paramétereinek meghatározása a kevert jelű peremfigyeléssel. A legelterjedtebb Z paraméteres leírást, használtam fel a modellezés és a vizsgálataim során, amely – mint kiderült – mérési oldalról kiválóan illeszkedik a kevert jelű peremfigyeléssel megvalósítható mérésekhez. A paraméterek meghatározása során a fenti egyenletek szerint, különböző csoportokba sorolható négypólusok esetén a következő feladatok vannak:

- Lineáris, reaktív elemet nem tartalmazó négypólusok esetén a gerjesztés DC vagy AC áram, mérni DC vagy AC feszültséget kell.
- Lineáris, reaktív elemet tartalmazó négypólusok esetén a gerjesztés AC áram, mérni AC feszültséget kell. A frekvenciafüggés megállapításához több mérési ponton (több frekvencián) meg kell határozni az átvitelt.
- A nemlineáris, frekvencia-független négypólusok esetén a gerjesztés lehet DC áram, a gerjesztő áram különböző értékeinél kell feszültséget mérni. Az áram változtatására a nemlineáris viselkedés meghatározása érdekében van szükség. A nemlineáris, frekvencia-független négypólusok AC gerjesztéssel is mérhetőek, ahogyan azt a következő pontban ismertetem.

[3] A levezetés néhány lépését a tömörség miatt összevontam vagy kihagytam

- A nemlineáris frekvenciafüggő négypólusokat (szinuszos) AC gerjesztéssel kell meghajtani. A lineáris torzítás miatt a gerjesztés hatására létrejövő válasz-feszültség felharmonikusokat fog tartalmazni, amelyek értékéből lehet következtetni a négypólus felépítésére. Azaz ebben az esetben nem egyszerűen AC feszültséget kell mérni, hanem meg kell határozni a válasz-feszültség spektrumát. Erre a célra jól implementálható algoritmusok állnak rendelkezésre (pl. FFT), amelyek a mérésvezérlőben leprogramozhatóak.
- A felsorolásból, és a korábbi cikkemben [11] megtalálható Z paraméterek meghatározására szolgáló egyenletekből jól látható, hogy a fenti példákban leírt módszerrel és az SVF kiegészítésére javasolt parancsokkal a mérések elvégezhetőek. Az általános négypólusok méréséhez szükséges ABM és TBIC[4] kapcsoló vezérléseket, valamint a mérés során felmerülő problémákat és azok megoldását részletesen tartalmazza a cikkem, [11] a részletek ismertetésétől itt terjedelmi okok miatt eltekintek.

Az ismertetett módszer hibahely-behatárolásra a következő módon és lépésekben használható:

1. A vizsgálandó áramkört négypólusokra (kétpólus-párokra) bontjuk fel, amelyek bemeneti és kimeneti kapcsait (4 darab) egy-egy analóg peremfigyelés-cellára (ABM) kötjük.
2. Megfelelő mérési eljárást és a négypóluselmélet módszereit alkalmazva megállapíthatóak a négypólus paraméterei, amelyekből következtetni lehet annak hibátlanságára, vagy az esetleges meghibásodásra, illetve annak jellegére.
3. A mérést a kevert jelű peremfigyeléses technika alkalmazásával úgy lehet megvalósítani, ha a peremfigyelés-vezérlőtől érkező parancsok alapján a peremfigyelő cellák felől a megfelelő meghajtást és érzékelést biztosítjuk. A mérőjeleket és az érzékelést szintén a peremfigyelés vezérlőnek kell megvalósítania.

A 2. pontban említett négypóluselmélet módszereinek alkalmazása esetünkben a következőket jelenti:

1. Az egyszerű négypólusok, azok paraméterei, valamint a négypólusok összekapcsolásának szabályait ismerve meghatározzuk az eredő (mérendő) négypólus paramétereit.
2. A fenti tényezők ismeretében meghatározzuk a mérendő négypólus átviteli jellemzőit.
3. Elvégezzük a paraméterek és/vagy az átviteli jellemzők mérését, illetve meghatározását.
4. A kapott eredmények, illetve a számítással meghatározott négypólus-jellemzőket összevetve meghatározzuk, hogy a vizsgált négypólus hibás-e vagy hibátlan, azaz a mérési eredmények eltérése a helyes értékektől megengedett hibahatáron belül van-e.

[4] Test Bus Interface Circuit, tesztbuszra csatlakozás áramköre

5. Amennyiben a vizsgált négypólus hibás, a mért jellemzők alapján szintetizáljuk négypólust (vagy helyettesítő képét), azaz meghatározzuk az azt felépítő elemek paramétereit.
6. A paraméterek eltérése alapján behatároljuk a hibahelyet.

Rövid listát állítottam össze, hogy (a teljesség igénye nélkül) milyen egyéb analóg paraméterek mérhetőek még az új, javasolt SVF parancskészlet segítségével. A fentiekhez hasonló részletes esettanulmányt terjedelmi okokból nem közlök.

Erősítő paraméterek
- bemeneti ellenállás
- kimeneti ellenállás
- feszültség erősítés

Komparátor paraméterek
- billenési szintek
- hiszterézis

Szűrő paraméterek
- törésponti frekvencia
- sávszélesség
- oldalmeredekség

## ÖSSZEFOGLALÁS

Megvizsgáltam a soros vektoros formátum (SVF) parancsrendszerét, meghatároztam a parancskészlet hiányosságait, amely jelenleg nem teszi megfelelővé a kevert jelű (IEEE 1149.4 szabványú) peremfigyelésben való alkalmazásra. Tanulmányozva a kevert jelű peremfigyelés módszerét, hangsúlyosan a gerjesztőjel előállításával és a válaszjel érzékelésével kapcsolatos igényeket, meghatároztam egy kiegészítő parancskészletet, amellyel feltételezésem szerint elvégezhetőek a gerjesztés és az érzékelés során adódó feladatok. Ezek után néhány tipikus parametrikus mérésnél esettanulmányokat végeztem, és vizsgáltam a kiegészítő parancskészlet használhatóságát. A cél az volt, hogy megállapítsam, hogy elegendő-e a parancskészlet 5 új parancsa, és ha nem, akkor meghatározzam a hiányosságokat.

Ezek után megkíséreltem a fenti elvet általánosítani, és megfogalmazni, hogy milyen elvek mentén lehet egy tetszőleges négypólus (jelen szemléletmódban analóg klaszter) paramétereinek a normális tartománytól való eltérését meghatározni, majd a mérés alapján a négypóluson belül a hibahelyet behatárolni. Közöltem még néhány egyéb analóg paramétert, amelyet mérni lehet. Úgy értékelem, hogy a munkám során sikerült kialakítani egy jól használható kiegészítő parancskészletet, amelynek alkalmazhatóságát vizsgálataim során igazoltam. Összefüggést találtam korábbi kutatásaimmal: a javasolt kiegészítő parancskészlet egy lehetséges módszert kínál a korábban említett, kevert jelű peremfigyelést támogató áramkör működtetésére, a két megoldást együttes használata egy gyakorlatban is működőképes, hatékony módszer alapjait teheti le. A kiegészítő parancslista integrálható a korábbi ide kapcsolódó kutatásaimnál röviden ismertetett naplózó és öntesztelő rendszerben is, amely az alapvető analóg vizsgálatokra megfelelő lehet.

Eredményként kiemelném a soros vektoros formátum specifikációjába illeszthető, kiegészítő parancskészletet, amely támogatja a kevert jelű peremfigyelés analóg méréseinek elvégzését azzal, hogy lehetővé teszi változatos gerjesztő jelek előállítását, és a válaszfeszültségek érzékelését, megmérését. Javaslom, hogy a tesztelési módszerek fejlesztését végző kutatók fontolják meg a soros vektoros formátum kibővítését az általam javasolt alapokon elindulva, amellyel hatékonyabbá tehető az analóg áramköri elemek vizsgálata, különösen a kevert jelű peremfigyelést támogató áramkörrel együtt használva.

## FELHASZNÁLT SZABVÁNYOK

[1] IEEE Standard for Test Access Port and Boundary-Scan Architecture, IEEE Std 1149.1-2013, IEEE Computer Society, New York, 2013.
[2] IEEE Standard for a Mixed-Signal Test Bus, IEEE Std 1149.4-2010, IEEE Computer Society, New York, 2011

## FELHASZNÁLT IRODALOM

[3] J.C. Knight, Safety critical systems: challenges and directions, Orlando, IEEE, 2002.
[4] Kenneth P. Parker, The Boundary-Scan Handbook, Switzerland, Springer International Publishing, 2016.
[5] Harry Bleeker, Frans de Jong és Peter van den Eijnden, Boundary Scan Test - A Practical Approach, Dordrecht, Kluwer Academic Publishers, 2001.
[6] Texas Instruments Inc., IEEE Std 1149.1 (JTAG) Testability Primer, Dallas, Texas Instruments, 1997.
[7] Molnár Zsolt, Analóg áramkörök beépített öntesztbe vonását támogató integrált áramkör, presented at the XXV. Kandó Konferencia, Budapest, 2009.
[8] Zsolt Molnár, Logging the operation and enhancing the reliability of safety-critical embedded systems using self-test, Interdisciplinary Description of Complex Systems, 17 3A pp 492-496, 2019
[9] Manoj Sachdev, A realistic defect oriented testability methodology for analog circuits, Journal of Electronic Testing, 6, pp. 265-276, 1995.
[10] ASSET InterTech, Inc., „Serial Vector Format Specification," in ASSET InterTech, Inc., Plano, 1999.
[11] Molnár Zsolt, Analog cluster test using mixed signal boundary scan test method, presented at the Proceedings of Factory Automation 2013., Veszprém, 2013.

# IDENTIFICATION OF CHROMATOGRAPHIC PARAMETERS FOR BLISTER AGENTS IN THE LOW DIESEL OIL CONTAMINATION

# HÓLYAGHÚZÓ HARCANYAGOK GÁZKROMATOGRÁFIÁS PARAMÉTEREINEK AZONOSÍTÁSA ALACSONY DÍZELOLAJSZENNYEZETTSÉG MELLETT

NAGY Rudolf[1]

**Abstract**

Thanks to the ongoing conflict in the Eastern region of Europe and the resulting confrontation between the great powers, the danger of a potential conflict involving the use of chemical weapons has also increased. After all, this is only one step away from organizing provocations intended to justify the use of chemical weapons and presenting them to the public in the media. So, in the new wars that broke out in the conflict zones of the world because of power struggles, there were more and more signs that the opposing parties were seriously considering the possibility of developments moving in this direction. In addition, terrorist organizations have already acquired the ability to produce this type of weapon. Thus, initiatives aiming at the development of high-sensitivity, fast analytical methods suitable for detecting these substances even from contaminated samples have received significant emphasis.

**Keywords**

warfare agents, diesel oil, GC, Lewisite, sulfur mustard

**Absztrakt**

Köszönhetően Európa keleti régiójában jelenleg is zajló konfliktusnak és az ennek nyomán fokozódó, a nagyhatalmak közötti szemben állásnak megnőtt a veszélye egy vegyifegyverek alkalmazásával végrehajtott esetleges összeütközés lehetőségének is. Hiszen ez már csak egy lépésre van a vegyi fegyverek bevetését igazolni szándékozó provokációk megszervezésétől és annak a közvélemény számára médiában történő tálalásától. Tehát a világ konfliktus övezeteiben a hatalmi viszályok nyomán kirobbantott újabb háborúkban egyre több jel utalt arra, hogy a szembenálló felek komolyan számolnak a fejlemények ilyen irányba történő elmozdulásának lehetőségével. Ráadásul e fegyverfajta előállításának képességére a már a terrorszervezetek is szert tettek. Így ismételten jelentős hangsúlyt kaptak az ezen anyagok akár szennyezett mintákból történő detektálására is alkalmas, nagy érzékenységű, gyors elemző módszerek fejlesztését célzó kezdeményezések.

**Kulcsszavak**

mérgező harcanyag, diesel olaj, GC, Lewisite, kénmustár

[1] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728| habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary| habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## INTRODUCTION

Although in recent decades the confrontation between the states that were at the forefront of the development of intensive chemical weapons has begun to ease, today we can see the reawakening of the previous antagonisms. The confidence-building steps that started the disarmament processes that brought significant results at the time completely dissipated and were replaced by considerations ready to intensify the confrontation. In addition to creating tension, very disconcerting news is coming from the conflict zones, which suggests that not all actors wish to submit to the intention to limit the spread of chemical weapons. These unfavorable signs prompted me to publish the previously unpublished results of my experiments conducted in the early 90's in the framework of training at the military CBRN department. These results were indeed obtained in my previous experiments as part of my thesis, but the applied validated methodology also makes it possible to reproduce and compare them in today's researches. [1]

Similar to the desperate battles in the battlefield reports we have seen now, we have already seen in other conflict zones of the world, as a result of which a party hoped to seize the strategic initiative from the deployment of chemical weapons in more than one case. However, the initial use of surprise strikes with local targets always resulted in extensive mass deployments. Many toxic munitions thus released onto the battlefield can often claim their victims not only during the period of direct military conflict but also long after. As shown by the confirmed degenerative changes in the population caused by the massively applied vegetation-destroying toxic warfare agents after the Vietnam War. Of course, in this case, the dioxin left over from the preparation is held responsible as a substance that permanently pollutes the soil, which does not qualify as a chemical weapon according to international conventions. [2]

However, we also find similarly stable, long-lasting types of toxic warfare agents in a wide range of chemical weapons, such as, for example, blistering compounds, starting from sulfur mustard to nitrogen mustard and including phosgene oxime, as well as recipes made by combining them. Sulfur mustard and lewisite occupy a prominent place in this category. Both have been known since the beginnings of extensive battlefield chemical warfare in the First World War. [3]

This early realization, however, aroused the interest of the Spanish, Japanese, and Italian nationalist leaders who were reviving their colonialist aspirations, and wanted to offset the numerical superiority of the masses of the Moroccan, Manchurian, and Ethiopian national resistance. [4] [5]

Our experience since then has also shown that the applicability of blister agents is significantly affected by environmental conditions. However, the increased environmental stability of the chemical substances classified in the category of these munitions has given these compounds a particularly great military importance in terms of the capture of the troops located in the combat activity area affected by the chemical attack, causing a decrease in their military capability. In addition, we can count on possible pollution of this kind in the case of accidental emissions following attacks on chemical weapons manufacturing facilities. As a result, their so-called persistence is permanent, producing environmental pollution that appears long after the end of the military conflict. [6]

As a result of the discouraging experiences on the battlefield, they were not deployed during the Second World War, despite the considerable amount of stockpiled on

the European battlefields on both sides. However, certain contingents of the arsenal, which did not fulfill their purpose at the time, have retained their potential danger to this day, as shown by the example of the thousands of tons of munitions filled with war material sunk into the Baltic Sea. [7]

Similarly, easily identifiable pollution can be found on the training grounds serving as the scene of combat exercises carried out with sharp, toxic munitions. Due to the repeated pollution here for decades, zones indicating the enrichment of toxic munitions, which often show a significant concentration, can be found even down to the deeper layers of the soil, which can, by definition, also affect the surface waters. We have precisely developed procedures for the risk assessment of pollution causing environmental hazards in these areas. [8] [9]

Given that some of the toxic munitions and their decomposition products have a corrosive effect on the structural materials of the stored ammunition. The rate of even this structural damage is relatively low, but due to the typically long storage cycle, the corrosion process can lead to contamination caused by unexpected damage. Although these factors are indeed considered during the development of the military-technical parameters of the toxic munitions intended for use or of the recipes combined with their additives, as well as strict and regular inspections are required by military standards during long-term storage. [10]

The elaborated storage provisions are created by considering many factors. As can be deduced from the previous ones, the duration of storage of the blistering agents also depends on the possible technological impurities in them, i.e., the degree of purity of the product. In general, we can consider that the cleaner the munitions are, the longer they can be stored. Therefore, for example, in the case of technical sulfur mustard produced in countries that do not have the appropriate production technology, damage to the chemical warfare material may be more likely than if it were replaced with distilled sulfur mustard. By adding stabilizers, the storability of toxic warfare agents and their mixtures can be increased. Safe storability can be further enhanced by adding stabilizers, but even so, chemical weapons stockpiles are renewed after the cycle time determined by the manufacturer's quality inspections. Stocks of ammunition with an expired storage period are subject to review based on military-technical requirements, and non-compliant stocks are disposed of using special procedures. [11]

As it is well known, in such battlefield conditions, the weapons technology devices that make up chemical weapons are gradually exposed to changing environmental effects. Of course, despite the relevant military logistics regulations at resupply and temporary supply points aimed at serving combat activities, it cannot be ruled out that there may have been contamination from leakage. Not to mention the strikes on chemical munitions stocks in combat conditions, which can also contaminate those preparing to deploy the munitions themselves. [12]

Unused chemical weapons stockpiles destined for destruction pose additional challenges for highly toxic vesicular agents. The technologies developed for this carry the risk of exposure due to the disintegration of weapons materials, as well as munitions that may be released into the environment through possible technological disruptions. In this case, it is essential to use detection procedures that ensure adequate and continuous control. [13] [14]

However, it is not always so obvious to identify the presence of toxic warfare agents. This can primarily occur in environments where the toxic munitions may have been present in much lower concentrations, such as traces found on surfaces in contact with toxic munitions left over from the illicit trade of chemical weapons containing toxic munitions. [15] The hidden nature makes detection even more difficult if the use of toxic munitions must be justified in the investigation of the implementation of special secret service operations against terrorist organizations. [16]

However, even its occasional use in a covert or unrecognized manner on the battlefield or against the civilian population can often only be reconstructed from samples containing hard-to-identify remains. [17] Proof of this can be particularly important to validate possible war crimes. Credibility in such matters is a fundamental condition in the subsequent evidentiary procedure, where the fact of guilt can only be supported with irrefutable evidence. [18] In the case of war crimes that violate international law, it is possible to consider the factors of chemical degradation caused by the time lag in sampling that takes place long after the events, which in itself is a big challenge. [19, 20]

Not only these but the disturbing effects of pollution that can generally occur in the area affected by the fighting must also be faced during detection. Among these, the most frequently found pollutant components come from hydrocarbon derivatives. This is especially true when we consider that oil mists are popularly used on the battlefield to conceal enemy visual observation. During their settling, these dispersed fogs cover a large area of the battlefield. [21]

Therefore, the extremely important goal of this work is to determine the test parameters for gas chromatographic identification of sulfur mustard and lewisite blistering munitions, which enable their separation in the presence of hydrocarbon derivatives. Thanks to its high sensitivity and the fact that it can be easily reconstructed in the field, the gas chromatography method was chosen as the test method of choice in this study. The evaluated results in this way can be called up at any time and compared with the results of others. [22]

## MATERIAL AND METHOD

During the training of chemical defense military officer students, the samples were based on the preparations of the mentioned compounds used in their chemical laboratory exercises for analytical reports, synthesized for training purposes by their own process. For the analysis of lewisite, the L-1 version was used. To determine the sulfur mustard, I worked using a distilled, highly pure product. This solvent is excellent at dissolving both the warfare agents and the diesel oil components used as contaminants in the test. For both substances, instead of the chemically pure state, I performed the measurements with their samples dissolved in an organic dichloromethane solvent. Test substances should be used at approximately 100-fold dilution to simulate low contamination. Adherence to the appropriate dilution ratio is important from the point of view of the effective evaluation of the peaks appearing in the chromatogram according to material components.

The use of the dichloromethane solvent during the measurements is justified by its low retention time and its applicability as an organic solvent proven in other tests. I simulated the oil spill with a mixture of the less volatile members of the saturated open-chain alkane series with 9-12 carbon atoms (nonane, decane, unodecane, and dodecane). The use

of personal protective equipment was essential for the safety of the laboratory work, as well as the disinfection of the used equipment with a calcium hypochlorite solution after the measurement.

The use of personal protective equipment was essential for the safety of laboratory work, as was the decontamination of the instruments used with a calcium hypochlorite solution after the measurement was completed.

## INSTRUMENTATION

I used an AMS Model-93 gas chromatograph for the determinations. This is a programmable, flame ionization detector equipped with a nitrogen carrier gas, and copper column, made in England. The 1.8 m long, 4 mm diameter separation column is filled with silicate material marked Chromosorb W-HP/100-120/, moistened with 4% SE-52 and 6% OV-210 separation fluid. The wetting fluid is chemically stable up to 300 °C. We can adjust the temperature of the column with an accuracy of ± 1 Co using a program. Thus, we had the opportunity to produce specific heat shocks. On the other hand, the temperature of the injector could be recorded electronically or manually with an accuracy of ± 50 Co. The syringe was a precision design, GL SGE (microfine) type.

With the help of the parameter adjustment system, it is possible to adjust the pressure of the gases coming from the gas tanks and to program the temperature of the injector and the column. The gas flow can be adjusted manually with an accuracy of ± 10 Pa. The $H_2$ and $O_2$ gas bottles are connected to the flame ionization detector, in the flame of which the tested sample is ionized. The instrument system used for the determination consists of the main components shown in Figure 1.

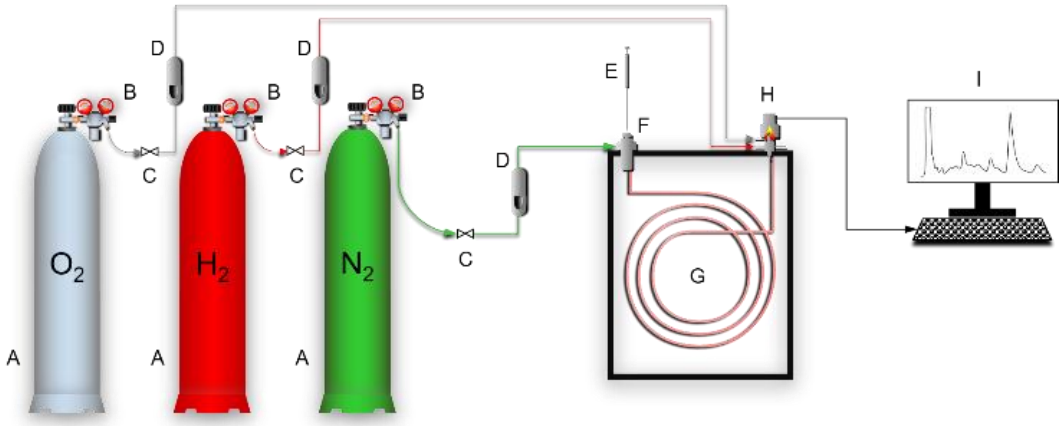



*Figure 1: Schematic diagram of GC equipment*
*Source: Edited by the author*
*A – Gas Cylinders, B – Gas Regulators, C – Pressure Regulators, D – Flow Controllers, E – Syringe, F – Injector, G – Column, H – Detector; I – Display System*

For all GC determinations, I used signal processing software connected to an IBM AT personal computer gas chromatography. The program supporting the evaluation of the signals from the gas chromatograph was the LabChrom software of Labinform Kft.

## ANALYSIS

Blistering toxic agents retain their effect for a longer or shorter period on the surface of the materials that come into contact with them or by being absorbed into them. To identify the permanent presence of the toxic substances that cause chemical pollution, various technical procedures have been developed in accordance with the goals to be achieved based on the detection of chemical pollution. A fundamental distinction between these results from the evaluation of the presence of toxic substances. Based on this, two main categories can be distinguished: subjective and objective methods.

Using subjective methods, we establish the presence of toxic substances through indicators. In many cases, non-organizational chemical reconnaissance soldiers must establish the presence of toxic substances in battlefield conditions without special chemical expertise. The participants learn chemical protection knowledge for handling the reconnaissance devices used for this purpose within the framework of a simple course. This typically means methods using detection tubes or paper test strips that show a color change following sampling from the polluted air using hand pumps, as illustrated in the following Figure 2. To monitor the color change, the reaction between the reagent with a non-obscuring base color and applied to the adsorbent placed in the detection tubes and the toxic warfare agent during the color change forms the basis of the detection. [23]

*Figure 2: Examples of detection tubes (VFK-66)*
*Source: Compiled by the author.*

At the same time, it should be noted that the toxic munitions adsorbed in this way may also be suitable for determining exposure values by interposing gas chromatographic analysis following dissolution by the appropriate method. However, to carry out the analytical work, sampling and sample handling carried out with sufficient precision are required, for which it is necessary the involvement of properly trained personnel. [24]

Objective methods require more sophisticated training and involve procedures supported by advanced laboratory techniques. They can use all the techniques available in modern analytical laboratories [25] Gas chromatography techniques, which follow a technology supported by standardised sampling procedures, are a prominent tool in military field or mobile chemical defence laboratories. [26]

The methods used here, based on the requirements of rapid detection and control of the chemical situation, make it essential to have the results in the database, which are the

basis for a pre-laid comparison based on research. The optimization study of the GC parameters carried out during this research was intended to ensure the fulfillment of the mentioned goals.

## CONCEPT FOR THE MEASUREMENT PROCEDURE

When determining the optimal parameters, I used members of the linear unsaturated alkane series with 12 carbon atoms, as I concluded from the literature data that the retention time of Lewisite and sulfur mustard falls within the range limited by the above-mentioned hydrocarbons [27] [28] [29]. At the beginning of the determination of the optimum, the starting parameters were planned to be set as follows:

- carrier gas pressure ($N_2$): 1.24 × 105 Pa
- column temperature: 250 °C
- injector temperature: 200 °C

In the future, I planned to reduce the column temperature by 50 oC, then adjust the values obtained by halving the temperature range. After determining the optimal temperature, I planned an increase or decrease of 1 × 103 Pa in the pressure of the carrier gas. I set the measurement execution time to 3 minutes, because the proper separation, and therefore the proper evaluation, can be achieved in this time by determining the optimal parameters. The other important factor that I considered when determining the duration of the measurement is that we need fast data provision during practical use.

## RESULTS AND DISCUSSIONS

It is an important observation that real samples are often contaminated with diesel fuel due to the fuel of combat and motor vehicles and other pollution sources already mentioned. Therefore, it is necessary to base the tests based on the analysis of the mixed samples of the interfering gas oil components, using the experimental conditions given by the choice of the standard measurement parameters.

I optimized the parameters of the measurement by dissolving a volume of 0.15 ml of the mixture of paraffin of the linear unsaturated alkane series with carbon numbers $C_9$-$C_{12}$ used for the measurements in 5 ml of solvent. The volume injected was 0.3 µl each time. Examining the effectiveness of the separation of the n-alkane components on the chromatograms, I found that the column temperatures of 250 °C, 200 °C and 150 °C are not suitable for the separation of the components. While the measurements performed at 140 °C showed well-appreciable differentiated peaks. Having recorded the obtained value on the device, I started recording the chromatogram of the substances to be tested. I fixed the parameters of the optimization as 1.245 × 105 Pa in terms of $N_2$ gas pressure.

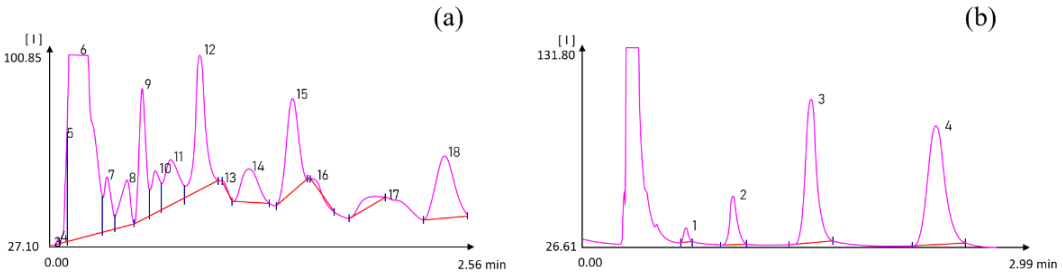



*Figure 3: Chromatograms of diesel fuel matrix (a) and linear unsaturated alkanes standard (b)*

| № | 9. | 12. | 15. | 18. |
|---|---|---|---|---|
| Component name | nonane | decane | undecane | dodecane |
| Retent.: (min) | 0.69 | 1.00 | 1.52 | 2.36 |
| Height: (I) | 50.72188 | 52.81673 | 35.92736 | 23.72249 |
| Rel.Hgt.: (%) | 4.93 | 5.14 | 3.49 | 2.31 |
| Integral: (min×I) | 127.4935 | 207.4846 | 163.6285 | 165.2154 |
| Rel.Int.: (%) | 2.78 | 4.52 | 3.56 | 3.68 |
| Int/Hgt.: (min) | 2.514 | 3.928 | 4.554 | 6.965 |
| Plate number: | 1067 | 466 | 1287 | 1502 |

*Table 1: Peak detection parameters of diesel fuel matrix (a)*

| № | 1. | 2. | 3. | 4. |
|---|---|---|---|---|
| Component name | nonane | decane | undecane | dodecane |
| Retent.: (min) | 0.696 | 1.011 | 1.528 | 2.368 |
| Height: (I) | 7.571232 | 25.89466 | 76.04636 | 63.08492 |
| Rel.Hgt.: (%) | 4.39 | 15.00 | 44.06 | 49.79 |
| Integral: (min×I) | 17.17122 | 89.91157 | 397.4881 | 500.2577 |
| Rel.Int.: (%) | 1.71 | 8.95 | 39.56 | 49.79 |
| Int/Hgt.: (min) | 2.268 | 3.472 | 5.227 | 7.930 |
| Plate number: | 1252 | 551 | 428 | 709 |

*Table 2: Peak detection parameters of linear unsaturated alkanes (b)*
*Source: Compiled by the author.*

The solvent identified by the number 6 in Figure 3(a) was not marked with a separate numerical value in the subsequent diagrams. Given that, thanks to its successful selection, it gave a signal producing an early elution without disturbing effects in the further stages of the analyses. By evaluating the characteristic peaks obtained from the data of the detected samples from diesel oil and appearing in the chromatograms of Figure 3(a), the retention times of pure n-alkanes, which are present in relatively large amounts and are also evaluated separately in Figure 3(b), are the four main diesel components, later, I performed the analysis of toxic munitions. The values obtained for the retention times of the peaks appearing in the mixture of the tested n-alkanes were obtained from the sample population as very close results that can also be read in Tables 1 and 2:

- $Rfc_9$= 0,689 min
- $Rfc_{10}$= 1.005 min

- $Rfc_{11}$= 1.522 min
- $Rfc_{12}$= 2.361 min

In order to record the basic values, I also carried out the pollution-free identification of Lewisite and sulfur mustard toxic munitions. In the volume composition of the solutions of the samples used here, the solvent was 0.5 µl. For this, in the case of Lewisite, the stock solutions used in the samples were prepared by dissolving 0.06 µl of t and then, leaving the amount of solvent unchanged, 0.09 µl of sulfur mustard. In each case, 0.3 µl of the solutions prepared in this way were injected per measurement.

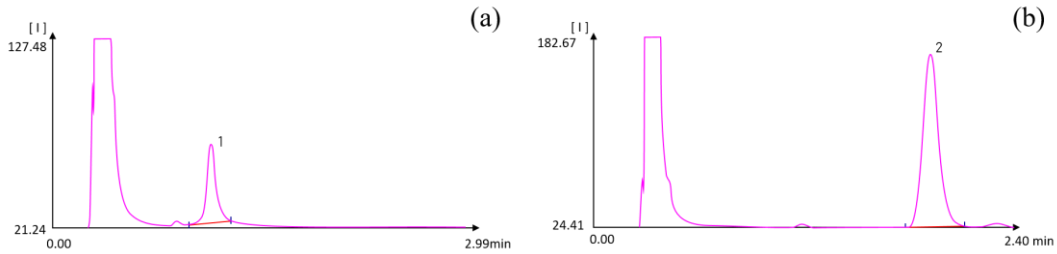



*Figure 4: Chromatograms of Lewisite (a) and sulfur mustard (b) with solvent*

| № | 1. | 2. |
|---|---|---|
| Component name | Lewisite ($L_1$) | Sulfur mustard (H) |
| Retent.: (min) | 1.114 | 1.894 |
| Height: (I) | 43.88408 | 144.9692 |
| Rel.Hgt.: (%) | 100.00 | 100.00 |
| Integral: (min×I) | 199.7884 | 914.1168 |
| Rel.Int.: (%) | 100.00 | 100.00 |
| Int/Hgt.: (min) | 4.553 | 6.306 |
| Plate number: | 239 | 520 |

*Table 3: Peak detection parameters of Lewisite (a) and Sulfur mustard (b)*
*Source: Compiled by the author.*

Evaluating the previously illustrated chromatograms, we can identify the following retention times for Lewisite in Figure 4(a) and sulfur mustard in Figure 4(b) (see Table 3.):

- $Rf_{L_1}$ = 1.097 min
- $Rf_{SM}$ = 1.897 min

After taking the chromatogram of the pure components and determining their retention time, the mixed samples were identified.

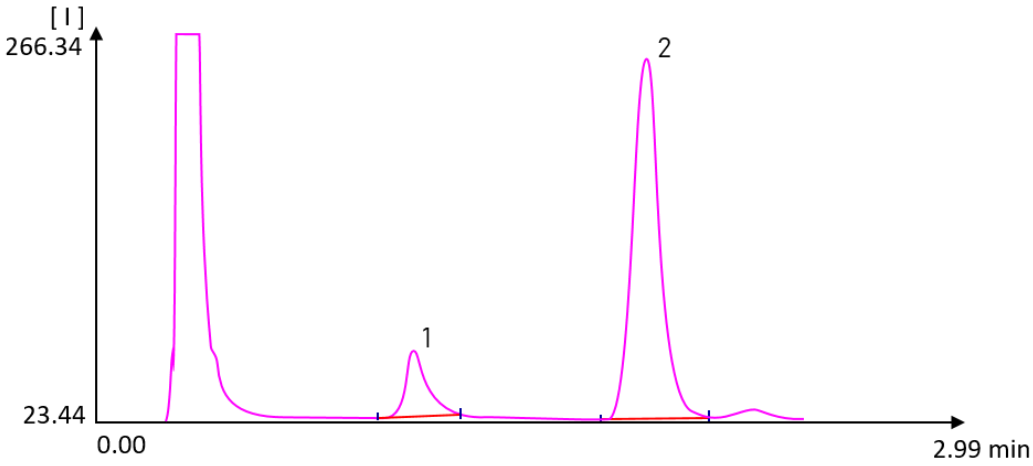



*Figure 5: Chromatogram of Lewisite and sulfur mustard mixture*

| № | 1. | 2. |
|---|---|---|
| Component name | Lewisite ($L_1$) | Sulfur mustard (H) |
| Retent.: (min) | 1.098 | 1.894 |
| Height: (I) | 41.65199 | 228.7282 |
| Rel.Hgt.: (%) | 15.40 | 84.60 |
| Integral: (min×I) | 216.3628 | 1493.571 |
| Rel.Int.: (%) | 12.65 | 87.35 |
| Int/Hgt.: (min) | 5.195 | 6.530 |
| Plate number: | 242 | 414 |

*Table 4: Peak detection parameters of Lewisite and Sulfur mustard mixture*
*Source: Compiled by the author.*

The chromatogram in Figure 5 clearly shows sufficient undisturbed separation (Table 4.) even in the simultaneous presence of both toxic warfare agents, which predicts their separability in samples contaminated with diesel.

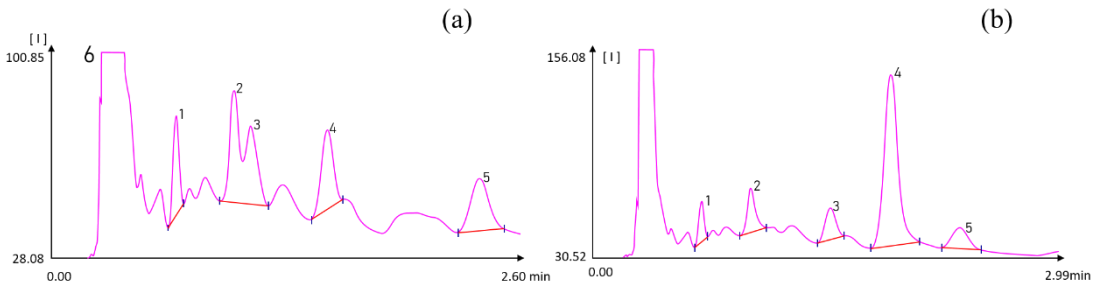



*Figure 6: Chromatograms of Lewisite (a) and sulfur mustard (b) in diesel fuel matrix*

| № | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|
| Component name | nonane | decane | Lewisite ($L_1$) | undecane | dodecane |
| Retent.: (min) | 0.681 | 1.002 | 1.097 | 1.523 | 2.373 |
| Height: (I) | 50.68088 | 57.03175 | 39.73513 | 40.05063 | 26.54458 |
| Rel.Hgt.: (%) | 23.68 | 26.64 | 18.56 | 18.71 | 12.40 |
| Integral: (min×I) | 117.2078 | 203.8490 | 190.6917 | 188.2663 | 190.4229 |
| Rel.Int.: (%) | 13.16 | 22.89 | 21.42 | 21.14 | 21.39 |
| Int/Hgt.: (min) | 2.313 | 3.574 | 4.799 | 4.701 | 7.174 |
| Plate number: | 1067 | 998 | 912 | 1199 | 1360 |

*Table 5: Peak detection parameters of Lewisite in diesel fuel matrix (a)*

| № | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|
| Component name | nonane | decane | undecane | Sulfur mustard (H) | dodec-ane |
| Retent.: (min) | 0.694 | 1.011 | 1.522 | 1.906 | 2.362 |
| Height: (I) | 24.92676 | 27.11155 | 19.46072 | 103.5742 | 12.57546 |
| Rel.Hgt.: (%) | 13.28 | 14.45 | 10.37 | 55.20 | 6.70 |
| Integral: (min×I) | 56.48465 | 99.81961 | 89.19949 | 660.4343 | 93.24816 |
| Rel.Int.: (%) | 5.65 | 9.99 | 8.93 | 66.10 | 9.33 |
| Int/Hgt.: (min) | 2.266 | 3.682 | 4.584 | 6.376 | 7.415 |
| Plate number: | 1108 | 564 | 1335 | 579 | 1377 |

*Table 6: Peak detection parameters of sulfur mustard in diesel fuel matrix (b)*
*Source: Compiled by the author.*

The peaks of the diesel components can be clearly identified on the emerging chromatograms. The appearance of Lewisite is consistent with literature sources between $C_{10}$ and $C_{11}$ in Figure 6(a). However, Lewisite, which appears here as peak 3, can be isolated with sufficient certainty by evaluating the chromatogram. However, the elution of the $C_{10}$ component of the diesel occurring here somewhat masks the Lewisite, which is well reflected by the very close retention times of the two components (Table 5).

At the same time, sulfur mustard, consistent with its longer-lasting battlefield persistence identifiable from military literature data, appeared much later and was clearly discernible. As can be read from Figure 6(b), sulfur mustard was detected in the range between $C_{11}$ and $C_{12}$ diesel oil components. This presupposes that it provides a suitable basis for detection from diesel-contaminated samples even in lower relative quantitative conditions.

However, sulfur mustard and Lewisite are used in military practice as so-called viscous mustard for greater persistence and adhesion. I also examined their simultaneous detectability with the polluting diesel oil in a mixed sample.

Among the signals transmitted by the detector, the peak of sulfur mustard stood out because it was present in high purity and in relatively larger quantities than the diesel components. An important factor was also the fact that were the peak of sulfur mustard appeared, there is no peak from interfering diesel components.

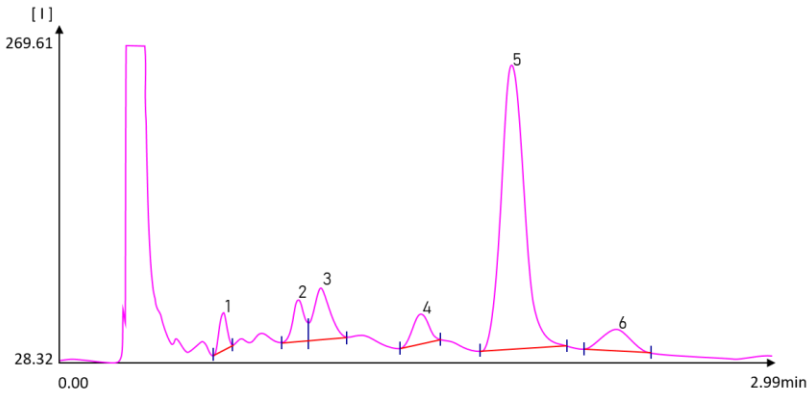



*Figure 7: Chromatogram of Lewisite and sulfur mustard mixture in diesel fuel matrix*

| № | 1. | 2. | 3. | 4. | 5. | 6. |
|---|---|---|---|---|---|---|
| Component name | nonane | decane | Lewisite ($L_1$) | undecane | Sulfur mustard (H) | dodecane |
| Retent.: (min) | 0.683 | 1.001 | 1.097 | 1.516 | 1.897 | 2.344 |
| Height: (I) | 28.65878 | 31.41221 | 39.24110 | 22.66326 | 217.4166 | 16.49500 |
| Rel.Hgt.: (%) | 8.05 | 8.83 | 11.03 | 6.37 | 61.09 | 4.63 |
| Integral: (min×I) | 65.38900 | 108.3167 | 185.2154 | 105.4823 | 1413.764 | 130.8322 |
| Rel.Int.: (%) | 3.25 | 5.39 | 9.22 | 5.25 | 70.37 | 6.51 |
| Int/Hgt.: (min) | 2.282 | 3.448 | 4.720 | 4.654 | 6.503 | 7.932 |
| Plate number: | 1125 | 1256 | 725 | 1309 | 442 | 1088 |

*Table 7: Peak detection parameters of Lewisite and sulfur mustard in diesel fuel matrix*
*Source: Compiled by the author.*

In the final phase of the analysis of the samples, I examined the mixture of diesel Lewis and sulfur mustard. For the stock solution to be used as a sample, I dissolved 0.3 ml of gas oil, 0.15 ml of sulfur mustard, and 0.06 ml of Lewisite in 5 ml of solvent.

Figure 7 shows the chromatogram of the mixture of the examined blister-inducing toxic warfare agents in a diesel oil matrix. Evaluating the chromatogram, it can be established that, in line with military combat practice, the chromatogram is dominated by sulfur mustard, which is also quantitatively dominant in viscous mustard. In this case, too, Lewisite was eluted in the ranges between $C_{10}$ and $C_{11}$, while sulfur mustard was eluted in the ranges between $C_{11}$ and $C_{12}$ alkanes. According to the retention times that allow the identification of the individual components, I found that the detection peaks characteristic of the two investigated blister-inducing toxic munitions can be seen at the same time. Even then, Lewisite is still partially eluted with the $C_{10}$ component.

## VALIDATION OF SIMULTANEOUS DETECTION

Simultaneous detection with $C_9$-$C_{12}$ alkanes found in diesel oil made it possible to use the retention times of Lewisite I and sulfur mustard to create comparability of the results obtained by determinations with various measurement parameters. For this purpose, based

on the retention times obtained with the same settings for $C_9$-$C_{12}$ linear unsaturated alkanes, I determined the Kováts retention time of Lewisite and sulfur mustard:

Kovats retention index of Lewisite ($\mathbf{I}_{L_1}$):

$$I_{L_1} = 100 \cdot n_{C_{10}} + 100 \cdot \frac{lg \frac{Rf_{L_1}}{Rf_{C_{10}}}}{lg \frac{Rf_{C_{11}}}{Rf_{C_{10}}}}$$

Where:

- $n_{C_{10}} = 10$
- $Rf_{L_1} = 1.097$ min
- $Rf_{C_{10}} = 1.005$ min
- $Rf_{C_{11}} = 1.522$ min

$\mathbf{I}_{L_1} = 100 \times 10 + 100 \times [\lg (1.097/1.005) / \lg (1.522/1.005)] =$ **1021.10**

Kovats retention index of sulfur mustard ($\mathbf{I}_{SM}$):

Where:

$$I_{SM} = 100 \cdot n_{C_{11}} + 100 \cdot \frac{lg \frac{Rf_{SM}}{Rf_{C_{11}}}}{lg \frac{Rf_{C_{12}}}{Rf_{C_{11}}}}$$

- $n_{C_{11}} = 11$
- $Rf_{SM} = 1.897$ min
- $Rf_{C_{11}} = 1.522$ min
- $Rf_{C_{12}} = 2.361$ min

$\mathbf{I}_{SM} = 100 \times 11 + 100 \times [\lg (1.897/1.522) / \lg (2.361/1.522)] =$ **1150.16**

## CONCLUSION

In modern chemical detection, a series of tools and chemical sets help us to perform the analysis of toxic munitions samples taken from the impact surface. However, the effectiveness of their tests to be carried out under field conditions is fundamentally influenced by the preliminary laboratory tests on which they are based.

However, during possible chemical disasters, the most important thing is quick identification in the field, because the time advantage they provide can save many lives through a successful analysis. In recent decades, almost all military chemical defenses. and at the civil emergency reconnaissance organization, model laboratory units equipped with modern equipment, including gas chromatographs, which are suitable for the detection of toxic warfare agents used in all chemical attacks, have been regularized. The data obtained because of such tests allow us to more accurately evaluate the degree of danger caused by various toxic warfare agents by researching in detail the disturbing effects of hydrocarbons present in samples contaminated with diesel oil. It should be noted that these tests are very

necessary, as the hydrocarbons present in individual samples can easily mask the signals from toxic warfare agents during tests performed with inappropriate parameter settings.

A basic requirement for these modern methods is that the results of the measurements can be reproduced in any laboratory. The deviations caused by the characteristics of individual gas chromatography devices can be eliminated by generating the Kováts reference data generated by me. The results presented here can therefore provide a suitable methodological basis for the separate rapid detection of Liewisit-1 and sulfur mustard diesel oil polluting hydrocarbon derivatives.

## REFERENCES

[1] Rudolf Nagy: Thesis, Gas chromatographic (GC) analysis of Lewisite toxic warfare agent as a function of column temperature, nitrogen carrier gas pressure and injection temperature, Hungarian Defence Forces, Bolyai János Military Technical College 1992.;

[2] Wilcox, Fred A.: Scorched earth: legacies of chemical warfare in Vietnam, Seven Stories Press 1st ed., New York, 2011, eISBN: 978-1-60980-340-7, p.10.;

[3] Hoenig Steven L.: Compendium of Chemical Warfare Agents, ISBN-13: 9780387346267, 2007, Springer Science Business Media, LLC, p. 1-43.;

[4] Pankhurst R: Italian fascist war crimes in Ethiopia: A history of their discussion, from the League of Nations to the United Nations (1936-1949); Northeast African Studies 6:83; 1999.;

[5] Elisabeth Bolorinos Allard: Spanish National Identity, Colonial Power, and the Portrayal of Muslims and Jews during the Rif War (1909–27), Tamesis, Woodbridge 2021, ISBN 978 1 85566 345 9, p. 85.;

[6] Mosher D. E., Lachman B. E., Greenberg M. D., Nichols T., Rosen B., Willis H. H.: Green Warriors - Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict, RAND Corporation, Santa Monica 2008, ISBN 978-0-8330-4318-4, p. 18.;

[7] Chemical Munitions Dumped in the Baltic Sea, Report of the ad hoc Expert Group to Update and Review the Existing Information on Dumped Chemical Munitions in the Baltic Sea (HELCOM MUNI), HELCOM – Baltic Marine Environment Protection Commission, Helsinki 2013, ISSN 0357-2994, p. 45.;

[8] Friedrich B., Hoffmann D., Renn J., Schmaltz F., Wolf M.: One Hundred Years of Chemical Warfare: Research, Deployment, Consequences, ISBN 978-3-319-51663-9, Springer International Publishing AG, 2017, https://link.springer.com/content/pdf/10.1007/978-3-319-51664-6.pdf, p. 293.;

[9] Kimm, G. L.; Hook, G. L.; Smith, P. A. Application of Headspace Solid-Phase Microextraction and Gas Chromatography-Mass Spectrometry for Detection of the Chemical Warfare Agent Bis(2-chloroethyl) sulfide in Soil. Journal of Chromatography A 2002, https://doi.org/10.1016/S0021-9673(02)00999-8, 971, 185–191.;

[10] Александров В. Н. – Емельянов В. И.: Отравляющие вещества, Военное издательство, Москва, 1990., 40. o.;

[11] U.S. Army Technical Center for Explosives Safety: EXPLOSIVES SAFETY MANAGEMENT PROGRAM, DEVELOPMENT GUIDE, U.S. Army Defense Ammunition Center, McAlester, OK 74501-9053, 2013., p. 20.;

[12] Brophy Leo P., Wyndham D. Miles and Rexmond C. Cochrane: United States Army In Ivorld War II The Technical Services The Chemical Warfare Service: From Laboratory to Field, Center of Military History United States Army WASHINGTON, D.C., 1988 p. https://history.army.mil/html/books/010/10-2/CMH_Pub_10-2.pdf, p. 387.;
[13] Shachneva MD , Leninskii MA, Savelieva. The Limitations and Capabilities of Wipe Samples Analysis in Control of Contamination of Facilities with Highly Toxic Organic Compounds, ISSN Online 2713-2765, Extreme Medicine Scientific and Practical Reviewed Journal of Federal Medical Biological Agency of Russia, 2021, DOI: 10.47183/mes.2021.018;
[14] Charles E. Kolb et al: Evaluation of Chemical Events at Army Chemical Agent Disposal Facilities Committee On Evaluation of Chemical Events at Army Chemical Agent Disposal Facilities, Board on Army Science and Technology Division on Engineering and Physical Sciences, National Research Council of the National Academies, The National Academies Press Washington, D.C. 2002, ISBN 0-309-08629-9, p. 19.;
[15] Lindblad A., Westerdahl K. S., Norlander L., Normark M., Rydqvist J., Unge W., Waldenström L., Noriander L.: Russian Biological and Chemical Weapons Capabilities: Future Scenarios and Alternatives of Actions, Swedish Defence Research Agency NBC Defence, Report ISRN FOI-R-1561—SE, Umea 2005, ISSN 1650-1942, p. 59.;
[16] Koren Herman, Michael Bisesi: Handbook of Environmental Health, Fourth Edition, Volume II, Biological, Chemical, and Physical Agents of Environmentally Related Disease, Pollutant Interactions in Air, Water, and Soil, Taylor & Francis Inc 2017, ISBN: 9780815371304, p. 656.;
[17] Javed Ali: Chemical Weapons and the Iran-Iraq War: A Case Study in Noncompliance, Nonproliferation Review Vol. 8 № 1 2001, ISSN 1073-6700, https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf, p. 43-58.;
[18] Haifa Zangana: City of Widows: An Iraqi Woman's Account of War and Resistance, Seven Stories Press, 2011, SBN: 3999906031, p. 53.;
[19] Romano J. A., Jr., Lukey B. J., Salem H.: Chemical Warfare Agents Chemistry, Pharmacology, Toxicology, and Therapeutics, sec. ed. CRC Press, Taylor & Francis Group, 2008, ISBN: 978-1-4200-4661-8, p. 11.·p. 520.;
[20] Haines D. D., Fox S. C.: Acute and Long-Term Impact of Chemical Weapons: Lessons from the Iran-Iraq War, Forensic Science Review 26:97, 2014., https://www.researchgate.net/publication/280583658_Acute_and_Long-Term_Impact_of_Chemical_Weapons_Lessons_from_the_Iran-Iraq_War, p. 109.;
[21] HQ DEPARTMENT OF THE ARMY DEPARTMENT OF THE AIR FORCE UNITED STATES MARINE CORPS: Field Behavior of NBC Agents (Including Smoke and Incendiaries), Washington, DC, 3 November 1986, https://irp.fas.org/doddir/army/fm3-6.pdf, p. 2-2.;
[22] Stanisław Popiel, Monika Sankowska. Determination of chemical warfare agents and related compounds in environmental samples by solid-phase microextraction with gas chromatography. Journal of Chromatography A 2011, 1218 (47) , 8457-8479. https://doi.org/10.1016/j.chroma.2011.09.066;
[23] Murray, G. M. Detection and screening of chemicals related to the chemical weapons convention, Encyclopedia of Analytical Chemistry, https://doi.org/10.1002/9780470027318.a0403.pub2 (2013).;

[24] Muir B, McDonald G, Cooper DB, Moran MC.: Optimisation of solvent desorption conditions for chemical warfare agent and simulant compounds from Porapak Q using experimental design. Part 2: Extraction of sulphur mustard from steel and glass Porapak tubes, Journal of Chromatogrraphy A. 2005 May 27;1076(1-2):1-6. doi: 10.1016/j.chroma.2005.03.107.;
[25] Willison S. Wipe selection for the analysis of surface materials containing chemical warfare agent nitrogen mustard degradation products by ultra-high pressure liquid chromatography–tandem mass spectrometry. Journal of Chromatography A. 2012; 1270: 72–79.;
[26] E.J. Pacsial-Ong, Z.P. Aguilar: Chemical warfare agent detection: a review of current trends and future perspective, Bioscience Research Institute, (2013), ISSN: 1945-0516 pp. 516-543.;
[27] Hooijschuur, E. W. J., Kientz, C. E. and Brinkman, U.A.T. (2002) Analytical separation techniques for the determination of chemical warfare agents, Journal of Chromatogr. A, 982, 177-200. p. 181.;
[28] Muir B., Slater B.n J., Cooper D. B., Timperley C. M.: Analysis of chemical warfare agents I. Use of aliphatic thiols in the trace level determination of Lewisite compounds in complex matrices, Journal of Chromatography A, ISSN 0021-9673, https://www.sciencedirect.com/science/article/pii/S0021967303022532?via%3Dihub, Vol. 1028 (2004) 313–320.;
[29] Oliver Terzic, Irvine Swahn, Gheorghita Cretu, Meehir Palit, Gary Mallard. Gas chromatography–full scan mass spectrometry determination of traces of chemical warfare agents and their impurities in air samples by inlet based thermal desorption of sorbent tubes. Journal of Chromatography A, 2012, 1225, 182-192. https://doi.org/10.1016/j.chroma.2012.01.003;

# FOOD CRISIS DUE TO THE RUSSIA-UKRAINE WAR

# ÉLELMISZERVÁLSÁG AZ OROSZ-UKRÁN HÁBORÚ TÜKRÉBEN

WU Yue[1] – HANKA László[2] –TAKÁCS-GYÖRGY Katalin[3]

**Abstract**

As the food crisis has been exacerbated yearly, particularly after the COVID-19 pandemic, we are facing the most severe food crisis since the 2007/2008 food crisis. What is worse to the global food supply is the war between Russia and Ukraine since Feb. 24 2022, the two combined are the crucial world food suppliers. The risks from war to agriculture and food push our planet into a long-term food insecurity crisis. To clarify and provide a comprehensive review of the heavy influence of the war on the food security crisis, we conducted this literature review based on content analysis. We have found that the Russia-Ukraine war pushes the existing food crisis more severely from the perspective of primary agricultural production, such as cultivation and harvesting, logistics, farmers' financial issues, infrastructure, and price volatility. In order to realize a sustainable future and food security, everyone on the planet is considered an active contributor. In this research, we also appeal to other export countries of food and agricultural products to emphasize their responsibility for world food security.

**Keywords**

food security; Russian-Ukraine war; simulation risks; food crisis

**Absztrakt**

Az élelmiszerválság súlyosbodása, különösen a 2007/2008-as élelmiszerválság óta és a COVID-19 világjárvány után, kritikus helyzetet idéz elő. Mindezt tovább fokozza a globális élelmiszerellátásban jelentős szerepet betöltő Oroszország és Ukrajna között, a 2022. február 24. óta dúló háború. A háborúból a mezőgazdaságra és az élelmezésre gyakorolt kockázatok hosszú távú élelmiszer-ellátási bizonytalansági válságba taszítják a világot. A háború élelmezésbiztonsági válságra gyakorolt súlyos hatásának tisztázására és átfogó áttekintésére tartalomelemzésen alapuló szakirodalmi áttekintést végeztünk. Megállapítottuk, hogy az orosz-ukrán háború az elsődleges mezőgazdasági termelés, például a termesztés és a betakarítás, a logisztika, a gazdálkodók pénzügyi problémái, az infrastruktúra és az árak ingadozása szempontjából súlyosbítja a fennálló élelmiszerválságot. A fenntartható jövő és az élelmezésbiztonság megköveteli minden szereplőtől a proaktív közreműködést. A tanulmány felhívja minden élelmiszer- és mezőgazdasági termékek exportáló országa felelősségének fontosságát.

**Kulcsszavak**

élelmiszer biztonság; Orosz-Ukrán háború; szimulációs kockázatok; élelmiszerválság

[1] wuyue.budapest@gmail.com | ORCID: 0000-0003-0349-5654 | PhD student, Óbuda University, Doctoral School on Safety and Security Sciences| PhD hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

[2] hanka.laszlo@uni-obuda.hu, hanka.laszlo@uni-nke.hu | ORCID: 0000-0002-9129-7481 | associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, Institute of Natural Sciences and Basic Subjects, University of Public Service, Faculty of Military Science and Officer Training, Department of Natural Sciences| egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Természettudományi és Alapozó Tantárgyi Intézet, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Természettudományi Tanszék

[3] takacsnegyorgy.katalin@kgk.uni-obuda.hu | ORCID: 0000-0002-9129-7481 | professor, Óbuda University, Keleti Faculty of Business and Management, Department of Business Development and Infocommunications | egyetemi tanár, Óbudai Egyetem, Keleti Károly Gazdasági Kar, Szervezési és Vezetési Intézet

## INTRODUCTION

As the food crisis has been exacerbated yearly, particularly after the COVID-19 pandemic, we are facing the most severe food crisis since the 2007/2008 food crisis. What is worse, the war (which started on Feb. 24 2022, and is still ongoing) [1] between the world's main food and agriculture export countries pilled top of the food crisis. The war between Russia and Ukraine, the COVID-19 pandemic, and extreme weather push our planet into a long-term food insecurity crisis [2], [3].

It is reported that close to 193 million population is acutely food insecure and in need of urgent aid in 2021 [4]. Food insecurity is estimated to persist at a similar level in 2021 or increase in 2022. However, the unfolding war between Russia and Ukraine exacerbates the food crisis, which is not considered even in the estimation of the mentioned report, Sixth Annual Global Report on Food Crises, 2022 [5]. Besides, even those countries heavily rely on grain imports from Russia and Ukraine, especially the Middle East and North Africa, do not have an obvious shortfall in a short run period, such as in March of 2022, they need to afford the higher price and additional transport costs from other farther suppliers [6].

Therefore, conducting this research to comprehensively review how the war influences or accelerates the global food security crisis is worthwhile. Our responsibility is to alert everyone that we must act immediately to achieve sustainable food and agriculture development. We highlight the simulation risks from the war between Russia and Ukraine [7]. This research was conducted in May 2022 amid the ongoing war between Russia and Ukraine because of the critical importance of these countries' role in the world's food supply system.

Global Network Against Food Crises (GNAFC) [8], an international alliance of the United Nations, the European Union, and governmental and non-governmental agencies (Global Report on Food Crises, 2022) announced a 3×3 approach to tackle the root cause of food crisis, promote the sustainable food systems and agriculture, and support the Sustainable Development Goal to End Hunger (SDG 2) at a regional, national and global level: understanding food crisis, leveraging strategic investments in food security, nutrition, and agriculture, going beyond food [5] (Figure 1). This research analyzed the simulation food security risks of the war between Russia and Ukraine and addressed the food crisis according to the 3×3 approach [9].


*Figure 1 The 3 x 3 approach to addressing food crises*
*Sources: FSIN, GRFC 2022.*

The research result contributed a literature review basis for future research on the influence of war or conflict on countries at war from the perspective of world food security and food safety. In addition, the influence of war or conflicts on other important agricultural countries which are not at war from the view of the world food supply.

## METHODOLOGY

In order to provide a comprehensive review of the food security crisis due to the war between Russia and Ukraine, we used secondary research review [10] and content analysis [11] as our research methodology. The secondary research data are from prestigious journals related to the research topic and some international official organizations' websites (reports and database), such as the UN and FAO.

## RESULTS

Our planet is suffering from a period of hunger on an unprecedented scale and the historical peak of food prices [5]. The war between Russia and Ukraine has brought catastrophic disaster to the world food supply [12]. In this research, the simulation risks of food and agriculture in Russia and Ukraine from the Ruassia-Ukraine war were discussed in detail. The simulation risks are mainly from aspects of the cultivation and harvesting season destroyed in Ukraine, transportation of food and other agricultural products influenced by the black sea, farmers in debt and poverty, civilian infrastructure destroyed, price volatility of food and agricultural input products, worse existing food security issues.

### Cultivation and harvesting season destroyed

According to the FAO report of Ukraine [13, p.], the winter crops (wheat and rapeseeds) sown in October 2021 should be harvested from June onwards. However, the Russian and Ukraine war outbreak uncertainly disrupted the winter crop harvesting resulting in population displacement (less labor force), restricted access for farmers to fields, and a lack of economic resources. As of Apr. 01, more than 11 million population have been displaced [14]. As of Mar. 25 2022, it is estimated that about 20-30% of winter sown crops will be unharvested during the 2022/23 season, and it will also negatively affect the spring planting cycle [15]. The escalation of the war also negatively impacted Ukraine and its neighboring country's farmer's capability to control animal diseases, notably African swine fever (ASF) [16]. The planned sunflower seed and spring cereal crops planting period started in April, facing fuel shortage challenges. As of Apr. 18, 17.6 percent of the planned sown area (2.5 million hectares) was completed, which is about 80% of the planned spring crops in 2021[17]. Even the seeds and fertilizer can be 70-80% enough for the needs, but the delivery to farmers cannot be sure due to the logistic interruption from the war. Compared to 2021, sunflower seed and maize planting could decline by 30% in 2022, and sunflower seed and maize yields may decrease by 20% below the average level [16].

In the case of Russia, the international sanctions imposed on it will also influence food export. Once Russia loses the food export market, the farmers' income will be decreased, impacting the coming decision-making on planting. The international sanctions on Russia could also influence necessary food imports, such as seeds and pesticides. The constraint of food input access exposed Russia to high risks of fewer plantings, lower yields, and

lower quality, which will also profoundly affect the global food market as Russia is one of the biggest global food suppliers [16].

**Transportation of food and other agricultural products are influenced (black sea)**

In the case of Ukraine, the war could also damage the inland transport infrastructureand seaports. On the other hand, the processing and storage infrastructure is also under insecurity risks. Black Sea is responsible for 75% of the world's sunflower oil exports, 30% of the world's wheat exports, and 20% of the world's maize exports [14]. Due to the conflict, the insurance premia for vessels destined to berth in the Black Sea region could raise the already high cost of maritime transportation [16]. Even though some vessels have been hit by shelling since the war. Usually, the maritime capacity of commercial shipments accounts for 90% of the total commodity export in Ukraine, but as of March 2022, Ukraine suspended the Russian Black Sea ports. "Black Sea ports are necessary for food export for Ukraine." said an officer in Ukrainian Agricultural Department [18]. Ukraine tried to figure out other exporting solutions via railway through neighboring countries. However, the capacity of any railway shipments is a constraint [14] of the rail carriages and the conflicting railcars' chassis between Ukraine and other neighboring countries, such as Poland. The longer halt of food exporting requires a higher condition of storage, such as a silo. Oilseeds can be more fragile and have a shorter storage duration than grains. Besides, the labor force is lacking in the supply chain as some international corporates in grain and oilseed export sectors recalled their employees for their safety guard in Ukraine [16].

**Farmers will be into debt and poverty**

Due to the shock of the Russia and Ukraine war, global economic growth will slow significantly in 2022. Ukraine is expected to drop a severe double-digit GDP in 2022, and the economy will contract by 35% in 2022 because of the invasion. Moreover, the population displacement, death, and destruction of physical capital hit severely in economic recovery. For Russia, the huge shrink is also estimated from the international sanctions and European countries' restrictions on energy imports, such as the loss of correspondent banking privileges, access of some banks to the SWIFT payments system, the interdiction of central bank assets, an embargo on oil and gas [19]. The depreciation of the Russian rouble makes agricultural products cheaper, but the cost of agricultural machinery and other production facilities is elevated. Similar challenges also happened to the weakened Ukrainian hryvnia since the war, which can also reduce remittance flows, the main factor of GDP. The depreciation of the Russian rouble and Ukrainian hryvnia also influences other countries that have a tight relationship with them. The contraction and damage in the Russian and Ukrainian economies have negatively impacted their food and agriculture since the purchasing power of households shrunk. At the same time, the agrifood products price increased. Even if there are available agricultural input products, some farmers might not be able to afford the increased price [10]. However, before the war, the COVID-19 pandemic had already resulted in a debt burden to the low and middle-income countries [11.

**Civilian infrastructure destroyed: agricultural land, farming equipment, and supply chains**

The agricultural livelihoods in the conflict-affected area and across the country are disrupted directly by the constrain of civilian displacement and commercial activities and

the damage to farming equipment and infrastructures, such as critical fuel, gas, electricity, buildings, homes, water management infrastructure, health facilities, and schools. As of Apr. 01, it was estimated that around 100 billion USD of infrastructure had been destroyed in Ukraine due to the war with Russia. It has been reported that several cargo vessels and tankers got attacked, and the grain storage and exportation infrastructure were damaged in Ukraine. Many ships carrying food or agricultural products are blocked in the black sea region or remain in Ukraine. And some agricultural companies paused operations, consequently influencing the agricultural commodities export, and the oilseed crushing operations were also suspended in Ukraine. The Ukraine government estimated that the Ukrainian economy contracted only by about 35-60 percent in March. And there were likely 50 businesses relocated from the east, where are most conflict-affected areas, to the west till Mar. 19, including domestic and foreign businesses [14].

**Price volatility of food and agricultural input products**

It is vital to monitor food price volatility than at any time before since the food price crisis in 2007-2008 and 2010-2011 [20], as the unfolding war between Russia and Ukraine brought more uncertainty to the food market and food security to millions. Before the war between Russia and Ukraine, food prices were already high [20]. The COVID-19 has shocked all industries since 2020, the labor markets are still struggling to recover from the pandemic consequences, such as shrunk income, and 60% of low-income countries are in debt or at high risk [6]. FAO estimates that the cereal production in 2022 can not be sufficient to meet the requirements in the 2022/2023 season, and the demand for cereal production will increase, keeping the rising pace of the increasing population. At the same time, tighter supplies and uncertain markets, such as the rising price of energy and input, will make cereal prices high in the coming season in 2022/23 [21]. The war between Russia and Ukraine just pushed up this food price inflation by disrupting the global grain supplies, natural gas, and fertilizer market, and the producers for harvesting and planting in a new season [2]. On the other hand, the raised cost of agricultural input products will further pressure farmers to start a new planting season [14]. Since the outbreak of the war, many countries suspended part of the agricultural commodities export, such as food and fertilizer, for safe domestic food supply, including Russia and Ukraine, which also drove the food price volatile. The increasing price of fertilizer can be an important threat to food production, raising the food price [20].

**The existing food security issues will be worse after the war**

The area around the Black Sea, including Russia and Ukraine, is known as "World's bread basket" which has fertile soil and high rates of grain production [22]. The region of the black sea has been a significant global supplier of grains and oilseeds for the last 30 years [2]. Due to the catastrophic disaster of COVID-19 and the war between Russia and Ukraine, it is estimated that wheat inventories are at 33% of annual consumption, a level not seen since 2007 and 2008 [23]. Sara Menker, the CEO of agriculture analytics firm Gro Intelligence and food insecurity expert, said, "The Russia-Ukraine war was not the cause of a food security crisis but simply added fuel to the fire that was long burning." And "We currently only have ten weeks of global consumption sitting in inventory around the world. Conditions today are worse than those experienced in 2007 and 2008." at Conflict and food security - Security Council, 9036th Meeting on May 19 2022 [24]. In Ukraine, the export

volumes shrank significantly due to the halted Black Sea and Sea of Azov ship traffic. As of the end of February, 10% of planned wheat exports and 31% of planned maize exports for the 2021/22 marketing year will remain in Ukraine [14].

During the ongoing war, Russia [19] and Ukraine [20] have launched some bans and suspended exports regulation on food products and fertilizers to safeguard the domestic food supply and the raw material needed for domestic processing and livestock industries. Russia introduced a temporary ban on the exports of wheat, meslin, rye, barley, and maize to the countries within the Eurasian Economic Union (EAEU) [25], except Belarus from Mar. 14 2022 until Jun. 30 2022, and white and raw cane sugar from Mar. 15 2022 until end of August 2022 [26]. Russia introduced the temporary export ban again for sunflower seeds and rapeseeds from Apr. 01 to Aug. 31 2022 on Mar. 31 2022 and jointly introduced a 1.5 million tonnes quota on sunflower oil exports and a 700 000 tonnes limit on sunflower meal exports till the end of August 2022 [27]. Ukraine released the export licensing requirements for wheat and meslin, maize, poultry, eggs, and sunflower oil on Mar. 05 2022 [28], which means that the exports of these products are only allowed with the permission of the country's Ministry of Economy. On Mar. 09 2022, the Ukraine government added barley and rapeseed to the list of products for which exports have been suspended since Mar. 05 2022, such as oats, buckwheat, millet, rye, meat, sugar, and salt [29].

Till May 29 2022, 27 countries released export restriction regulations on food and fertilizers [30]. Comparing the impact of the Ukraine war, the COVID-19 pandemic, and the food price crisis in 2007 and 2008 ( Table 1, Table 2, Table 3), the share in the world market of calories during the Ukraine war was 17.22%, after the food crisis in 2007&2008 18.69%, and it is 9.97% during COVID-19. However, the influence of calories and the shares are the worst during the Ukraine war, 703, 846 Bn Kcal and 60, 894 million USD (5.79%), respectively.

| Category | Number of Countries | Share in World Market of Calories | Count of Products | Bn Kcal | Mio USD | ShareDollars_Total |
|---|---|---|---|---|---|---|
| Grand Total | 27 | 17.22% | 59 | 703,846 | 60,894 | 5.79% |
| Announcement | | | | | | |
| Actual Ban | 24 | 13.42% | 45 | 548,339 | 43,244 | 4.11% |
| Export Licensing | 8 | 3.33% | 10 | 136,047 | 15,680 | 1.49% |
| Not Binding Export Taxes | 3 | 0.48% | 4 | 19,460 | 1,970 | 0.19% |

*Table 1. The global export restrictions during the Ukraine crisis, 2022*
*Source: Food & Fertilizer Export Restrictions Tracker*

| Category | Number of Countries | Share in World Market of Calories | Count of Products | Bn Kcal | Mio USD | ShareDollars_Total |
|---|---|---|---|---|---|---|
| Grand Total | 25 | 9.79% | 44 | 400,199 | 32,028 | 3.05% |
| Announcement | 2 | 0.12% | 2 | 5,027 | 290 | 0.03% |
| Actual Ban | 22 | 8.01% | 34 | 327,403 | 27,370 | 2.60% |
| Export Licensing | 6 | 0.14% | 7 | 5,569 | 538 | 0.05% |
| Not Binding | 1 | 1.52% | 1 | 62,200 | 3,831 | 0.36% |
| Export Taxes | | | | | | |

*Table 2. The global export restrictions during COVID-19, 2020*
*Source: Food & Fertilizer Export Restrictions Tracker*

| Category | Number of Countries | Share in World Market of Calories | Count of Products | Bn Kcal | Mio USD | ShareDollars_Total |
|---|---|---|---|---|---|---|
| Grand Total | 33 | 18.69% | 59 | 510,135 | 42,503 | 9.32% |
| Announcement | | | | | | |
| Actual Ban | 27 | 12.32% | 42 | 336,356 | 27,030 | 5.93% |
| Export Licensing | 3 | 0.13% | 3 | 3,450 | 1,147 | 0.25% |
| Not Binding | | | | | | |
| Export Taxes | 9 | 6.24% | 14 | 170,329 | 14,327 | 3.14% |

*Table 3. The global export restrictions during Food price crisis, 2008*
*Source: Food & Fertilizer Export Restrictions Tracker*

Suppose the fertilizer availability and affordability crisis cannot be addressed. Russia and China were among the top ten global exporters of nitrogenous fertilizer, phosphate fertilizer, and potash fertilizer in 2021 [11]. Due to the Ukraine war, Russia and China announced export bans or export licensing for fertilizer for the different duration ( Figure 2), updated on May 29 2022 [22], which together account for more than 20% of global export nitrogenous fertilizer, 3% potash fertilizer and near 20% phosphates fertilizer impacted. In that case, further harvesting will suffer, food prices will keep rising, and the food insecurity problem will be more severe [31].

| Policy Status | Category | Country Label | Products | Ⓐ(Starting Date) | Ⓐ(End Date) | Share of global exports of Nitrogenous impacted | Share of global exports of Potash impacted | Share of global exports of Phosphates impacted |
|---|---|---|---|---|---|---|---|---|
| Inactive | Actual Ban | Korea, South | Fertilizer: Urea | 11/11/2021 | 03/31/22 | 0.3% | 0.0% | 0.0% |
| Active | Actual Ban | China | Phosphate rock | 09/28/2021 | 12/31/22 | 0.0% | 0.0% | 0.6% |
| | | Kyrgyzstan | Mineral fertilizers | 02/26/2022 | 08/26/22 | 0.0% | 0.0% | 0.0% |
| | | Russia | Fertilizer | 02/04/2022 | 08/31/22 | 10.1% | 18.7% | 8.6% |
| | | Ukraine | Nitrogenous fertilizers (inc. compound).. | 03/12/2022 | 12/31/22 | 0.9% | 0.2% | 0.0% |
| | Export Licensing | China | Fertlizers | 09/24/2021 | 12/31/22 | 10.6% | 1.2% | 11.4% |
| | | Russia | Nitrogenous fertilizers (inc. compound) | 11/03/2021 | 05/31/22 | 10.1% | 2.8% | 8.5% |

*Figure 2. List of export restrictions on fertilizers during the Ukraine crisis episode (2022)*
*Source: Food & Fertilizer Export Restrictions Tracker*

From previous experience, including the food crisis in 2007 and 2008, usually, the export restrictions have cascading effect from the first country to announce the export restrictions, and later the others will follow suit. It further exacerbates supply issues and creates a panicked atmosphere in the global market [32]. In order to curb price increases amid the growing global food price [3], close to 20 countries May 26 2022 have taken measures to ensure the sufficient availability of foodstuffs in the domestic market via shortening exports temporarily, such as Kazakhstan, India, Belarus [33], Burkina Faso [34], Serbia [35] etc. For example, Kazakhstan [36] introduced a temporary quota on wheat (1 million tonnes) and wheat flour (300 000 tonnes) export during Apr. 15 to Jun. 15 2022. And it is obliged for exporters to sell 10% of declared export volumes to the state purchasing company in order to meet the demands of local bakeries, flour mills, livestock, and poultry farming. India prohibited exports of wheat on May 13 2022 [37]. As the world's biggest producer of sugar and the second largest exporter behind Brazil [3], [38], India declared the limitation on sugar exports to 10 million tonnes from Jun. 01 2022 up to Oct. 31, 2022, while its sugar export from October 2021 to May 2022 was 78 million tonnes.

## DISCUSSION

The war between Russia and Ukraine is still unfolding [1], which means the risks to agriculture and food in Russia, and Ukraine is continuing and unknown. As a result, the world food supply has been under insecurity for an uncertain time due to the Russia-Ukraine war. For example, primary agricultural production is influenced negatively from the perspective of cultivation and harvesting [13], [14], [16], [17], the logistics [14], [16], [18], farmers' financial issues [14], [16], [19], infrastructure [14] and price volatility [2], [14], [20]. Besides, the existing food security crisis will be worse due to the war [14], [24], [32]. The main food crisis risk factors from the Russia-Ukraine war are the infrastructure of agriculture, such as the cultivation and harvesting season interruption, supply chain changes, and producer challenges. Regards value chain, the production, processing and logistics are the crucial stages cause food crsis.

## CONCLUSION

As a result, this research result provided a food security crisis due to the Russia-Ukraine war to Russian and Ukrainian policymakers. At the same time, we appeal to other food and agricultural products export countries to emphasize their responsibility for the world food supply. In order to realize a sustainable future and food security, everyone on the planet is considered an active contributor.

## REFERENCES

[1] H. Livingstone, P. Beaumont, M. Belam, and M. B. with agencies, 'Russia-Ukraine war at a glance: what we know on day 432 of the invasion', *The Guardian*, May 01, 2023. Accessed: May 01, 2023. [Online]. Available: https://www.theguardian.com/world/2023/may/01/russia-ukraine-war-at-a-glance-what-we-know-on-day-432-of-the-invasion

[2] 'How will Russia's invasion of Ukraine affect global food security? | IFPRI : International Food Policy Research Institute', Feb. 24, 2022. https://www.ifpri.org/blog/how-will-russias-invasion-ukraine-affect-global-food-security (accessed May 27, 2022).
[3] 'India moves to restrict again! 20 countries around the world implement grain export bans, and there are only 10 weeks of wheat stocks left! The main line of domestic stable growth investment is sorted out. (印度再出手限制！全球20国实施粮食出口禁令，小麦库存只剩10周！国内稳增长投资主线梳理)', May 26, 2022. https://baijiahao.baidu.com/s?id=1733895948227595952&wfr=spider&for=pc (accessed May 27, 2022).
[4] FAO, '2022 Global Report on Food Crises |KORE - Knowledge Sharing Platform on Resilience| Food and Agriculture Organization of the United Nations', 2022. https://www.fao.org/in-action/kore/publications/publications-details/en/c/1514109/ (accessed Sep. 04, 2023).
[5] 'This sixth annual Global Report on Food Crises', Global Network Against Food Crises (GNAFC), 2022. Accessed: May 25, 2022. [Online]. Available: http://www.fightfoodcrises.net/fileadmin/user_upload/fightfoodcrises/doc/resources/GRFC_2022_FINAl_REPORT.pdf
[6] Arif Husain, Friederike Greb, and Stefan Meyer, 'Projected increase in acute food insecurity due to war in Ukraine', Mar. 2022. Accessed: May 26, 2022. [Online]. Available: https://docs.wfp.org/api/documents/WFP-0000138155/download/
[7] M. F. Rabbi, T. Ben Hassen, H. El Bilali, D. Raheem, and A. Raposo, 'Food Security Challenges in Europe in the Context of the Prolonged Russian–Ukrainian Conflict', *Sustainability*, vol. 15, no. 6, p. 4745, Mar. 2023, doi: 10.3390/su15064745.
[8] FAO, 'Global Report on Food Crises: Number of people facing acute food insecurity rose to 258 million in 58 countries in 2022', *Newsroom*, 2023. https://www.fao.org/newsroom/detail/global-report-on-food-crises-GRFC-2023-GNAFC-fao-wfp-unicef-ifpri/en (accessed Sep. 04, 2023).
[9] M. A. Nasir, A. D. Nugroho, and Z. Lakner, 'Impact of the Russian–Ukrainian Conflict on Global Food Crops', *Foods*, vol. 11, no. 19, p. 2979, Sep. 2022, doi: 10.3390/foods11192979.
[10] D. W. Stewart, M. A. K. Ph.D, and M. A. Kamins, *Secondary Research: Information Sources and Methods*. SAGE, 1993.
[11] S. Stemler, 'An overview of content analysis', doi: 10.7275/Z6FM-2E34.
[12] 'Ukraine war: World Bank warns of "human catastrophe" food crisis', *BBC News*, Apr. 21, 2022. Accessed: Apr. 22, 2022. [Online]. Available: https://www.bbc.com/news/business-61171529
[13] 'FAO GIEWS Country Brief on Ukraine -', Apr. 22, 2022. https://www.fao.org/giews/countrybrief/country.jsp?code=UKR (accessed Jun. 08, 2022).
[14] 'UKRAINE Targeted Analysis', FEWS NET, Apr. 2022. [Online]. Available: https://fews.net/sites/default/files/documents/reports/FEWS%20NET_Ukraine_Targeted_Analysis_Final.pdf
[15] FAO, 'Information Note - The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the war in Ukraine', 2022.

[16] 'The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the current conflict', FAO, Mar. 2022. [Online]. Available: https://www.fao.org/3/cb9236en/cb9236en.pdf
[17] 'Ukraine's spring crop planting covers 2.5 million hectares to date', Apr. 22, 2022. https://www.agricensus.com/Article/Ukraine-s-spring-crop-planting-covers-2-5-million-hectares-to-date-21754.html (accessed Jun. 08, 2022).
[18] 'Ukraine looks to reopen Black Sea ports to boost food exports （乌克兰期盼重开黑海港口以拉动粮食出口）', May 27, 2022. https://m.gmw.cn/baijia/2022-05/27/1302968020.html (accessed Jun. 08, 2022).
[19] INTERNATIONAL MONETARY FUND, *WORLD ECONOMIC OUTLOOK, APRIL 2022*. S.l.: INTL MONETARY FUND, 2022.
[20] 'The Russia-Ukraine war is exacerbating international food price volatility | IFPRI : International Food Policy Research Institute', Mar. 30, 2022. https://www.ifpri.org/blog/russia-ukraine-war-exacerbating-international-food-price-volatility (accessed Jun. 16, 2022).
[21] 'FAO Cereal Supply and Demand Brief | World Food Situation | Food and Agriculture Organization of the United Nations', Jun. 03, 2022. https://www.fao.org/worldfoodsituation/csdb/en/ (accessed Jun. 13, 2022).
[22] K. Vlamis, 'How Russia's assault on Ukraine, the "world's breadbasket," could lead to famine in Yemen', *Business Insider*, May 17, 2022. https://www.businessinsider.com/russia-assault-ukraine-could-lead-to-famine-in-yemen-2022-3 (accessed May 27, 2022).
[23] United Nations, 'Lack of Grain Exports Driving Global Hunger to Famine Levels, as War in Ukraine Continues, Speakers Warn Security Council | UN Press', 2022. https://press.un.org/en/2022/sc14894.doc.htm (accessed Sep. 04, 2023).
[24] 'Conflict and food security - Security Council, 9036th Meeting | UN Web TV', May 19, 2022. https://media.un.org/en/asset/k10/k10mjpv1u3 (accessed May 27, 2022).
[25] Global Trade Alert, 'Intervention 101844: Russian Federation: Temporary export ban on certain types of grains', 2022. https://www.globaltradealert.org/intervention/101844/export-ban/russian-federation-temporary-export-ban-on-certain-types-of-grains (accessed Sep. 04, 2023).
[26] 'Russian Federation bans exports of wheat, maize and other cereals to Armenia, Kazakhstan and Kyrgyzstan until 30 June 2022 | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Mar. 15, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1477294/ (accessed May 30, 2022).
[27] 'The Russian Federation bans exports of sunflower seeds and rapeseeds, and introduces quotas on sunflower oil and meal exports | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Apr. 15, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1506344/ (accessed May 27, 2022).
[28] Global Trade Alert, 'Ukraine: Export bans for grains and meat and export licensing requirements for sunflower oil, poultry and eggs introduced', 2022. https://www.glo-

baltradealert.org/state-act/62432/ukraine-export-bans-for-grains-and-meat-and-export-licensing-requirements-for-sunflower-oil-poultry-and-eggs-introduced (accessed Sep. 04, 2023).
[29] 'Ukraine suspends exports of some food products | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Mar. 09, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1476888/ (accessed May 27, 2022).
[30] D. Laborde Debucquet and A. Mamun, 'Documentation for Food and Fertilizers Export Restriction Tracker: Tracking export policy responses affecting global food markets during crisis', International Food Policy Research Institute, Washington, DC, 2022. doi: 10.2499/p15738coll2.135857.
[31] 'High fertilizer prices contribute to rising global food security concerns | IFPRI : International Food Policy Research Institute', Apr. 25, 2022. https://www.ifpri.org/blog/high-fertilizer-prices-contribute-rising-global-food-security-concerns (accessed Jul. 02, 2022).
[32] 'From bad to worse: How Russia-Ukraine war-related export restrictions exacerbate global food insecurity | IFPRI : International Food Policy Research Institute', Apr. 13, 2022. https://www.ifpri.org/blog/bad-worse-how-export-restrictions-exacerbate-global-food-security (accessed Jul. 02, 2022).
[33] 'Belarus extends grain export ban and introduces temporary ban on exports of rice, rye and barley flour and groats, processed cereals and pasta | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Apr. 21, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1513276/ (accessed May 27, 2022).
[34] 'Burkina Faso bans exports of millet, maize and sorghum flours, complementing a ban on exports of cereal grains | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Mar. 29, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1492066/ (accessed May 27, 2022).
[35] 'Serbia introduces temporary ban on wheat grain, wheat flour, maize and sunflower oil exports | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Mar. 10, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1476887/ (accessed May 27, 2022).
[36] 'Kazakhstan to introduce temporary quotas on wheat and wheat flour exports | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', Apr. 15, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1505413/ (accessed May 27, 2022).
[37] 'India prohibits wheat exports | Food Price Monitoring and Analysis (FPMA) | Food and Agriculture Organization of the United Nations', May 23, 2022. https://www.fao.org/giews/food-prices/food-policies/detail/en/c/1513589/ (accessed May 27, 2022).
[38] D. M. Business CNN, 'India, the world's largest producer of sugar, is restricting exports', *CNN*, May 25, 2022. https://www.cnn.com/2022/05/25/business/india-sugar-export-restrictions-food-prices/index.html (accessed May 27, 2022).

# EFFECT OF SEWAGE FARMS ON WATER QUALITY OF RÁBA UNDER SÁRVÁR – LONGITUDINAL CHANGES OF WATER QUALITY PARAMETERS

# SZENNYVÍZTISZTÍTÓK HATÁSA A VÍZMINŐSÉGRE A RÁBA SÁRVÁR ALATTI SZAKASZÁN – VÍZMINŐSÉGI PARAMÉTEREK HOSSZ-SZELVÉNYI VÁLTOZÁSAI

KERÉK Gábor[1]

**Abstract**

In 2001 unknown origin foam was observed on the upper reaches of the Rába, at Szentgotthárd, on the downstream of the dam. The phenomenon appeared on several occasions and at several locations later, drawing attention to the water quality risks of the Rába and leading to a transboundary conflict situation between Hungary and Austria. In order to solve this, a series of water quality and ecological surveys were conducted in 2008-2009. In this study, I deal with the analysis of the water quality data of the Rába section below Sárvár, looking for trends and correlations between the chemical parameters of the river at the sampling points, including the sewage farms. The data are analyzed longitudinally, taking into account the results of the mentioned survey.

**Keywords**

Raab, Raab survey, water quality, chemical safety, trendanalysis

**Absztrakt**

2001-ben a Rába magyarországi felső szakaszán, Szentgotthárdnál addig ismeretlen eredetű habzást figyeltek meg a duzzasztómű alvízi oldalán. A jelenség több ízben, és több helyszínen jelent meg a későbbiekben, és ráirányította a figyelmet a Rába vízminőségi kockázataira, és határvízi konfliktushelyzethez vezetett Magyarország és Ausztria viszonylatában. Ennek megoldása érdekében vízminőségi és ökológiai vizsgálatsorozat készült 2008-2009-ben. Jelen tanulmányomban a Rába Sárvár alatti szakaszának vízminőségi adatainak elemzésével foglalkozom, trendvizsgálatokkal és regressziós elemzésekkel kapcsolatot keresve a folyó mintavételi pontjain mért kémiai jellemzői között, figyelembe véve a szakasz szennyvíztisztító telepeinek kibocsátásait. Az adatokat hossz-szelvény szerint, az említett felmérés eredményeinek tükrében is elemzem.

**Kulcsszavak**

Rába, Rába survey, vízminőség, kémiai biztonság, trendvizsgálat

[1] kerek.gabor@eduvizig.hu | ORCID: 0000-0002-5804-3594| Deputy Head of Department, North Transdanubian Water Directorate, Győr, Hungary; PhD Student University of Public Service, Doctoral School of Military Engineering | Szakágazati vezető, osztályvezető-helyettes, Észak-dunántúli Vízügyi Igazgatóság, Győr; doktorandusz, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

## VÍZMINŐSÉGI PROBLÉMÁK A RÁBÁN ÉS VÍZGYŰJTŐJÉN

A Rába folyó vízminőségi problémái az ezredfordulót követően kerültek a közérdeklődés fókuszába, amikor is visszatérő jelleggel, eredendően ismeretlen eredetű, esztétikailag rendkívül visszatetsző, fehéres-barnás habzás jelent meg a magyar szakasz duzzasztóműveinek alvízi szakaszain, ahol a műveken átbukó víz energiatartalmánál fogva a detergensekhez hasonló módon felhabosította a víz felszínét, mely a duzzasztóművek (Szentgotthárd, Ikervár, Nick) alsó oldalán, az áramlási holtterekben gyűlt össze. A magyar hatóságok és az akkor még működő vízügyi kutatóintézetek már 2003-ban vizsgálat-sorozatokat végeztek a szennyezés forrásának felderítése céljából. Számos határvízi egyeztetést, konfliktust és vizsgálatot követően világossá vált, hogy a szennyezést a folyó osztrák oldalán, a Feldbach és Jennersdorf településeken működő bőrfeldolgozó üzemekből elfolyó, csak részben tisztított ipari szennyvizek okozzák, mégpedig a bőrcserzés segédanyagaként használt naftalin-szulfonát. A naftalin-szulfonát definíciója szerint: „Az anyag káros a környezetre és szennyeződést okozhat a víztestben és a légkörben, és a savas eső könnyen kialakulhat a légköri kémiában és a légköri fizikai változásokban. Tehát, ha a pH értéke 5-nél alacsonyabb, súlyos károkat okozhat az állatok és a növények számára, a haltenyésztést és -fejlesztést súlyosan érinti, a talajban levő üledékeket és a víz fém mérgezését a víz feloldhatja. A víz savasodása a vízi élőlények összetételében bekövetkező változásokhoz is vezethet. A sav-toleráns algák és gombák megnövekednek és a szerves anyagok bomlási sebessége csökken. A savasodás súlyos veszteséget okozhat a tavakban és folyókban.” [1]

A szennyezőanyag a 2000-es években több éven keresztül okozott vissza-visszatérő habzást a Rábán, ami a két ország között határvízi konfliktust okozott. 2004. májusában az ausztriai Bad Schönauban tartottak osztrák-magyar kormányközi vízminőségi bizottsági ülést. Jegyzőkönyvben rögzítésre került az osztrák fél elismert felelőssége, miszerint Ausztriából származik a Rába habzását okozó szennyezés. Szentgotthárdnál ekkor már két éve kisebb-nagyobb intenzitással, szinte folyamatosan tapasztalható volt a habzás a Rába vizében, amelyet a későbbiekben a folyó más szakaszain is detektáltak. A habzást biológiai eredetűnek vélték a szakemberek, ehhez az elpusztult algák fehérjéi ténylegesen hozzá is járultak a jelenséghez, azonban a naftalin-szulfonátot nevű bőrgyári segédanyagot is kimutatták a Rába vizéből. Az osztrák felet cselekvési terv kidolgozására kötelezte a Bizottság. A naftalin-szulfonát egyébként az emberre nézve nem mérgező, és a halakra is csak nagy koncentrációban jelent veszélyt. Az osztrák fél a terv kidolgozására ígéretet tett. Ezt követően a Bécsi Műszaki Egyetem és az osztrák Szövetségi Mező- és Erdőgazdasági, valamint a Környezet- és Vízgazdálkodási Minisztérium szakértői elvégezték a Boxmark cég jennersdorfi és feldbachi, valamint a Schmidt nevű cég wollsdorfi szennyvízbevezetésének elemzését. A vizsgálatok mindhárom esetben az egyes szennyezőanyagok magasabb koncentrációját igazolták. [2]

A habzást okozó anyag kibocsátása végül a bőrfeldolgozó üzemek tisztítástechnológiai fejlesztéseit követően szűnt meg 2008-ban, és rávilágított a határral osztott vízgyűjtők vízminőség-védelmi kérdéseire, az ipari és kommunális szennyvízbevezetések környezeti kockázataira. Ennek megfelelően létrejött egy közös osztrák-magyar munkacsoport, és egy átfogó kémiai és biológiai vizsgálatsorozat elvégzését irányozták elő 2007-ben. A vizsgálatok a Rába/Raab Survey nevű közös vízminőség-védelmi projekt végrehajtásában öltöttek testet 2008-2009-ben.

## RÁBA SURVEY – VÍZMINŐSÉGI ÉS BIOLÓGIAI ÁLLAPOTÉRTÉKELÉS A TELJES VÍZRENDSZEREN

A Rába vízminőségi kérdéseinek kezelése céljából 2008-2009-ben közös osztrák-magyar cselekvési tervet dolgoztak ki, melynek része volt egy átfogó vízminőségi monitoring a teljes Rába-vízgyűjtőre kiterjesztve. A monitoring egy vízminőségvédelmi projekt keretében történt meg. 2008-ban és 2009-ben vízkémiai és ökológiai felméréseket végeztek a folyón és vízgyűjtőjén. A vízkémiai felmérés során a paramétereket a főbb kibocsátók és mellékfolyók figyelembevételével vizsgálták, és vízminőségi hossz-szelvényeket készítettek a releváns paraméterek vonatkozásában. A teljes vízgyűjtőn összesen 29 mérési szelvény (23 db a Rábán és 6 db a mellékfolyókon), valamint 24 db jelentős szennyvízkibocsátó bevezetett szennyvizét mintázták és dolgozták fel. [3] A vizsgálatok célzottan koncentráltak a bőrfeldolgozó üzemek kibocsátott szennyvizeinek vizsgálatára. A vizsgálatsorozat végeredményeként minősítették a Rába és vízrendszerének vízminőségi állapotát. A folyó magyar szakaszán a projekt zömében kommunális szennyvíztisztítók bevezetett tisztított vizeinek vizsgálatára koncentrált, természetesen a Rába vízminőségi hossz-szelvényének vizsgálata mellett.

A projekt eredményeinek frissítése céljából 2020-ban új projekt indult a Rába vízgyűjtőjén érintett vízminőség-védelmi szervezetek bevonásával, ez a RaabStat néven futó projekt, mely 2022-ben ért véget.

Jelen kutatásomban a 2009-es vizsgálat alapjain néhány alapvető vízkémiai paraméter tér- és időbeni változásának elemzésével megvizsgáltam a Rába alsó szakaszának (Sárvár-Győr) vízminőség-változásait. E paraméterek a következők:

- pH
- elektromos vezetőképesség
- BOI5
- Összes Nitrogén
- Összes Foszfor
- oldott oxigéntartalom

### pH-érték

A pH a felszíni vizek savasságának mérőszáma. Megítélése szempontjából kulcsfontosságú a vízgyűjtőterület talajának bázikus puffertartalma. A mészkőtartalmú vizek pH-értéke a jelenlegi terhelésnél 7 - 8. Alacsony puffer tartalmú területeken (kristallin, kristályos, mészkőhiányos kőzetek) az antropogén savasodás következtében 7 alá süllyedhet. [3]

### Elektromos vezetőképesség [µS/cm]

A vizek ásványianyag-tartalmának jellemző paramétere. Amennyiben a víz nem tartalmaz nagymennyiségű geológiai eredetű sókat, akkor a magasabb ásványisó-tartalom antropogén hatást feltételez (útszórósó, ipari szennyvíz). [3]

### $BOI_5$ - Biológiai oxigénigény nitrifikációs gátlás nélkül [mg $O_2$/l]

A $BOI_5$ a biológiai oxidáció 5 napos oxigénfogyasztásának mértékét jelzi, így a biológiailag lebomló szerves anyagok mennyiségének mérőszáma. Jó indikátora a kommunális szennyvizekkel terhelt felszíni vizeknek, mivel annak könnyű bomlása miatt az ezzel terhelt vizek $BOI_5$- értéke rendszerint magas. [3]

**Oxigén-tartalom [mg/l]**

A felszíni víz oldott oxigén-koncentrációját jelzi. Mértékét mg$O_2$ /l [mg/l] dimenzióban adjuk meg.

**Összes nitrogén [mg/l]**

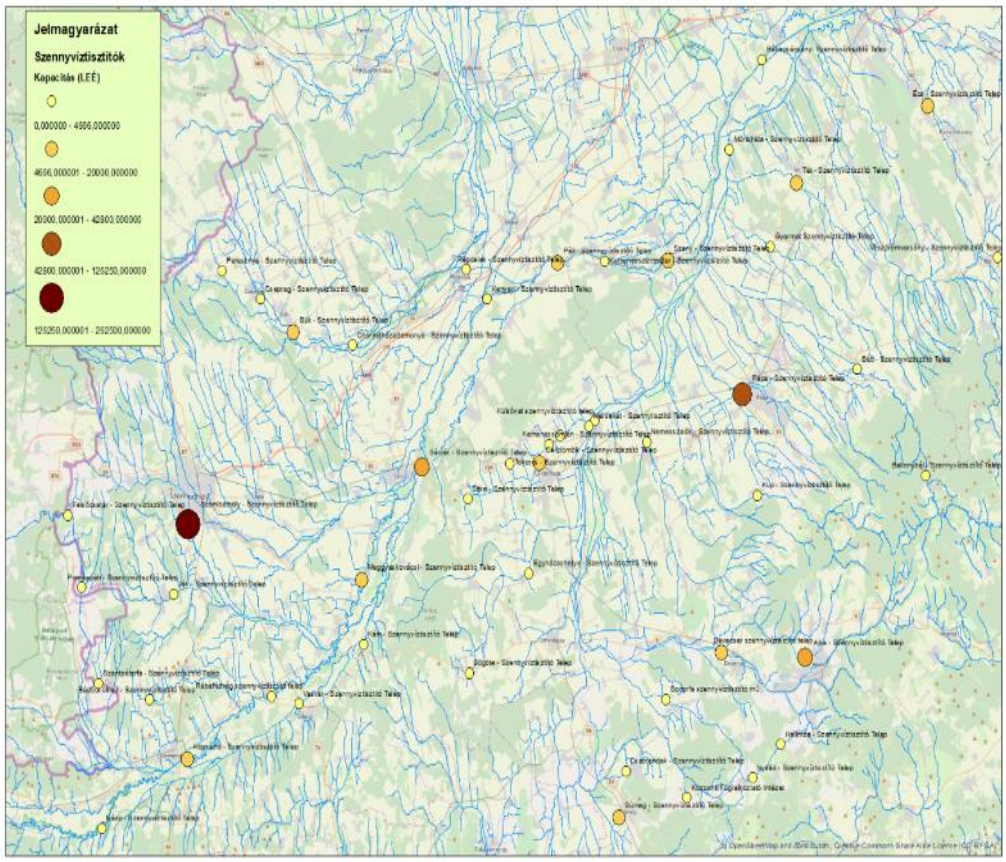
A szerves, kötött állapotú, ill. szervetlen nitrogén mérőszáma, melynek felszíni vizek szempontjából legjelentősebb megjelenési formái a következők: elemi nitrogén ($N_2$), nitrát ($NO^{2-}$), nitrit ($NO^{-}$) és az ammónium ($NH^{4+}$). A folyóvizekben a legfontosabb szervetlen nitrogénforrást a nitrát jelenti, mely zömében mezőgazdasági tevékenység következtében jelenik meg a felszíni vizekben, mivel magas arányban találhatók meg műtrágyákban. Mivel a kijuttatott műtrágya nitrogén-tartalmát a növénykultúra viszonylag alacsony hányadban hasznosítja, a maradék a talajvizekbe és a felszíni vizekbe jut. Ezt a folyamatot a nitrát jó vízoldhatósága is elősegíti. A kommunális szennyvíz mintegy egyharmada is szerves nitrogén- vegyületekből áll, ezen kívül ammónium sók, pl. NTA (nitrilotriacetát) is megjelennek benne. Nem megfelelő műszaki védelemmel ellátott hulladéklerakókból is juthatnak nitrogén-tartalmú csurgalékvizek felszíni vizekbe. [3]

**Összes foszfor (mint P) [µg/l]**

A vízbe jutó foszfor és származékai, mint növényi tápanyagok közvetlenül tehetők felelőssé a felszíni vizekben kialakuló eutrofizáció miatt. Az eutrofizáció, avagy vízvirágzás intenzív vízinövények intenzívebb életciklusát okozza, az ezáltal erősödő bomlás intenzívebb oxigénfogyasztást okoz, aminek következtében oldot-oxigén hiányos állapot lép fel a felszíni vízben, az anaerob bomlás pedig mérgező kénhidrogén, ammónia és metán képződéséhez vezet. E folyamatok a vízminőség drasztikus romlásához vezetnek, szélsőséges esetben halpusztulást és/vagy bűzhatást okozva, vagyis a felszíni vizek trofitása a foszforbevitel csökkentésével javítható.
Diffúz mezőgazdasági vagy pontszerű szennyvízbevezetések ugyancsak a foszforbevitel növekedését okozzák.
Az összes foszfor tartalom valamennyi oldott és oldatlan, szerves és szervetlen foszforvegyület mérőszáma. [3]

## SZENNYVÍZTISZTÍTÓ TELEPEK A RÁBA ALSÓ SZAKASZÁN ÉS MELLÉKFOLYÓI MENTÉN

A Raab/Rába Survey projektben kiemelt figyelmet kaptak a magyar szakasz szennyvíztisztító telepei, mint a Rába magyar vízgyűjtőterületén legnagyobb számban megtalálható szennyezők. Ezek bármelyikén bekövetkező esetleges üzemzavar jelentős vízkémiai kockázatot jelent a Rába folyó élővilágára és a Rába menti településeken élőkre.
A Rába vízrendszerében számos kommunális szennyvíztisztító telep üzemel, ezek kapacitás alapján tett osztályozás szerinti elhelyezkedését a következő áttekintő helyszínrajzon ábrázoltam:




*1. ábra Szennyvíztisztítók a Rába vízgyűjtőjén [4] (Szerkesztette a szerző)*

Természetesen az ábrázolt telepek csak egy része bocsát be közvetlenül a Rábába, zömük első- másod vagy esetleg harmadrendű mellékvízfolyásba bocsátja tisztított szennyvizét.

A Sárvár-Győr szakaszon két közvetlen bebocsátó szennyvíztisztító működik, Szany és Rábacsécsény településeken. A szanyi telep a Rába 40,590 fkm, míg a rábacsécsényi a Rába 16,900 fkm szelvényében vezeti tisztított szennyvizét a folyóba. A szanyi telep 10, a rábacsécsényi pedig 8 db Rába menti település kommunális szennyvizét kezeli. A két szennyvíztisztító elfolyó vizéből vett vízminták önellenőrzési vizsgálati eredményeit a 2010-2018-as időszakra vonatkoztatva bocsátotta rendelkezésemre az üzemeltető Pannon-Víz Zrt. [5]

## A 2007-2018 KÖZÖTTI IDŐSZAK VKI MONITORING EREDMÉNYEINEK HOSSZ-SZELVÉNY SZERINTI ELEMZÉSE

Az egyes vízminőségi paraméterek hossz-szelvény szerinti vizsgálatának alapját, mint referenciaállapotot a 2008-2009-ben a Rába/Raab Survey projektben elvégzett vizsgálatok jelentették. Ezen referenciaállapot a 2007 óta folyamatosan működő VKI[2] felszíni víz monitoring adatokkal vethető össze. A felszíni vizek monitoringja az ökológiai és a kémiai állapot minősítése szempontjából indikatív biológiai elemek és veszélyes anyagok vizsgálatára terjed ki, ezen kívül olyan fizikai, kémiai és hidromorfológiai paraméterekre, amelyek az ökológiai állapotra befolyással bírnak. A VKI előírásai szerinti monitoring és a korábbi hazai mérések együttesen teszik lehetővé a felszíni víztestek jelentős hányadának állapotértékelését. A VKI miatt a felszíni vizek megfigyelésének jellege, az eddig alapvetően kémiai és hidrológiai megfigyelések mellett kibővült biológiai és hidromorfológiai vizsgálatokkal is. [6]

A Rába vizsgált szakaszán 3 db mintavételi ponton állnak rendelkezésünkre vízkémiai vizsgálati adatok, melyek a következők:

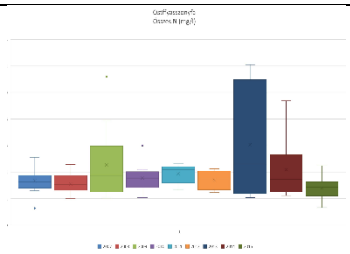
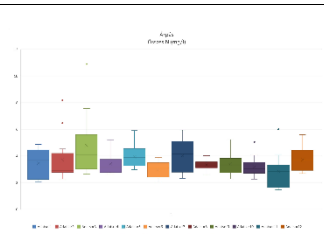
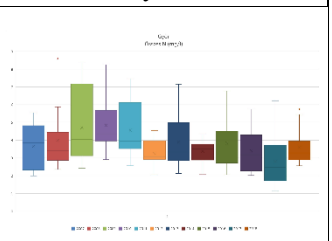
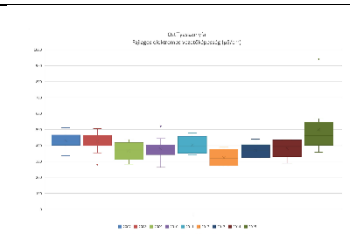
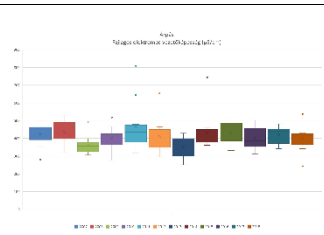
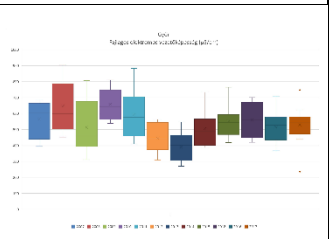
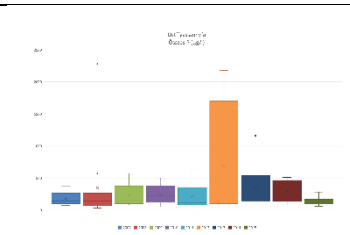
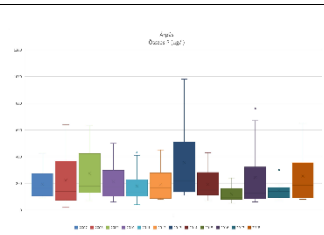
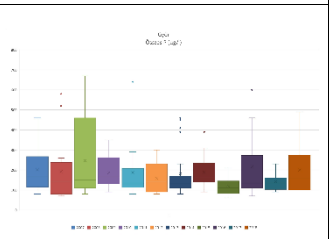
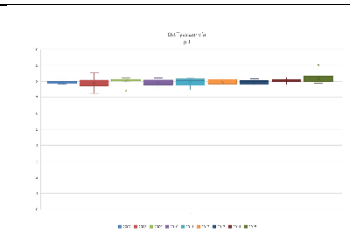
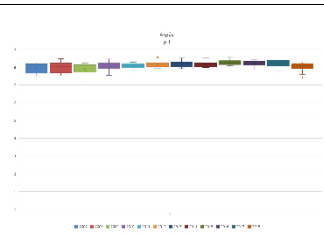
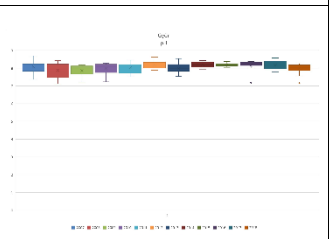
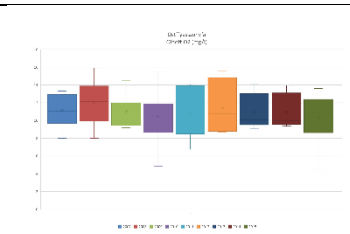
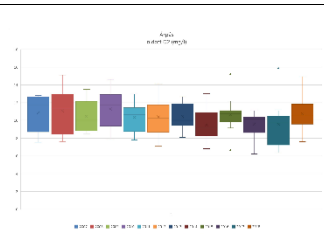
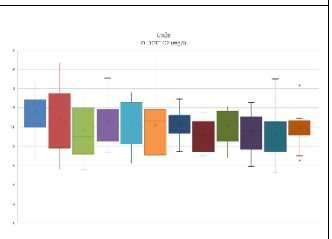
- Rába 73,295 fkm – Ostffyasszonyfa, Ragyogóhíd (2007-2015)
- Rába 29,130 fkm – Árpás vízmérceszelvény (2007-2018)
- Rába 1,629 fkm – Győr (2007-2018)

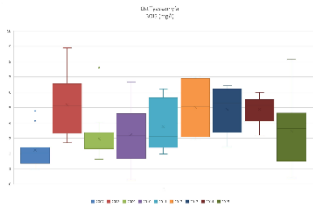
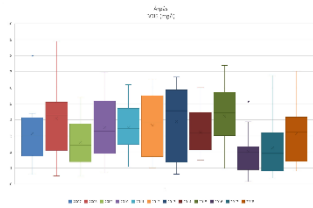
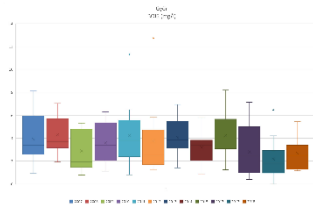
A Rába alsó szakaszának esetleges vízminőség-változásait, valamint a szennyvíztisztítók hatását a folyó vízminőségére a fent említett paraméterek vonatkozásában hossz-szelvény szerinti feldolgozással vizsgáltam.

A VKI mintavételi pontok vízminőségi adatait a vízügyi ágazatban alkalmazott FORRÁS-LIMS adatbázisból nyertem ki. Valamennyi mérési ponton legalább havi gyakoriságú mérések történtek, így minden szelvényből évente legalább 12 mérési eredmény állt rendelkezésemre. [7] Az egyes paraméterek időbeni változásainak szemléltetésére a Box&Whisker (Box plot) módszert választottam, mely egy robusztus módja az évenkénti mérési eredmények vizualizációjának. Az egyes vízminőségi paraméterek időbeni változékonysága is jellemezhető ezzel a módszerrel, az egymást követő évek ábrázolásával. A módszernél az adatok sorba rendezésével az adatok 50%-át egy dobozzal ábrázoljuk, aminek a felső éle az adatok felső kvartilisét (Q3) jelöli, alsó éle pedig az adatsor alsó kvartilisét adja (Q1), így a „doboz" vertikális kiterjedése a változók 50%-át foglalja magában, azaz megegyezik az interkvartilis (iq) terjedelemmel. Az ábra „talpai" az interkvartilis terjedelem 1,5-szeresét (1.5xiq) jelentik, az ezen kívül eső értékek az outlierek. A 3xiq-n kívül eső értékek az adatsor extrém értékei. [8]

Ennek megfelelően az egyes paraméterek éves változásai az érintett Rába-szakasz 3 állomásán a következő grafikonokon ábrázoltam a VKI monitoring megkezdése óta.

[2] Az Európai Unió Víz Keretirányelve

| pm | Ostffyasszonyfa | Árpás | Győr |
|---|---|---|---|
| összes Nitrogén (mg/l) |  |  |  |
| Fajl. el. vez.kép (µS/cm) |  |  |  |
| Össz. Foszfor (µg/l) |  |  |  |
| pH |  |  |  |
| oldott oxigén (mg/l) |  |  |  |

| pm | Ostffyasszonyfa | Árpás | Győr |
|---|---|---|---|
| BOI5 (mg/l) |  |  |  |

*1. Táblázat: VKI kémiai monitoring eredmények a Rába alsó szakaszán [7]*

| | Síkvidéki közepes és nagy folyók (13, 14, 19, 20 típusok) |
|---|---|
| pH | 6,5-9 |
| Vezetőképesség (µS/cm) | <900 |
| Oldott oxigén (mg/l) | >7 |
| $BOI_5$ (mg/l) | <4 |
| Összes N (mg/l) | <3 |
| Összes P ($mg/m^3$) | <250 |

*2. táblázat, 10/2010 (VIII.18.) VM rendelet vízminőségi-komponens határértékek*

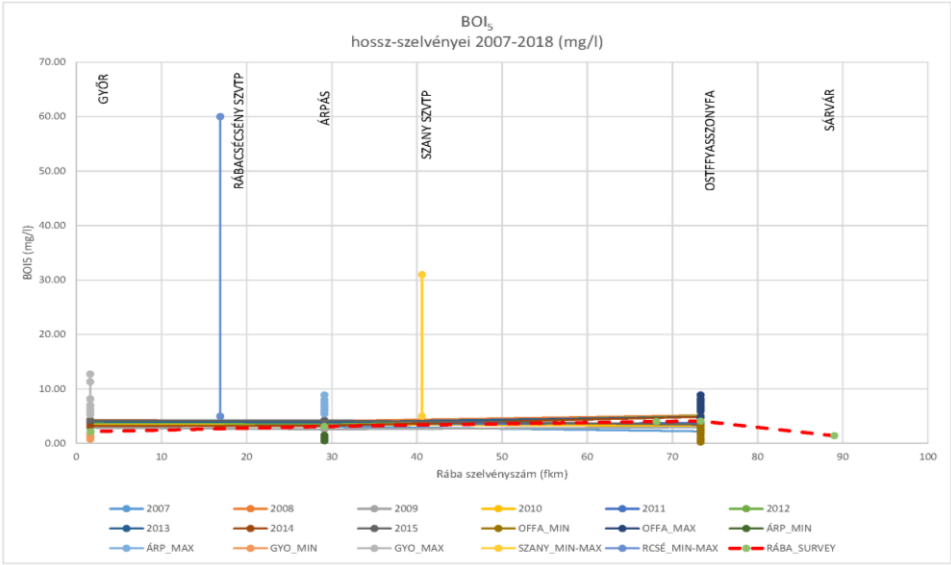
Az egyes vízminőségi paraméterek hossz-szelvény-menti változásait a 10/2010. (VIII. 18.) VM rendelet szerint meghatározott határértékekhez képest vizsgáltam, melyet az 1. sz. táblázatban tüntettem fel. Az egyes vizsgált paraméterek vonatkozásában látható, hogy a Rába $BOI_5$ értéke a felső szakaszon szélesebb, az alsóbb szakaszon kisebb tartományban változik, ebben a két szennyvíztisztító bevezetett tisztított szennyvize nem változtat érdemben, és trendszerű változások sem figyelhetők meg benne. A Rába 2007 és 2018 között havonta mért pH értékei a kívánatos 8 körüli érték körül szóródnak, rendkívül kis változékonysággal, ami jó vízminőséget jelent. Az oldott $O_2$-tartalom is a határérték felett, a kívánatos tartományon belül változik, e paraméter vonatkozásában az alsó szakaszon egy nagyon enyhe csökkenő trend mutatkozik a mérési adatok szerint. Az elektromos vezetőképesség Győrben az időszak első néhány évében, 2007 és 2011 között szignifikánsan nagyobb változékonyságot mutat, mint az azóta eltelt időszakban. Ennek oka kereshető akár a méréstechnológiában is, de utalhat trendszerű változásra az alsó szakaszon, a mért idősor hossza nem elegendő ennek a kérdésnek a megválaszolására. Hasonló a helyzet az összes N helyzetében is, ahol ugyanazon időszak mérési adatai

jóval szélesebb interkvartilissal jellemezhetők. Ostffyasszonyfa esetében mutatkozik 1-1 olyan év az összes N és P vonatkozásában is, ahol a mért adatok 50%-ának értékei lényegesen szélesebb sávban szóródnak a többi év adataihoz képest. Valamennyi komponens esetében kijelenthető, hogy a két szennyvíztisztító hatása nem okoz érdemi változást a Rába alsó szakaszának vízminőségében.

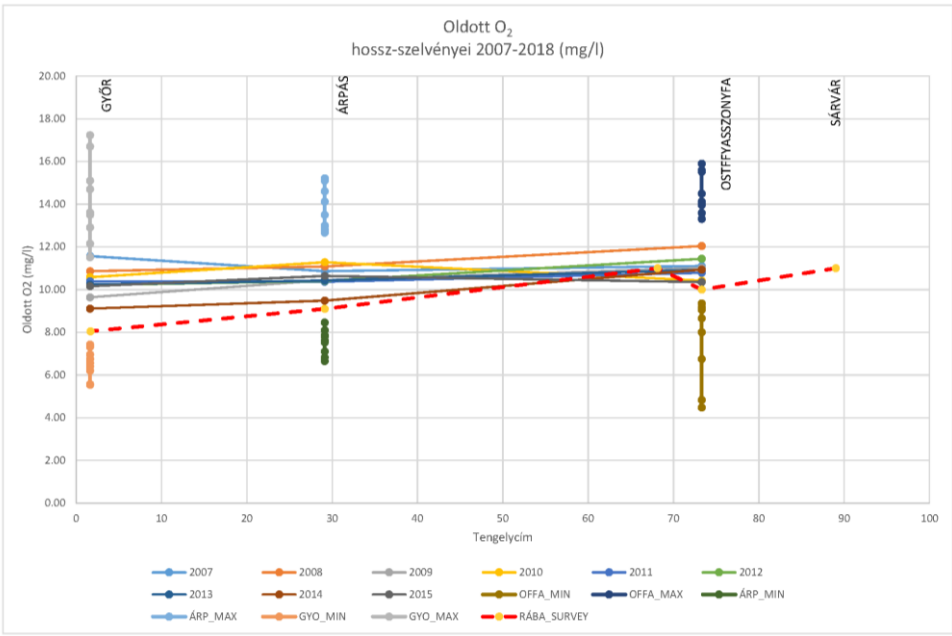
Az adatok hossz-szelvény menti feldolgozásával is szembetűnő ez a jelenség, ami egyrészt a két szennyvíztisztító telep megfelelő üzemére vezethető vissza, másrészt a folyó megfelelő öntisztuló képességére utal.

Ugyanezen vízminőségi komponensek hossz-szelvényei a Rába Sárvár-Győr szakaszára ábrázolva a következő ábrákon láthatók. Az egyes mérési pontokon mért és a bevezetett tisztított szennyvizek eredményeinek szélsőértékeit vertikális metszékekben ábrázoltam, hossz-szelvény szerint pedig az egyes paraméterek éves átlagolt értékeit tüntettem fel. Ezzel az ábrázolással szintén érzékeltethető a paraméter abszolút értelmű változékonysága. Az évenkénti szélsőértékeket megvizsgálva látható, hogy a növényi tápanyagok (N,P) vonatkozásában a vizsgált Rába-szakasz éves maximumai szélesebb tartományban változnak, mint az alsó szakasz mérési helyein, ami a vízgyűjtő felső részéről érkező, szélesebb spektrumon változó vízminőségnek tudható be.

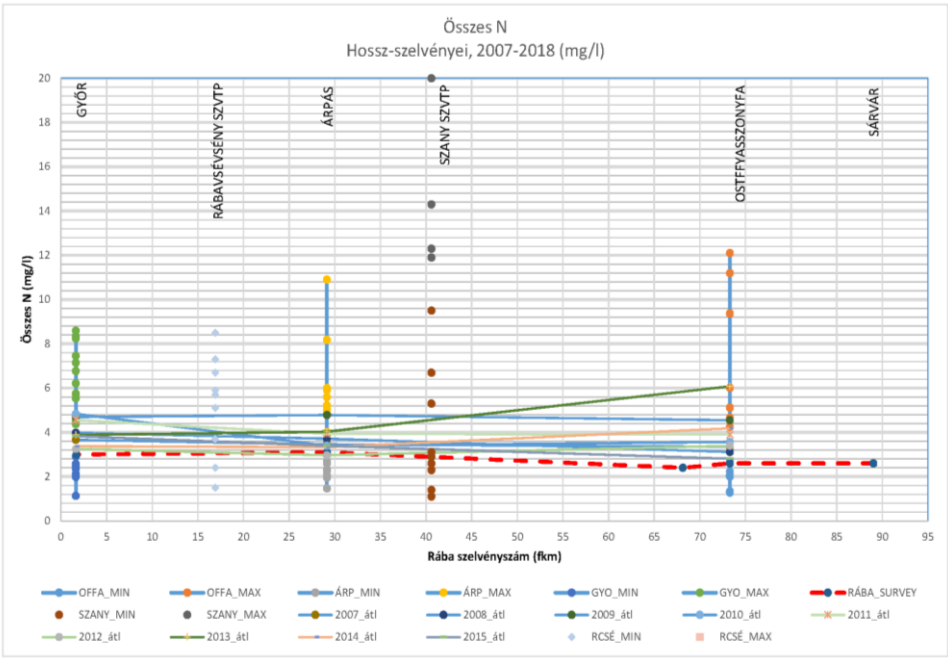
A pH változása hosszmentén sem mutat szignifikáns változást, a kívánatos 8,0 körül változik. $BOI_5$ és az oldott oxigén éven belüli változékonysága a torkolat közelében növekszik, és az oldott $O_2$ hosszmentén enyhe csökkenő trendet mutat a Rába alsó, 90 km-es szakaszán. Az elektromos vezetőképesség Árpásig gyakorlatilag állandó, Árpás és Győr között kismértékű trendszerű emelkedést mutat.



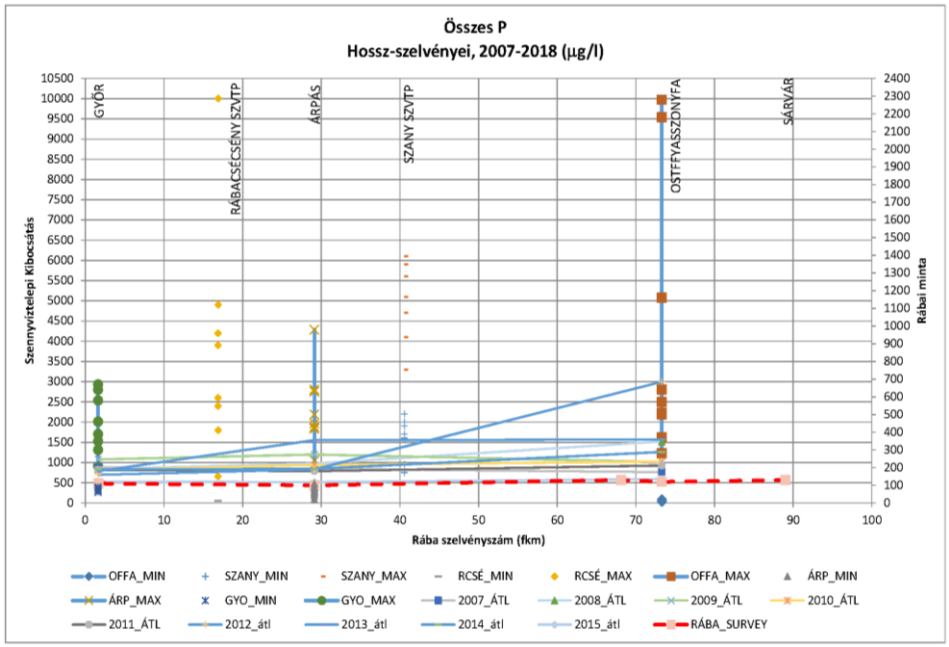

*2. ábra $BOI_5$ hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*



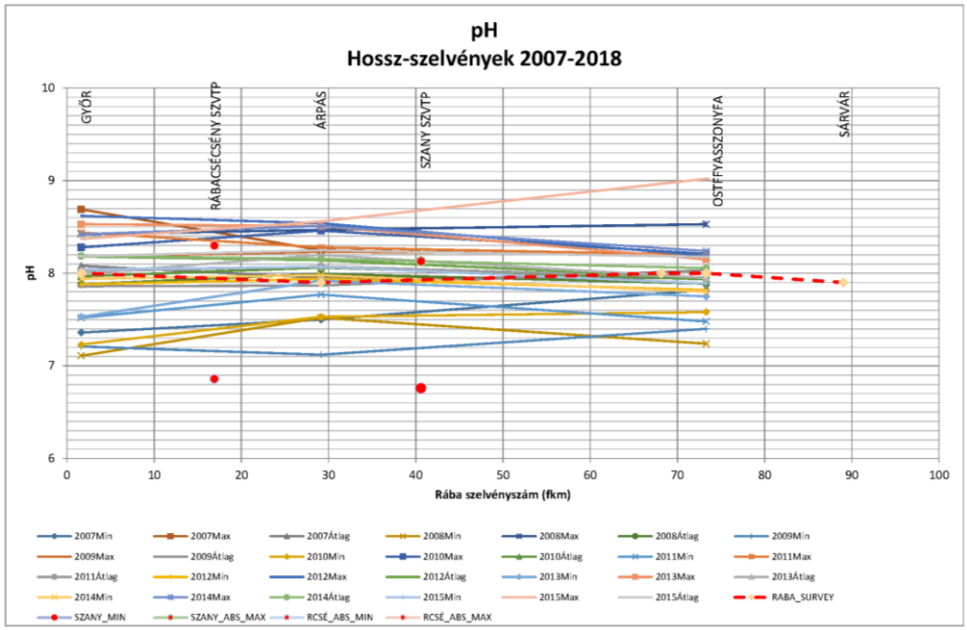

*3. ábra Oldott $O_2$ hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*



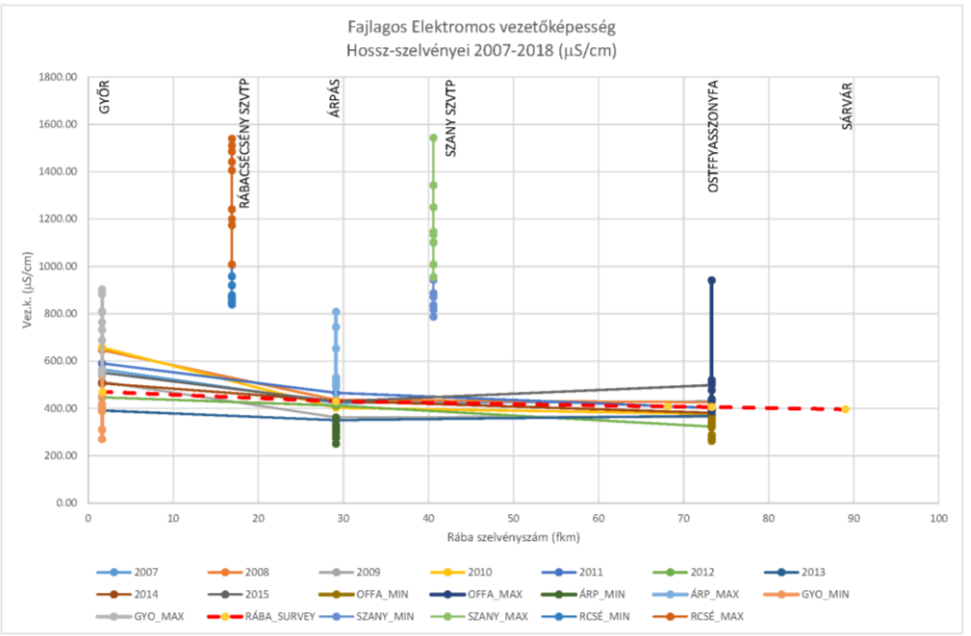

*4. ábra Össz Nitrogén hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*




*5. ábra Össz Foszfor hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*




*6. ábra pH hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*




*7. ábra Fajlagos elektromos vezetőképesség hossz-szelvény; Rába Sárvár - Győr [5], [7] (Szerkesztette a szerző)*

## KÖVETKEZTETÉSEK

A Rába vízminőségi adatainak, valamint alsó szakaszán található közvetlen kommunális szennyvízkibocsátók tisztított szennyvíz-kibocsátásainak vizsgálata arra a fő következtetésre vezet, hogy a normál üzemeltetési helyzetben a vizsgált két szennyvíztisztítónak a Rába alsó szakaszának vízminőségére szignifikáns, hosszabb szakaszon és időhorizonton kimutatható hatása nem jelentős. Ez nyilvánvalóan a Rába természetes vízhozama és a kibocsátott szennyvízhozamok arányából is következik, a Rába több nagyságrenddel magasabb térfogatárama a tisztított szennyvizet megfelelő módon hígítja és elkeveri.

Fontos következtetése a vizsgálatnak, hogy a VKI monitoring mintavételek helyszíneit az idősorok folytonosságát is figyelembe véve kellene kijelölni és üzemeltetni. (Ostffyasszonyfán 2016-tól nincs mintavétel). A VKI monitoring eredmények jó támpontot adnak egy-egy mintavételi helyszín vízminőségi állapotának gyorselemzésére, illetve megfelelő méréstervezés esetén a vízminőség hosszmenti változásaira.

Rendkívül hasznosak a vizsgálati monitoring kampányok a teljes vízgyűjtő vízminőségi állapotának – és így kémiai biztonságának – megfigyelése és elemzése céljából. A Rába vízgyűjtőn a 13 évvel ezelőtti felmérést az elmúlt két évben, szintén közös magyar-osztrák projekt keretében megismételték a változások detektálhatósága érdekében, mely egy új vízminőségi referenciaállapotként szolgálhat a további elemzések elvégzésére.

## IRODALOMJEGYZÉK

[1] Chemistry, SIMO Research Institute of Organic, „http://hu.simo-chemicals.com/news/the-definition-and-components-of-naphthalene-s-11477827.html," [Online]. Available: http://hu.simo-chemicals.com/news/the-definition-and-components-of-naphthalene-s-11477827.html. [Letöltve: 2019. december 5.].

[2] Czigler, Melinda, „http://www.publikon.hu/application/essay/216_1.pdf," [Online]. Available: http://www.publikon.hu/application/essay/216_1.pdf.

[3] VITUKI Nonprofit Kft. - Umweltbundesamt, „Rába Survey 2009 - A Rába hossz-szelvény-vizsgálata," 2009.. [Online]. Available: http://www.nyuduvizig.hu/index.php/vedekezes/informaciok-a-rabarol/raba-survey-2009. [Letöltve: 2019. december 2.].

[4] Országos Vízügyi Főigazgatóság, „Magyarország felülvizsgált, 2015. évi Vízgyűjtő-gazdálkodási terve," 2016. [Online]. Available: http://www.vizugy.hu/index.php?module=vizstrat&programelemid=149. [Letöltve: 2019. december 3.].

[5] Pannon-Víz Zrt., Önellenőrzési eredmények a Szanyi és Rábacsécsényi szennyvíztisztító telepekről, 2019.

[6] Budapesti Műszaki és Gazdaságtudományi Egyetem, „Felszíni vizek Víz keretirányelv (VKI) szerinti monitoringja," [Online]. Available: http://enfo.agt.bme.hu/drupal/sites/default/files/VKI%20szerinti%20monitoring.pdf.

[7] Országos Vízügyi Főigazgatóság, Forrás Lims vízminőségi adatbázis, 2019. Elérhetőség: Észak-dunántúli Vízügyi Igazgatóság

[8] „Bevezetés az SPSS alapjaiba," [Online]. Available: http://docplayer.hu/1145736-Bevezetes-az-spss-alapjaiba-belso-hasznalatra.html. [Letöltve: 2019 december 13.].

# THE EVOLUTION OF ARTIFICIAL INTELLIGENCE RESEARCH

# A MESTERSÉGESINTELLIGENCIA-KUTATÁS FEJLŐDÉSE

PAULIK László [1]

**Abstract**

A few years ago, what is now reality was science fiction. Robotics and artificial intelligence research and development have grown rapidly in the twenty-first century. My study focuses on robots and artificial intelligence. I largely concentrate on the former in my study, and I briefly discuss the history and current state of artificial intelligence research within the context of this essay. I briefly describe the AI systems that are evolving the most quickly. I explore the idea of artificial intelligence as we currently understand it. I briefly address the temporal dynamics of the superintelligences that might develop from generative artificial intelligence while also discussing potential modalities of emergence for such intelligence. I also bring up the subject of responsibility in general.

**Keywords**

artificial intelligence, robotics, artificial intelligence research, superintelligence, machine learning

**Absztrakt**

Ami pár éve még science-fiction volt, az ma már a valóság. A mesterséges intelligencia és vele együtt a robotok kutatása, fejlesztése a XXI. században robbanásszerű fejlődésen ment keresztül. Kutatásom célja az MI és a robotok vizsgálata. Ebben a tanulmányban főként az előbbire koncentrálok, ezen cikk keretein belül ismertetem honnan is indult és hová jutott a mesterségesintelligencia-kutatás. Bemutatom röviden a legdinamikusabban fejlődő MI rendszereket. Körüljárom a mai értelemben vett mesterséges intelligencia fogalmát. Ismertetem a generatív mesterséges intelligencia kialakulásának lehetséges módozatait, valamint a belőle nagy valószínűséggel kialakuló szuperintelligencia lehetséges változatait, röviden érintve ezek idődinamikáját. Megemlítem az emberi felelősség kérdését is.

**Kulcsszavak**

mesterséges intelligencia, robotika, mesterségesintelligencia-kutatás szuperintelligencia, gépi tanulás

[1] paulik.laszlo@bgk.uni-obuda.hu | ORCID: 0009-0007-5332-9327 | assistant lecturer, Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering | tanársegéd, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## BEVEZETÉS

Az elmúlt közel 20 évben a mesterséges intelligencia (MI) és a robotika területén olyan intenzív fejlődést tapasztalhattunk, ami egykor csak a science-fiction világában létező álomnak tűnt. Míg a XX. század második felében főként a katonai és egyetemi szektorban folyt ezeknek a technológiáknak a kutatása és fejlesztése, mára a nagyvállalatok és a technológiai óriások felé tolódott el a súlypont. Ezzel egyidejűleg a robotok és az MI mindennapi életünk részévé váltak, és egyre több területen terjedtek és terjednek el. Ami a jelenünkben újdonság, az a napjainkban vagy a jövőben születő emberek számára már hétköznapi lesz. Az okosházaktól az önvezető autókig már most is tapasztalhatjuk az ember és technológia szorosabb kapcsolatát. Az MI és a robotika egyre inkább összefonódó jövője ígéretes. Eljöhet az asimovi jövőkép, a Jarvisok és Cortanák kora, azonban fontos figyelembe venni a biztonsági és kiberbiztonsági szempontokat, hogy a technológia hasznos és biztonságos maradjon. Az ideális cél egy etikus, generatív mesterséges intelligencia vagy a távolabbi jövőben egy etikus szuperintelligencia megszületése, amely az emberi kultúra és társadalom céljaival összhangban és vele együtt tevékenykedik egy jobb, élhetőbb és fenntartható jövőért.

### Kezdetektől napjainkig

Bár már a középkorban, sőt korábban is voltak az embereknek ez irányú gondolataik és elképzeléseik – elég, ha csak a XVI. századi prágai Gólem legendájára gondolunk – a mesterséges intelligencia és a robotok megvalósításának korát meg kellett, hogy előzze a kibernetika kialakulása, mely a XX. század korai évtizedeiben kezdi meg bontogatni a szárnyait. Ezen kívül vagy éppen emellett három fontos feltételnek kellett még teljesülnie. A számítógépek számítási kapacitásának és sebességének fellendülése, a megfelelő mennyiségű adat felhalmozása (digitális formában) és a megfelelő matematikai és statisztikai módszerek kidolgozása. Mindez az 1990-es évek végétől kumulálódott oly mértékben, hogy eljussunk oda, ahol jelenleg tart a technológia.

A gondolkodó gép ötlete az informatika és a mesterséges intelligencia korai fejlődése során kezdett formálódni. Az első jelentős gondolatok és elméletek a gondolkodó gépekről az 1950-es években jelentek meg. Az egyik meghatározó alakja a témának ezen a területen Alan Turing, aki már korábban (1936) megfogalmazta a „Turing-gép” koncepcióját, amely egy absztrakt számítógépes modellt jelentett, amely képes lenne elvégezni bármilyen számítási feladatot, amit egy algoritmus leírhat. 1947-ben ír először a számítógépes intelligenciáról. Valamint megalkotja a Turing-tesztet (1950). Munkássága nagymértékben hozzájárult a mesterséges intelligencia és a gondolkodó gépek fejlesztéséhez. Az ezt követő évtizedeket a fellángolások és a szkepticizmus időszakainak a váltakozásai követték. 1956-ban a Darthmouth Summer Projekttel megindult egy fejlődési folyamat. A projektben Dr. John McCarty szervezésében közel 10 tudós vett részt egy több hétig tartó workshopon, amely a mesterségesintelligencia-kutatás hajnalának is nevezhető. Az ez utáni időszakban olyan rendszereket hoznak létre a tudósok, amely az addig lehetetlennek tartott feladatokat oldják meg. A korai rendszerek matematikai tételeket tudtak bizonyítani, IQ tesztek bizonyos feladatait tudták megoldani vagy például egy ELIZA nevű program meg tudott személyesíteni egy úgynevezett „nem irányított terápiának” is nevezett módszerrel dolgozó pszichoterapeutát.

Ezen korai MI-k legnagyobb problémája a „kombinatorikai robbanás”, melynek a lényege, hogy egy adott szűkebb feladat megoldására alkalmasak voltak ugyan, de amint megpróbálták kiterjeszteni a megoldandó problémák körét, a megoldási lehetőségek száma, amelyből mindent vizsgálta volna a program, ugrásszerűen megnőtt és meghaladta az akkori számítógépek számítási kapacitását, akár több nagyságrenddel is. Olyan képességekkel, mint például a heurisztikus keresés vagy a flexibilis absztrakt reprezentációk, melyek alkalmasak lettek volna ezen probléma áthidalására, még nem igazán rendelkeztek ezek a korai rendszerek. Erre a tudósok is rájöttek és persze idővel a támogatók is. A 70-es évek közepére beköszöntött az első „MI-tél”, amikor is úrrá lett a szkepticizmus, kiapadni látszottak a kutatásokat támogató források. A mesterséges intelligencia és a vele kapcsolatos kutatások hirtelen nem voltak annyira népszerűek, mint addig.

De nem kellett sokat várni, hogy feltámadjon az érdeklődés. A 80-as évek elején Japánban beindul az Ötödik Generációs Számítógépes Rendszerek elnevezésű program, mely egyaránt kap komoly támogatást az állami és a versenyszférából is. Elsődleges célja egy olyan, az akkori csúcstechnikát meghaladó számítógépes architektúra létrehozása, mely az eddigieknél hatékonyabb terepe lehet a mesterséges intelligencia alkalmazásának. A japán példát követve több ország is újra felkarolja az MI-kutatásokat. Ez hozza el a szakértői rendszerek felemelkedését, melyek fő szerepe a döntéshozók megsegítése volt tényalapú tudásbázis alapján, amit nagy munkával és kézzel, formális nyelven kódolva kellett bevinniük emberi szakértőknek. A kezdeti sikerek után azonban mégsem váltották be a hozzájuk fűzött hosszú távú reményeket. Vagy hasznuk volt csekély, mint a kisebb rendszereknek, vagy pedig kifejlesztésük, fenntartásuk és naprakészségük volt irracionálisan erőforrásigényes és használatuk is nehézkes volt. Így hát a nyolcvanas évek végére újra fagyos lett a hangulat az MI körül, eljött a második tél időszaka.

Persze a technikai fejlődés nem állt meg, így az 1990-es évekre az enyhülés jelei mutatkoznak. Ezek az újfajta vívmányok jó alternatívákat kínáltak a hagyományos logikai alapokra épülő módszerekkel operáló régi, merev megközelítések (GOFAI – Good Old-Fashioned Artificial Intelligence) mellett. A két legnépszerűbb, a neurális hálózat és a genetikai algoritmus eléggé ígéretesnek tűnt, hogy megoldjon olyan problémákat, amelyekkel a GOFAI nem boldogult. A neurális hálózatok olyan matematikai modellrendszerek, amelyek az emberi agy neuronhálózatának működését utánozzák. Ez a megközelítés lehetővé teszi a rendszerek számára a komplex feladatok megoldását, például képfelismerést vagy nyelvi feldolgozást. Ezek a hálózatok apróbb hibákra kisebb mértékű teljesítménycsökkenéssel reagáltak, míg a klasszikus, merev MI-k ilyenkor érthetetlen eredményt produkáltak vagy akár összeomlásukhoz is vezethetett. A legfontosabb jellemzőjük a neurális hálózatoknak azonban a tanulási képesség, a mintafelismerés és a csoportosítási problémák megoldása.

A másik főszereplői az enyhülésnek az evolúción alapuló rendszerek megszületése. A genetikai algoritmusok és genetikai programozási technikák megoldási lehetőségek populációival dolgoznak. A populációk mutációinak és rekombinációinak kidolgozásával a megoldások új lehetőségei jönnek létre, majd azokat új szűrési feltételek mentén ritkítják, hogy csak a legjobb lehetőségek maradjanak meg a következő generációra. Több száznyi vagy akár ezernyi generáció ismétlődése során a megoldások minősége fokozatosan növekszik.

Előnye ennek például az, hogy a kezdeti feltételek megadása után gyakorlatilag nem szükséges az emberi beavatkozás, hátránya viszont, hogy nehéz őket hatékony működésre bírni tapasztalat és tehetség híján, valamint gyakran előfordul, amikor az evolúciós keresés nem jut el egy számunkra ideális eredményre, csak bolyong a keresési halmazban vagy éppen megakad egy lokális optimumponton, ami csak félsiker.

Az 1990-es évek végétől napjainkig az MI-kutatás tovább folytatta fejlődését. Az új évezred kezdetén számos technológiai és társadalmi változás indította el az MI területén bekövetkező áttöréseket. Az adatmennyiség robbanásszerű emelkedése és a számítási kapacitás folyamatos növekedése (összefügg a Moore-törvénnyel: kétévente megduplázódik az integrált áramkörök összetettsége) jelentős lendületet adott a mesterségesintelligencia-kutatásának. Az internet megjelenése és széles körűvé válása, valamint a digitális eszközök elterjedése lehetővé tette, hogy hatalmas adatbázisokat és adathalmazokat gyűjtsünk és tároljunk. Ezek az adatok kulcsfontosságúak lettek a mesterségesintelligencia-rendszerek tanításához és fejlesztéséhez. Az algoritmusok terén számos fejlesztés történt, amelyek hatékonyabbá és pontosabbá tették az MI rendszereket.

Az igazi fellendülés és újraéledés a gépi tanulás terén is ez idő tájt, a 1990-es években következett be. Ekkor jelentek meg új algoritmusok és módszerek, mint például a támogató vektor gépek (Support Vector Machines) és a döntési fák (Decision Trees). Az említett számítási kapacitás növekedése és az adatgyűjtési technológiák fejlődése lehetővé tette nagyobb adathalmazok és komplexebb problémák feldolgozását. A 2000-es évektől kezdve a gépi tanulás egy még újabb korszakába lépett, amit az ún. mély tanulás (deep learning) fémjelzett. A mély tanulás egy olyan neurális hálózatokon alapuló megközelítés, amely több rétegben feldolgozza és reprezentálja az adatokat, és így képes magasabb szintű absztrakciókat és komplex feladatokat is elvégezni. A mély tanulás rendkívül sikeres lett a képfelismerés, beszédfelismerés, nyelvi feldolgozás és más területeken.

A mesterséges intelligencia alkalmazási területei is bővültek az elmúlt évtizedekben. Az MI technológiákat használják például az autonóm járművekben, a virtuális asszisztensekben, a gépi tanulás alapú ajánlórendszerekben és a termelési folyamatok optimalizálásában. Az MI további területei közé tartozik az egészségügy, a pénzügy, az oktatás, az energiaipar és a kiberbiztonság. Az üzleti világban is egyre nagyobb hangsúlyt kap az MI. A vállalatok felismerik az MI-ben rejlő lehetőségeket a hatékonyság növelése, a döntéshozatal támogatása és az ügyfélélmény fejlesztése terén. Az MI alapú analitika és prediktív elemzések segítségével a vállalatok nagy mennyiségű adatot tudnak feldolgozni és értékes információkat nyerni a versenytársak, a piac és a fogyasztók viselkedésével kapcsolatban. Megkezdődött, illetve folytatódott a robotok, valamint a (főként katonai) drónok és a mesterségesintelligencia-rendszerek összeolvadása.

A gépi tanulás és az MI területén végzett kutatások az elmúlt években is dinamikusan fejlődtek, de jelenünkben ez már exponenciálissá vált. Az egyre összetettebb és intelligensebb rendszerek kifejlesztése és az emberi intelligencia utánzása továbbra is kiemelt cél. Ugyanakkor a kutatók és szakemberek számos kihívással is szembesültek, például az etikai és jogi kérdésekkel, a biztonsági kockázatokkal és a társadalmi elfogadással kapcsolatban.

Összességében az MI-kutatás az 1990-es évek végétől napjainkig látványos fejlődést mutatott. Az adatmennyiség robbanásszerű növekedése, a fejlett algoritmusok és az alkalmazási területek bővülése lehetővé tette az MI-technológiák széles körű felhasználását.

A jövőben további innovációk és áttörések várhatók, amelyek tovább formálják és fejlesztik az MI-kutatást és alkalmazásokat.

**A mesterséges intelligencia: erős vagy gyenge?**

A mesterséges intelligencia fogalma, bár napjainkban az egyik legdivatosabb kifejezés, sokféleképpen értelmezhető. Egyelőre azonban semmiképpen sem úgy, ahogy az interpretálva van az átlagember számára, azaz vagy világmegváltó és -megmentő szuperelme vagy éppen azt elpusztító „Skynet". Valójában nagyon sokszor nincs éles határvonal a mesterséges intelligencia és az általános, de fejlett szoftverek között. Már pár évtizede léteznek olyan mesterséges intelligencia alapú rendszerek, amelyek bizonyos területeken túltesznek az emberi intelligencián. Ilyenek az úgynevezett játékos MI-k. Ezek közül bőven találunk szakértői szinten működőket, de szép számmal akadnak emberfeletti teljesítményűek is.

1994-ben a CHINOOK nevű program megveri a világbajnokot dámában, ez az első alkalom, hogy egy program nyer meg egy szellemi világbajnokságot. 1997-ben a Deep Blue sakkprogram megveri Garri Kaszparov, többszörös sakkvilágbajnokot. Azóta már a sakkprogramok túlhaladták ezt a szintet. Ezeken kívül jó pár játékban az MI-k meghaladják az emberi teljesítményt (ostábla, Scrabble, pasziánsz). Persze vannak még meghódítható területek, hiszen bár a Google DeepMind AlphaGo algoritmusa 2016-ban visszavonulásra készteti a dél-koreai go világbajnokot, Li Sze Tolt, 2023-ban az amerikai Kellin Pelrine 15-ből 14-szer győzött a játékban a KataGo nevű MI ellen.

Korábban a tudósok azt gondolták, ha létrehoznak egy nagymester szintű sakkprogramot, akkor az rendelkezni fog egyfajta általános intelligenciával. De valójában nem így van, ezeknek a programoknak korlátozott képességeik vannak. Egy sakkmesteri szintű MI nagyon jól sakkozik, de semmi több, hiszen valójában egy meglehetősen egyszerű algoritmus áll mögötte. Ma már az élet rengeteg területén használunk ilyen korlátozottabb, de az adott területükön nagyon is hatékony mesterségesintelligencia-rendszert. Útvonaltervező programok, az internetes keresésen alapuló reklámajánló rendszerek, orvosi képdiagnosztizáló algoritmusok, robotfűnyírók, chatbotok, e-mail forgalom felügyelő szoftverek vagy éppen a globális pénzpiacon működő MI-k, csakhogy a teljesség igénye nélkül párat felsoroljunk.

Ezek a rendszerek tulajdonképpen „gyenge MI"-nek tekinthetők, melyek jellemzője, hogy segítik az emberi gondolkodást, és ezekben a szűkebb feladatkörökben, ha meg is haladják a képességeinket, de összességében nem érik el az általános emberi intelligencia szintjét. A konzervatívabb, és persze óvatosabb tudósok (pl.: Nilsson, Minsky, Winston) egy efféle jövőképre koncentrálnak, ahol talán nincs is helye egy generatív mesterséges intelligenciának, sem pedig a belőle kifejlődő szuperintelligenciának. A kutatók másik része (pl.: Bostrom, Amstrong, Sotala) viszont nagyobb valószínűséggel feltételezi az „emberi szintű gépi intelligencia" (Human Level Machine Intelligence, HLMI) létrejöttét. Bár eme tudósok kellő magabiztossággal predesztinálnak, de a mérföldkövek időpontjáról nagy szórással nyilatkoznak. Jövendölésük lényege, hogy el fog jönni a mesterséges intelligencia generatív szintje, amit erős MI-nek is neveznek. Ez a generatív mesterséges intelligencia képes lehet azokra a kognitív funkciókra, szinte az összesre, vagy akár az összesre is, amelyekkel rendelkezik egy emberi agy. Jelenleg ettől még eléggé távol áll a technológia. Persze, a már fentebb említett szűkebb területeken meghaladhatja a képességeinket, de ez alapvetően a számítási kapacitás és az adattároló képességek különbségéből fakad. Az emberi

absztrakt gondolkodás, a kreativitás, az intuíció vagy akár az érzelmek, csakhogy a legfontosabbakat említsük, még nem jellemzőjük az MI-nek.

A kutatók előrejelzései a lehetséges eredményekkel kapcsolatban igencsak tág időintervallumokat ölelnek fel, a következő évtizedtől akár a század végéig bezárólag. Valójában a legfontosabb kérdés ezzel kapcsolatban nem az időpont, hanem az, hogy az általános emberi szintű mesterséges intelligencia – amennyiben létrejön – milyen hatással lesz az emberiségre, illetve mennyi időbe telik, míg tovább fejlődhet a szuperintelligencia szintjére.

**Az MI jövője**

A szuperintelligenciák kifejlődésének több módozatát is elképzelhetőnek tartják, ezek közös célja az emberi intellektusnál fejlettebb mesterséges intelligencia létrehozása. Bár jelenleg a reflektorfényben a „klasszikus" MI-k állnak, köszönhetően talán az OpenAI ChatGPT-jének, valójában több útját is felvázolták egy emberi szintű, illetve egy abból kifejlődő, de annál fejlettebb mesterséges intelligencia létrejöttének. Ezeket itt csak megemlítem, de részleteikbe nem megyek bele.

A klasszikus mesterséges intelligencia mögött a programozás, algoritmusok és gépi evolúció állnak és hozhatják el a végső célt, ezek fejlődését fejtettem ki fentebb. A következő lehetséges út a teljes agy emulációján alapuló technológia, mely ma még csak gyerekcipőben jár. Egy emlősagy emulációja – beleértve az emberi agyat is – ma még olyan formában, hogy az MI-ként, netán szuperintelligenciaként működhetne, nem lehetséges. Az emulációs út megvalósulásának a lehetősége nem tűnik lehetségesnek a közeljövőben. A jelenlegi technikai fejlettségünk még nem teszi ezt lehetővé, bár részeredmények vannak (férgek egyszerű idegrendszerének emulációja).

Megemlítjük a biológiai gondolkodás útját is, amely tulajdonképpen egy géntechnológiával megtámogatott mesterséges evolúcióval megvalósuló intelligencianövekedés magában az emberiségben, de az itt elérhető reális cél, hogy ez a növekedés elhoz egy olyan technológiai fejlődést, amely révén könnyebben kreál az emberiség egy gépi MI-t. A harmadik lehetséges narratíva kollektív intelligencia létrejötte. Az emberi tudásfelhalmozás, mely napjainkra már egy tudat-hálónak is tekinthető, az írás, nyomtatás és végül az internet fejlődésvonalán keresztül, melegágya lehet egy MI kialakulásának.

A fő kérdés az, hogy válhat-e MI-vé az interneten felhalmozott óriási információmennyiség, öntudatra ébredhet-e? Spontán módon erre nem sok esélyt látnak a szakértők, de mi van, ha ez direkt generált folyamat? Végül megemlítjük az agy–számítógép interfészek nem újkeletű ötletét. Itt elsősorban a terápiás eljárásokban hozhat a technológia áttörést, és csak elenyésző az esélye, hogy egy számítógép és az emberi agy összeolvadásából jöjjön létre egy szuperintelligencia. Sokkal nagyobb a valószínűsége a többi megemlített verzió megvalósulásának. Elviekben bármelyik úton is, de megszülethet egy valódi szuperintelligencia, akár párhuzamosan is, egymás létrejöttét szinergista módon segítve.

Ha a kialakult szuperintelligenciát pontosabban szeretnénk definiálni, és megérteni, szét kell bontanunk annak fajtáit, amelyek közül hármat említenek a leggyakrabban. A gyors szuperintelligenciát, a kollektív szuperintelligenciát és a minőségi szuperintelligenciát. A gyors verzió minden tud, mindenre képes, amit, illetve amire az emberi agy képes, de azt sokkal, akár nagyságrendekkel gyorsabban. Ez a fajta szuperintelligencia inkább a digitális térben tevékenykedhet majd hatékonyan, hiszen a mi világunk történéseinek valós

ideje számára rettentően lassú lesz. Percek, vagy akár másodpercek alatt képes lesz elvégezni egy ember évnyi munkáját; évek, vagy akár hónapok alatt évezredek kutatótevékenységét, persze csak egy virtuális valóságban. Létezik számukra is egy felső korlát, hiszen fénysebességnél gyorsabb kommunikációra, jelenlegi tudásunk szerint legalábbis, ezek sem lennének képesek. Valamint, ha az emberi elméből indulunk ki, felvetődhet a kérdés, hogy ha számukra úgy telik az idő, mint ahogy, akkor az anyagi világ lassúsága nem okoz-e valamiféle mentális problémát nekik, amit akár nevezhetünk egyfajta „őrületnek". Egyelőre azonban ezek csak hipotetikus kérdések.

A kollektív szuperintelligencia tulajdonképpen sok kisebb intelligenciából felépülő rendszer, melynek összteljesítménye túlszárnyalja a mai technológiák képességeit. Ez egy kevésbé határozott körvonalakkal rendelkező definíció, mint a gyors változat. Tulajdonképpen ennek egy korai, ám biológiai formáját megtaláljuk már az emberi történelemben. Hiszen már a törzsközösség is egyfajta magasabb rendű és kollektív elmeként funkcionál az egyetlen emberhez képest, amely a túlélésért folytatott harcban hatékonyabbnak bizonyult. A kollektív szuperintelligencia teljesítménye nagyban függ annak integráltságától. Ahhoz, hogy igazán nagy magasságokba emelkedjen, az szükséges, hogy egy lazább kapcsolatokkal rendelkező rendszer integráltságát fokozatosan növeljük és így válhat egyetlen szuperelmévé, amely már végül minőségi intelligenciának tekinthető.

Ezzel el is jutottunk a harmadik formához, a minőségi szuperintelligenciához, amely gyorsaságában az emberi szintet éri el, de legalábbis nem haladja meg túlságosan azt, viszont minőségileg egy magasabb szintet képvisel, akár nagyságrendekkel is. Ez szintén egy ködbe vesző terület, hiszen semmi tapasztalatunk nincs egy, a miénknél magasabb intelligenciáról. A legtöbb, amit tehetünk egyelőre, hogy egyfajta viszonyítási alapot képzünk abból, hogy léteznek nálunk kevésbé intelligensebb létformák. Így próbálhatjuk meg azt feltárni, hogy egy minőségi intelligencia annyival „okosabb" nálunk, mint amennyivel mi vagyunk intelligensebbek a csimpánzokhoz, delfinekhez vagy egyéb emlősfajokhoz képest. Az már persze még ennél is ijesztőbb lehet, ha elképzelünk egy nagyobb szakadékot, hiszen nem tudhatjuk, hogy egy efféle intellektus milyen logika, etika és morál mentén értelmezi a valóságunkat. Elvégre igazán kevés ember érez megbánást egy ízeltlábú vagy netán egy egysejtű elpusztításakor.

Egy dolog biztosnak látszik, bármelyik forma idővel képessé válna megalkotni a másik kettőt. A kérdés inkább abban rejlik, hogy mi képesek vagyunk-e megalkotni azt a mesterséges intelligenciát, amely majd kialakítja valamelyik szuperintelligenciát. Abban alapvetően megegyeznek a vélemények, hogy nekünk lesz a legtöbb időre szükségünk eljutni addig a technológiai áttörésig, amikor ez a faktor már kikerül a kezünkből és egyre rövidebb idő alatt jut el az egyik pontból a másikba a történet. Végezetül egyelőre kellő magabiztossággal kijelenthetjük, hogy olyan állomásán vagyunk ennek a fejlődési folyamatnak, amikor még van lehetőségünk befolyásolni a történéseket, a fejlődés irányát és akár az ütemét is. De ez nemcsak lehetőség, hanem inkább kötelességünk is az eljövendő nemzedékek érdekében.

## ÖSSZEGZÉS

Míg a XX. századot nevezhetjük az atomkor évszázadának, addig jogos a felvetés, hogy a XXI. századot nem tekinthetjük-e a mesterséges intelligencia korának. A technológia kialakulásának hajnala, mint láthattuk, az elmúlt évszázad közepén indult, de a nagy

áttörések és a széles körű elterjedése egyértelműen a 2000-es évektől jellemzik az ágazatot. Ahogy fejlődött a számítástechnika, a kibernetika és az információelméleti tudományterület, úgy sikerült túljutni a buktatókon és egyre fejlettebb rendszereket létrehozni. Így, bár voltak hullámvölgyek, egyre messzebb jutottunk a mesterséges intelligencia megvalósításának történetében. Mint látjuk, nem tudhatjuk pontosan, hogy a nagyon közeli jövőben történik meg az áttörés, vagy még évtizedeket kell várni a megvalósulásig, de a trendek már most látszanak. A lehetséges jövőbeli fejlődési utakról megvannak az elképzelések. Hogy valójában milyen formában manifesztálódik mindez, az majd ténylegesen csak visszatekintve kristályosodik ki számunka.

Végezetül, bár ebben a cikkben nem foglalkozunk bővebben az MI társadalomra gyakorolt hatásával, azonban mint már fentebb utaltunk rá, és ez számottevő tudós véleménye is, valamint jómagam is így gondolom, kevesebb idő lesz, míg az emberi szintű MI eljut a szuper MI szintjére, mint amennyi idő eltelik az emberi szintű MI-k megjelenéséig, tehát ha van időnk felelősen cselekedni, az még most van. Ezen kívül, és ez már tényleg csak sötétben tapogatózásnak tűnik, a lehetséges végkimenetelek közül a szélsőségesek – utópia kontra armageddon – azok, amelyek valószínűségét a két táborra szakadt tudósvilág, az óvatosak és az optimisták is, elképzelhetőbbnek tartanak, mint egy kiegyensúlyozottabb forgatókönyvet. Ezek alapján komoly felelősség nyomja a jelenkor tudósainak és döntéshozóinak a vállát.

Egy biztosnak látszik a jelenünkben. A szellem már kiszabadult a palackból. Egyelőre azonban nem önmagában az MI jelent jelentős veszélyt ránk nézve, hanem annak emberi felhasználása. Homokba azonban nem dughatjuk a fejünket. A mesterséges intelligencia jött és látott. A nagy kérdés az, hogy győz-e, és ami még fontosabb, hogy ellenünk vagy velünk együtt?

## FELHASZNÁLT IRODALOM

[1] Nick Bostrom: Szuperintelligencia. Első kiadás. Bp., Ad Astra Kiadó, 2015. (Eredeti-megjelenés: Oxford University Press, 2014.) 464 oldal. ISBN 978-615-5229-61-9
[2] Tilesch György és Omar Hatamleh: Mesterség és intelligencia. Első kiadás. Bp., Libri Kiadó, 2021. 240 oldal. ISBN 978-963-433-829-1
[3] Kollár Csaba: A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában. In: Kiberbiztonság – Cybersecurity 2. Szerk.: Prof. Dr. Rajnai Zoltán). Bp., Biztonságtudományi Doktori Iskola, 2019. 47-61. p. ISBN: 978-963-449-185-9
[4] https://80000hours.org/problem-profiles/artificial-intelligence/
[5] https://index.hu/techtud/2019/11/27/a_mesterseges_intelligencia_miatt_visszavonul_a_go_kira lya/
[6] https://www.britannica.com/biography/Alan-Turing
[7] https://www.europarl.europa.eu/news/hu/headlines/priorities/mesterseges-intelligencia-az-eu-ban/20200827STO85804/mi-az-a-mesterseges-intelligencia-es-mire-hasznaljak
[8] https://www.europarl.europa.eu/news/hu/press-room/20201016IPR89544/a-mesterseges-intelligencia-fejlesztesenek-etikai-es-jogi-oldala-ep-ajanlasok
[9] https://hvg.hu/tudomany/20230220_go_jatek_mesterseges_intelligencia_kellin_pelrine_ember_legyozte_a_gepet

# ROLE OF ARTIFICIAL INTELLIGENCE IN FOOD SAFETY

# A MESTERSÉGES INTELLIGENCIA SZEREPE AZ ÉLELMISZERBIZTONSÁGBAN

REVOLY ANDRÁS[1] – TARR BENCE [2] - Dr. SZABÓ ISTVÁN[3]

**Abstract**

The emergence of precision agriculture poses new safety challenges for farmers. The development of digital production systems requires the acquisition of IT tools, sensors, the establishment of telecommunication networks and the installation of complex database management and analysis software. These tools not only require investment, but also present producers with security challenges they have not had to face before. We have to be prepared to defend against attacks on traditional IT systems. To do this, farmers will need protection and security solutions that have not been used before. Nevertheless, modern technologies are the right answer to the growing challenges of productivity, food safety and food quality. Artificial intelligence can be an effective complementary tool.

**Keywords**

artificial intelligence, precision farming, food safety, vertical farms

**Absztrakt**

A precíziós mezőgazdaság megjelenése új biztonsági kihívások elé állítja a mezőgazdasági termelőket. A digitalizált termelési rendszerek kialakításához informatikai eszközök: érzékelők beszerzésére, távközlési hálózatok kiépítésére és összetett adatbázis-kezelő, valamint elemző szoftverek alkalmazására van szükség. Ezek az eszközök olyan biztonsági megoldásokat kívánnak a termelőktől, amelyekkel korábban nem kellett szembesülniük. Felkészültnek kell lenniük a hagyományos informatikai rendszereket érintő támadások elleni védelemre is. A mesterséges intelligencia hatékony kiegészítő eszköze a digitális termelési technikáknak tovább növelve a termelékenységet és javítva az élelmiszer biztonságot.

**Kulcsszavak**

mesterséges intelligencia, precíziós mezőgazdaság, élelmiszer-biztonság, vertikális farm

[1] Revoly.Andras@uni-mate.hu| ORCID: 0009-0002-6468-1098 | Phd. student, Institute of Technical Sciences, Hungarian University of Agriculture and Life Sciences | Phd. hallgató, MATE Műszaki Intézet

[2]Tarr.Bence.Gyula@uni-mate.hu| ORCID: 0009-0004-1790-9234 | Phd. student, Institute of Technical Sciences, Hungarian University of Agriculture and Life Sciences | Phd. hallgató, MATE Műszaki Intézet

[3] Szabo.Istvan.prof@uni-mate.hu | ORCID: | Professor, Institute of Technical Sciences, Hungarian University of Agriculture and Life Sciences | Professzor, MATE Műszaki Intézet

## BEVEZETÉS

A precíziós mezőgazdaság nem csak a modern kor követelménye, nem puszta kényszer melyet a technológiai fejlődés diktál. Hanem az egyik legjobb eszköz arra, hogy a mezőgazdasággal szemben támasztott, egyre növekvő igényeket fenntartható módon kielégítsük. A precíziós mezőgazdaság növeli a termelékenységet, javítja az erőforrások – például a növényvédő szerek, műtrágyák, víz, takarmány és munkaerő – hatékonyabb elosztását, stabilabb termelést biztosít, és csökkenti a mezőgazdasági termelés környezeti hatásait [1].

A precíziós mezőgazdaság megoldásai a piaci szereplőknél egyre nagyobb szerepet kap, alkalmazása folyamatosan bővül. Mára elmondhatjuk, hogy a piacon egyszerre van jelen a nagy és közepes gazdaságok modern, informatika-vezérelt termelési rendszere és a kisméretű gazdaságok hagyományos termelési módszerei.

Az ENSZ Élelmezési és Mezőgazdasági Szervezete szerint az élelmezésbiztonság négy fő alapelve az élelmiszer elérhetősége, hozzáférhetősége, felhasználása és stabilitása.

A precíziós mezőgazdaság bevezetése új biztonságtechnikai feladatok megoldását teszik szükségessé, a precíziós technológiát alkalmazó mezőgazdasági szereplőknek.

Amíg tehát egyfelől a digitális megoldásokkal javítható, ez élelmiszer-biztonság, addig maguk a gazdaságok bizonyos értelemben sebezhetőbbé válnak. A modern digitalizált gazdaságok esetében megjelennek ugyanazok a biztonságtechnikai problémák, amelyekkel más technológiai vállalatok már korábban szembesültek. Az érzékelők és a szoftvervezérelt farmok korában a biztonsági jellegű kihívások is az informatika területéről érkeznek.

Tekintsük át röviden az adatvezérelt precíziós mezőgazdaság biztonsági kihívásait [2]:
**Adatvédelem:** az adatokat azonosítással, hozzáférés szabályozásával kell védeni

- **Integritás**: az adatátvitel és -tárolás során nem sérülhetnek az adtok
- **Titkosság:** az adatokhoz nem férhet hozzá illetéktelen személy
- **Elérhetőség:** a döntéshez, vezérléshez szükséges adatoknak mindig elérhetőnek kell lenni
- **Megbízhatóság:** a dedikált felhasználók tökéletes biztonságú azonosítása

Ezek a legfontosabb elvárások a precíziós gazdálkodás során használt eszközök és megoldások biztonsága érdekében. Hardver oldalról a valós veszély a fizikai eszközök megsemmisítése vagy ellopása. De ide sorolhatjuk még az átviteli jelek zavarását, eltérítését is. A hálózatot a máshol is tapasztalható biztonsági veszélyek fenyegetik: túlterheléses támadás, botok használata, felhő-rendszerek ellen végzett támadás stb. És végül magát az „adatot" is lehet támadni: az adatszivárgás, és a zsarolóvírusok jelentik a fő kockázati tényezőket. A szoftverek is külön veszélyforrást jelenthetnek: frissítésekor, adatcsere esetén illetéktelen kód kerülhet a rendszerbe.

Láthatjuk, hogy ezeknek a veszélyeknek a kezelése klasszikus informatikai, mérnöki megközelítést igényelnek, és a mezőgazdaság területén korábban nem szükséges kompetenciák meglétét teszik szükségessé a gazdálkodóknál.

Miért éri meg mégis a precíziós mezőgazdaságra való áttérés? A precíziós mezőgazdaság végtermék szempontjából számos előnyt nyújt. Nem pusztán a hatékonyságot lehet növelni az új, digitális módszerek segítségével. Az élelmiszer-biztonság, az élelmiszerminőség javításában, valamint a vegyszerhasználat csökkentésében is sikeresen alkalmazhatóak a precíziós mezőgazdaság megoldásai.

## TÉMA BEMUTATÁSA

### Az élelmezésbiztonság

Az élelmezésbiztonság tágan értelmezve az élelmiszertermelés mennyiségének növelését és a termelés stabilitását jelenti. De az, hogy mindig mindenki elegendő táplálékhoz jusson több tényező is befolyásolja: a családok jövedelmi helyzete, az időjárás, világjárványok vagy a politikai és biztonsági környezet [3]. Az élelmiszertermelés és az élelmiszer-elosztási rendszer komplexitása eredményezi, hogy az élelmiszertermelés szintjének növelése nem biztosítja az élelmiszer-stabilitást, és nem feltétlenül nyújtja a teljes lakosság számára az élelmiszer-biztonságot.

### A technológiai fejlődés hatása az élelmezésbiztonságra

A mezőgazdaság eddig szerencsére nem követte Malthus népesedési elméletét (Thomas Malthus, 1766–1834), mivel az általános élelmiszertermelés lépést tartott a világ népességének növekedésével. A gazdaságok gépesítése, az egyre jobb és hatékonyabb mezőgazdasági termelési technológiák terjedése a termelékenység növekedéséhez és a szükséges munkaerő csökkenéséhez vezetett. A növényvédő szerek az 1900-as évek közepén kezdtek el elterjedni, ami lehetővé tette a termés gyomoktól, rovaroktól és betegségektől való fokozott védelmét. Ugyanebben a korszakban zajlott a zöld forradalom is: genetikai alapú szelekció a modern gazdálkodási gyakorlatokkal és egyre jobb műtrágyákkal párosulva jelentősen növelte a termelékenységet [4].

### A precíziós mezőgazdaság szerepe

A termelékenység további növeléséért és a környezeti, energetikai terhelés további csökkentésére új módszerekre van szüksége az emberiségnek. Erre jelenthet megoldást a precíziós mezőgazdaság elterjedése.

Az adat alapú technológiák a termelés minden részterületén megjelennek. A genetikai szelekciótól, a farmok vezérlése, üzemeltetése, valamint a prediktív döntéshozatali technikák az elmúlt évtizedben megjelent új eszközök a mezőgazdaságban. A fejlődés nyilvánvaló az új technikákkal tovább nő a termelékenység, az erőforrások felhasználásának hatékonysága és nem utolsó sorban javul az élelmiszer- biztonság is.

Cikkünkben két esetet tanulmányozunk részletesebben. A két esetleírás különböző területről származik, és mindkettő a mesterséges intelligencia szerepét mutatja be az élelmiszer-biztonság javításában.

## MESTERSÉGES INTELLIGENCIÁVAL A JOBB TEJMINŐSÉGÉRT

### Tőgygyulladás (mastitis) előrejelzése tejmintából

A tej szomatikus sejtjei (SCC) tejtermelő sejtek és immunsejtek keverékét jelentik. Ezek a sejtek a fejés során kiválasztódnak a tejbe, és az emlő egészségének és a tej minőségének becslésére szolgáló indexként használhatóak [5]. Az SCC index fő szerepe a fertőzések elleni küzdelem és a szöveti károsodások helyreállítása. Minden fejlett országban a tej szomatikus sejtszámát (SCC) használják markerként a tejelő állományokban a tőgygyulladás gyakoriságának nyomon követésére.

Az SCC mennyiségére 100ml tejben az alábbi határértékeket adják meg:

- A 100 000 vagy annál kisebb SCC érték jelzi a „nem fertőzött" tehenet,
- a 200 000-es SCC azt jelzi, hogy a tehén nagy valószínűséggel fertőzött tőgygyulladással,
- míg a 300 000 vagy annál nagyobb SCC jelentős mennyiségű kórokozóval fertőzött tehenet jelent.

A szomatikus sejtszám szórása meglehetősen nagy, ezért a szakirodalomban általában az úgynevezett linearizált szomatikus sejtszámot használják (Dégen, Monostori). A logaritmikus szomatikus sejtszám (LogSCC) a szomatikus sejtszám transzformált mérése, amely a számot logaritmikus skálán fejezi ki. A LogSCC-t úgy számítják ki, hogy a szomatikus sejtszám logaritmusát veszik, majd megszorozzák 100-zal. Például egy 400 000 sejt/ml szomatikus sejtszám esetén a LogSCC 5,6 lenne. A LogSCC-t eszközként használják a szomatikus sejtszám szintjének összehasonlítására különböző tejminták, állományok vagy régiók között. A szomatikus sejtszám kifejezésére szolgáló módszer azért hasznos, mert felnagyítja a minták közötti különbségeket, és pontosabb statisztikai elemzést tesz lehetővé. A LogSCC-t a szomatikus sejtszám-csökkentő programok hatékonyságának értékelésére is használják a tejelő állományokba [5].

A szomatikus sejtszám becslésére, előrejelzésére számos matematikai, statisztikai megoldás létezik. Egyetemünkön egy olyan gépi tanuláson alapuló algoritmus kifejlesztésén dolgozunk, amely képes a szomatikus sejtek számának előrejelzésére a laboratóriumokban mért egyéb tejparaméterek alapján.

A logaritmikus SCC-t nem az eredeti 9, hanem 3 csoportra osztottuk. Mivel 3 csoport elegendő a mindennapi osztályozáshoz (nem fertőzött = 0; lehetséges fertőzés = 1, fertőzött = 2), a lineáris pontszámokból 3 SCC-kategóriát hoztunk létre.

Az adattisztításhoz először töröltük az összes nulla értéket és minden olyan rekordot, ahol hiányzó értéket találtunk. A szoftver Python programozási nyelven készült a Pandas és sickit-learn támogatásával. Nem volt szükség normalizálásra, mivel fa-alapú modelleket használtuk, amelyek sokkal robosztusabbak a kiugró értékekkel szemben, mint a lineáris modellek. A fa-alpú – amelyek jól használhatóak többosztályos osztályozásra – modell használatát az tette lehetővé, hogy a kimeneti változónk (linearizált SCC) 3 kategóriára volt osztva. Több, mint 15 kombinációt futtattunk a legjobb bementi paraméterek kiválasztásához.

Eredményünket az alábbi táblázatban közöljük:

| ML | LSCC=0 | LSCC=1 | LSCC=2 | átlag |
|---|---|---|---|---|
| **Extra Trees Classifier** | 0.89 | 0.88 | 0.86 | 0.88 |

*1. Táblázat: A szomatikus sejtszámbecslés eredménye*

További adatokra szükség van, de az előzetes eredmények alapján látható, hogy tudunk olyan algoritmust készíteni, ami akár 1–2 héttel előre jelezni tudja az SCC növekedését a tejben. Ezzel a fertőzésgyanús állat kiemelhető a többiek közül, kezelése időben

megkezdhető. Így kevesebb gyógyszer felhasználásával, biztonságosabb termelést és jobb tejminőséget tudunk biztosítani. Tehát ez a módszer, a meglévő adatok felhasználásával, a mesterséges intelligencia segítségével tovább növeli az élelmiszer-biztonságot, és könnyen a napi rutin részévé válhat.

## VERTIKÁLIS FARMOK SZEREPE AZ ÉLELMISZERBIZTONSÁGBAN

A föld népessége növekvő ütemben emelkedik, és egyes előrejelzések szerint 2030-ra eléri a 8,5 milliárdot (UNNS, 2015). Az Egészségügyi Világszervezet (WHO, 2018) szerint az élelmiszertermelést 70%-kal kell növelni ahhoz, hogy 2050-re mintegy 10 milliárd ember élelmiszerigényét kielégítsük, amelyből körülbelül 6,5 milliárdan városi területeken fognak élni.

Ezért egyre nagyobb figyelem és érdeklődés kíséri a zárt növénytermesztési rendszereket, mivel itt alkalmazzák legrégebben precíziós technológiákat. A zárt növénytermesztési rendszerek, olyan modern mezőgazdasági megoldások, amelyekben a növényeket zárt térben, kontrollált körülmények között termesztik. Ezek az innovatív megoldások lehetővé teszik a termesztési folyamatok teljes ellenőrzését, amely nagyobb hatékonyságot, nagyobb terméshozamot és jobb minőséget eredményez.

A környezeti tényezőket, mint például a hőmérsékletet, a páratartalmat, a $CO_2$-koncentrációt, az öntözést és a megvilágítást úgy szabályozzák, hogy a növények optimális körülmények között fejlődjenek. A rendszerben működő érzékelők és automatizált vezérlők segítségével a növények pontosan azon a szinten kapnak tápanyagot és vizet, amelyek a legmegfelelőbbek a fejlődésük szempontjából.

A zárt növénytermesztési rendszerek lehetővé teszik a gazdálkodók számára, hogy élelmiszereket termeljenek olyan területeken, amelyek korábban nem voltak alkalmasak a termesztésre, például városi területeken vagy sivatagos területeken. A zárt növénytermesztési rendszerek az élelmiszer-biztonságot is növelik, mivel a termesztési folyamatok teljes mértékben ellenőrzöttek és biztonságosak.

Előnyei közé tartozik az éves termesztési ciklusok növelése: ez a zárt technológia lehetővé teszi a termelést az egész évben, a termesztési ciklusok rövidülnek, a hozam nő, valamint a víz és a műtrágya hatékonyan és biztonságosan van felhasználva. Az ilyen rendszerek a környezetbarát mezőgazdasági megoldások közé tartoznak, mivel a vízfogyasztás és a műtrágyahasználat a termesztett növények igényeihez igazodik, és így kevesebb hulladékot termelnek.

A zárt növénytermesztési rendszerek egyre népszerűbbek a világban, és az iparág egyre fejlettebbé válik az új technológiák és megoldások bevezetésével. Ezek a rendszerek nem csak a mezőgazdaságban jelentenek új lehetőségeket, hanem az élelmiszeripar egészében is új megközelítéseket, szemléletet hoznak.

*1. Ábra: Zárt növénytermesztési rendszer,*
Forrás: https://vtx.vt.edu/articles/2019/02/ext-innovgreenhousefarming.html

## Vertikális farm

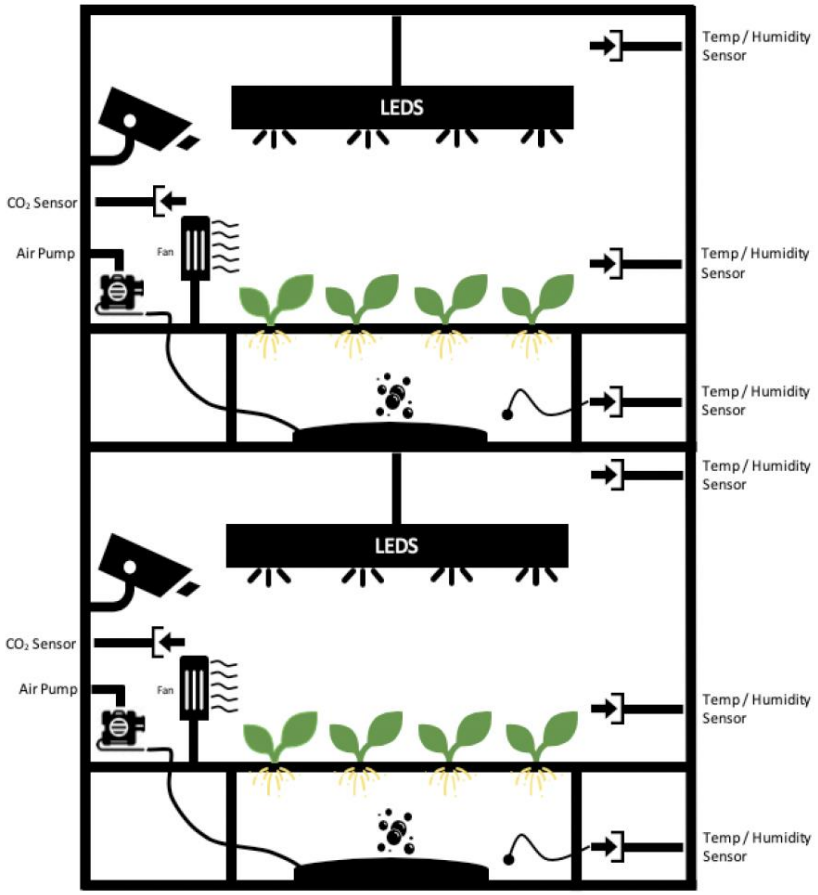
A városi mezőgazdaság (UA) területén egy viszonylag új koncepció, a vertikális gazdálkodás (VF) jelent meg. Ez is egy zárt növénytermesztési rendszer, csak itt a növények több emeleten (polcon) speciális táptalajon vagy oldatban növekednek. Ezzel a módszerrel egész évben egyenletes minőségű és növényvédőszer-mentes, tápláló élelmiszereket állíthatunk elő akár városi környezetben is. A VF a beltéri hidroponikus növénytermesztés gyakorlatát jelenti függőlegesen egymásra helyezett rétegekben vagy ferde felületeken. A zárt növénytermesztési rendszerek számos előnnyel rendelkeznek:

- **Térkihasználás**: A zárt növénytermesztési rendszerek és különösen a vertikális farmok hatékonyan használják ki a rendelkezésre álló területet. A vertikális farmok lehetővé teszik a növénytermesztést több emeleten, ezzel jelentősen növelve az egységnyi felületre jutó termesztési kapacitást.
- **Környezeti tényezők**: A zárt rendszerek lehetővé teszik a környezeti tényezők, mint például a hőmérséklet, a páratartalom, a $CO_2$-koncentráció, a vízellátás és a megvilágítás szabályozását.
- **Energiafelhasználás**: A vertikális farmok energiaigénye is kedvezően alakul, mivel a növényeket több emeleten termesztik, és így a megvilágítás, hűtés és fűtés stb. működtetéséhez szükséges energia több növény számára biztosítható.
- **Tápanyag és vízfelhasználás**: Hatékonyan használják fel a tápanyagokat és a vizet a növények optimális fejlődése érdekében. A vertikális farmokban a növények azonos vagy hasonló mennyiségű tápanyagot és vizet kapnak, függetlenül attól, hogy melyik szinten helyezkednek el.

- **Költségek**: A zárt termesztési rendszerek általában magasabb termelési költségekkel járnak, mint a hagyományos mezőgazdasági termelés. A vertikális farmok magasabb beruházási költségeket igényelnek, mivel több épületet kell felépíteni, és a rendszer működtetésének nagyobb az energiaigénye. A vertikális farmok esetében kizárólag mesterséges megvilágítást alkalmaznak.
- **Élelmiszer-biztonság**: A teljesen kontrollált környezet miatt minimálisra csökkenthető a kártevők okozta fertőzések veszélye. A szándékos mérgezés vagy idegenek behatolása is kizárható a zárt rendszerű termesztési megoldások esetén. Ezért az élelmiszer-biztonság területén is a zártrendszerű technikák felelnek meg a legjobban a modern kor kihívásainak.

*2. Ábra: Vertikális farm Szingapúrban,*
*Forrás: https://en.wikipedia.org/wiki/Vertical_farming#/media/File:Sgverticalfarming1.png*

Egy zárt, vertikális farm LED-fényekkel és a felügyelethez szükséges különböző IoT-eszközökkel kerül kialakításra. A rendszer irányítását egy képfeldolgozó algoritmus végzi. A mikrométerű vertikális gazdálkodás koncepcióját a következő 3. ábra szemlélteti.




*3. ábra Mikroméretű vertikális gazdálkodás koncepciója [7]*

Kísérleti vertikális farm üzemel a MATE gödöllői campusában. A VF szabályozott klimatikus körülmények között 12 sávos LED-es megvilágítási technikával, IoT eszközökkel, kamerákkal, automatikusan végzi az adatgyűjtést, a kamerák és IoT szenzorok adatai alapján gépi tanulással adatalapú modellt állítunk fel az energiafelhasználás minimalizálására, a zöldtömeg maximalizálása mellett.

Kutatási célunk olyan mesterséges intelligencia alapú vezérlő rendszerek kialakítása, amely nem csak a vegyszer használatot minimalizálja (és ezáltal az élelmiszer minőséget növeli) hanem a termesztési költségeket is optimalizálja egyszerre. A mesterséges intelligencia alapú vezérlési programok kidolgozásával tovább növelhető a vertikális farmok termelékenysége és csökkenthető az energiafelhasználása.

## ÖSSZEFOGLALÁS

A precíziós mezőgazdaság a technológiák és az elvek alkalmazása a mezőgazdasági termelés térbeli és időbeli változékonyságának kezelésére, a termés és a környezeti hatások minőségének javítása érdekében [8].

A precíziós gazdálkodás egy olyan modern mezőgazdasági megközelítés, amely lehetővé teszi a gazdálkodók számára, hogy pontosan meghatározzák a termesztési folyamatok minden lépését. Ennek érdekében adatgyűjtést végeznek, és érzékelőket használnak a mezőgazdasági területeken, hogy mérjék az időjárási körülményeket, a talajminőséget, a növények egészségét és más fontos paramétereket.

A gyűjtött és feldolgozott adatok lehetővé teszik a gazdálkodók számára, hogy optimalizálják a farmjaik működést és maximalizálják a hozamot, minimális erőforrás felhasználás mellett.

A technológia további fejlődésével a precíziós gazdálkodás sem kerülheti el a nagy adatbázisok (Big Data) kezelését, használatát [9]. Napjainkban már annyi adat áll rendelkezésünkre, amelyeket hagyományos adatfeldolgozási módszerekkel nem is lehet érdemben feldolgozni. Az adatok feldolgozásában pedig elkerülhetetlen a mesterséges intelligencia (MI) használata. Az MI technológia használatával a nagy adathalmazokban olyan mintákat is észre tudunk venni, amit a hagyományos adatkezelési módszerekkel nem tudtunk volna.

A precíziós technikák megjelenése az ehhez kapcsolódó eszközök, hálózatok és szoftverek alkalmazása a hagyományos mezőgazdasági technológiákban újfajta biztonságtechnikai kihívásokat jelentenek a gazdálkodóknak. A precíziós farmok biztonsági megoldásainál bátran támaszkodhatunk a digitális technikát régebb óta használó iparágak esetében már jól bevált megoldásokra. Bár az új technológia, új veszélyeket is rejt magában, az előnyei messze felül múlják a megjelenő új kockázati tényezőket. A historikus adatokra támaszkodó adatalapú predikciós, vagy vezérlő algoritmusok – melyre két példát is bemutattunk – jól illusztrálják a gépi tanulásban az élelmiszeripar számára rejlő komoly lehetőségeket.

## FELHASZNÁLT IRODALOM


[1] Blackmore, B.S., Wheeler, P.N., Morris, J., Morris, R.M. and Jones, R.J.A. (1995). The Role of Precision Farming in Sustainable Agriculture: A European Perspective. In Site-Specific Management for Agricultural Systems (eds P.C. Robert, R.H. Rust and W.E. Larson). https://doi.org/10.2134/1995.site-specificmanagement.c60

[2] Jensen, K.K., Sandøe, P. Food Safety and Ethics: The Interplay between Science and Values. *Journal of Agricultural and Environmental Ethics* **15**, 245–253 (2002). https://doi.org/10.1023/A:1015726423707

[3] R. E. Evenson, D. Gollin, Assessing the Impact of the Green Revolution, 1960 to 2000.*Science***300**,758-762(2003).DOI:10.1126/science.1078710

[4] C. Burvenich, et al.: Physiological and Genetic Factors That Influence the Cows Resistance to Mastitis, Especially during Early Lactation, Proceedings of the 5th IDF Mastitis Congress, Symposium on Immunology of Ruminant Mammary Gland (2000).

[5] S. Dabdoub, G. Shook: Phenotypic relations among milk yield, somatic cell count and clinical mastitis, Journal of Dairy Science 67.1 (1984), pp. 163–164

[6] De Oliveira, F. J., Ferson, S., & Dyer, R. (2021). A Collaborative Decision Support System Framework for Vertical Farming Business Developments. International Journal of Decision Support System Technology (IJDSST), 13(1), 34-66. http://doi.org/10.4018/IJDSST.2021010103

[7] Siropyan, M.; Celikel, O.; Pinarer, O. (2022). "Artificial Intelligence Driven Vertical Farming Management System". *Proceedings of the World Congress on Engineering 2022*, WCE 2022, July 6 - 8, 2022, London, U.K.
[8] Pierce F.J., Nowak P.: Aspects of precision agriculture (1999), pp. 1-85 Advances in Agronomy, Academic Press, Volume 67
[9] Wolfert, S.; Ge, L.; Verdouw, C.; Bogaardt, M.-J. Big data in smart farming—A review. Agric. Syst. 2017, 153, 69–80.

# WORK DIAGNOSTIC MEASURING INSTRUMENTS IN CAREER GUIDANCE AND OCCUPATIONAL REHABILITATION

# MUNKADIAGNOSZTIKAI MŰSZERES VIZSGÁLATOK A PÁLYAVÁLASZTÁSBAN ÉS A FOGLALKOZÁSI REHABILITÁCIÓBAN

NAGY Sarolta[1] – JÓKAi Erika[2]

**Abstract**

We have previously examined the usefulness of instrumental measures of ability in work of Occupational Health The work of Occupational Safety and Occupational Health professionals, in context of job-worker matching, occupational rehabilitation and career counselling (for people starting or changing career), is greatly assisted by instrumental ability tests. In career counselling, the Piarist Lookout Centre uses instrumental skills tests for young people from disadvantaged backgrounds, who come to them. We present the follow-up of our studies carried out in 2018-2019 at the request of the Piarist Outlook Centre and present a case study on the place of instrumental skills tests in occupational rehabilitation

**Keywords**

work diagnostics, career guidance, occupational rehabilitation, work simulator, disabled person

**Absztrakt**

Korábban vizsgáltuk a műszeres képességmérések hasznosságát a foglalkozás-egészségügyi munka során. A munkavédelemben és a foglalkozás-egészségügyben dolgozó szakembereknek a munkáját, a munkakör-munkavállaló illesztés, a foglalkozási rehabilitáció és a pályaválasztási tanácsadás (pályakezdő, vagy pályát módosító személy esetében) során jelentősen segítik a műszeres képességvizsgálatok. Pályaválasztási tanácsadás során a Piarista Kilátó Központ munkadiagnosztikai méréseket használ, a hozzájuk forduló hátrányos helyzetű fiataloknál. A Piarista Kilátó Központ felkérésére 2018-2019-ban végzett vizsgálataink utókövetését ismertetjük és esettanulmányon keresztül az eszközös munkadiagnosztikai vizsgálatok helyét a foglalkozási rehabilitációban.

**Kulcsszavak**

munkadiagnosztika, pályaválasztás, foglalkozási rehabilitáció, munkaszimulátor, fogyatékos személy

[1] nagy.sarolta@nnk.gov.hu ; szakellatotudomany@gmail.com| ORCID: 0000-0002-8560-1002 |PhD Student, Óbuda University Doctoral School on Safety and Security Sciences | occupational health specialist, National Public Health Center Occupational Health Department | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola | foglalkozás-egészségügyi szakorvos, Nemzeti Népegészségügyi és Gyógyszerészeti Központ

[2] jokai.erika@bgk.uni-obuda.hu|ORCID: 0000-0001-5867-5041| assistant professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering| egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## BEVEZETÉS

A fogyatékos személyek sikeres nyílt-munkaerő piacon való foglalkoztatásának az egyik feltétele a munkakör-munkavállaló megfelelő illesztése, azaz a munkakör ellátáshoz szükséges képességek és a munkavállaló funkcióképességének illesztése. A munkakör-munkavállaló illesztés és a foglalkozási rehabilitációs eljárás a munkavédelem és a foglalkozás-egészségügy szakembereinek feladata. A foglalkozás-egészségügyi szakorvos az orvosi alkalmassági vizsgálat alapján ad javaslatot, hogy milyen korlátozások figyelembevételével kell kiválasztani az új munkakört a munkavállaló részére. A foglalkozás-egészségügyben dolgozó szakemberek támogatják olyan módszerek bevezetését, melyeknek köszönhetően objektív adatokon alapul a döntés az alkalmasságról, a korlátozásokról a foglalkoztatás során, ilyen módszerek a műszeres képességvizsgálatok. A foglalkozás-egészségügy munkája során a műszeres vizsgálatok rendszeres igénybevételének köszönhetően, a fogyatékos személyek munkába állása zökkenőmentes lesz és tartósan tudnak az adott munkakörben dolgozni. Gyakran kerül sor foglalkozási rehabilitációs eljárásra a megváltozott munkaképességű személyek, ezen belül a fogyatékos személyek esetében, melynek célja, hogy az egészségi elváltozás miatt eredeti munkakörére, az eredeti munkakörülmények között alkalmatlanná vált munkavállalót másik munkakörben, az eredeti munkáltatójánál tudják tovább foglalkoztatni. A foglalkozási rehabilitáció és munkakör-munkavállaló illesztés folyamatát hatékonyan segíthetik a munkadiagnosztikai műszeres mérések objektív adatai. [1]. A hatékony munkavégzés és a ritka pályaelhagyás egyik kulcsa a megfelelő szakmai képzettség megléte. A fogyatékos személyek az ép populációhoz képest alacsonyabb iskolai végzettséggel rendelkeznek, nagyobb százalékuk rendelkezik csak általános iskola 8 osztállyal, illetve be nem fejezett 8 osztállyal. [2]

Az olyan munkadiagnosztikai eszközöket, mint a hordozható munkapszichológiai képességvizsgáló műszereket és munkaszimulátorokat régóta használják nagy figyelmet igénylő, fokozott baleseti veszéllyel járó munkakörök esetében (atomerőmű, tömegközlekedés, légi közlekedés dolgozói) és a klinikai rehabilitáció során. A foglalkozási rehabilitáció és pályaválasztás folyamatában eddig még csak nagyon ritkán került sor a használatukra.

2018. január 31-én alakult meg a ferences és a piarista rend együttműködésében és 2020 tavaszán költözött be Váci ferences kolostor felújított épületébe a Kilátó Piarista Pályaorientációs és Munkaerőpiaci Fejlesztő, Módszertani Központ (Piarista Kilátó Központ). Egyik fő feladatuk az életpálya tanácsadás, mely során térítésmentesen végzik hátrányos helyzetű fiatalok részére a pályaválasztási és munkaerőpiaci kérdésekben az egyéni tanácsadást, munkadiagnosztikai mérőeszközöket is használva. Nem találtunk más intézményt, mely rendszeresített munkadiagnosztikai mérőeszközöket használna a pályaválasztási tanácsadás során. [3] A Kormány fővárosi és a vármegyei kormányhivatalokat jelölte ki rehabilitációs hatóságnak, akiknek rendelkezésükre áll számos munkadiagnosztikai eszköz között ErgoScope munkaszimulátor is, a komplex minősítés és a foglalkozási rehabilitáció elősegítésére.

## MÓDSZER ÉS IRODALMI HÁTTÉR

A Piarista Kilátó Központ fő profilja, mely már létrehozásának alapját is képezte, az „Élet-pálya tanácsadás”. A tanácsadási folyamat részét képezik a pályaorientációs, önis-

mereti kérdőíves felmérések, pszichológiai és gyógypedagógiai felmérések, illetve fejlesztések mellett a munkadiagnosztikai műszeres vizsgálatok is. A munkadiagnosztikai vizsgálatokat a Piarista Kilátó Központ saját ErgoScope munkaszimulátorán és hordozható munkapszichológiai képességmérő műszerein végzik. A munkadiagnosztikai vizsgálatok módszertanát 2018-2019-ben a Kilátó Projekt szakaszában készítettük el, táblázatok formájában, melyeken megtalálható az eszközökkel mérhető összes képesség és 30 szakma esetében a szakmákhoz szükséges kompetenciák, illetve ezen szakmák esetében a protokoll javaslat a munkadiagnosztikai mérésekre, részmérésekre. [1] [4] [5] [6] [7] A kidolgozott mérési módszertant nem csak az egyéni tanácsadásra jelentkező fiatalok esetében alkalmazzák, hanem szakiskolákban is végeznek rendszeres kompetenciamérést, utókövetést és munkadiagnosztikai méréseket is. 1991-ben Gödön megalapították a Piarista Szakképző Iskolát, ahol építőipari szakmát oktattak és 2019-ben elsőként vezették be a szakképzésbe az orientációs évfolyamot. Ezzel egy időben az iskola tanárai és diákjai részt vettek a Piarista Kilátó Központ módszertani munkáját megalapozó projektmunkában. Ebben a projekt szakaszban kezdtük el a gödi Piarista Szakképző iskola orientációs évfolyamára járó diákok vizsgálatát munkadiagnosztikai mérőeszközökkel. Kutatási projektünk másik részében különböző fogyatékossági csoportba tartozó fiatalokat is vizsgáltunk képességmérő műszerekkel és az ErgoScope munkaszimulátorral, annak érdekében, hogy felmérjük, vajon mindenki számára hozzáférhetővé válhatnak-e ezek a műszeres vizsgálatok. [5] [6] [7] A Piarista Kilátó Központ megbízásából elvégzett pilot vizsgálataink során, így a gödi Piarista Szakképző Iskolában is a magyar gyártmányú ErgoScope munkaszimulátort és a szintén magyar fejlesztésű stabilométert, Ricossay ujjügyesség vizsgálót, tachisztoszkópot, figyelemképesség-vizsgálót, tanulás és emlékezet vizsgálót, komplex szenzomotoros konfliktométert, Crawford munkapróbát használtuk.

2023 tavaszán interjút készítettünk a Gödi Piarista Szakképző Iskola orientációs csoportjának vezetőjével a 2019-ben általunk végzett műszeres képességvizsgálatokon részt vett diákok sorsáról, illetve az azóta a szakiskola orientációs tanéveibe járó diákok munkadiagnosztikai vizsgálatokkal történt felméréséről és az iskola tanárai által szerzett tapasztalatokról. A szakképző iskola pedagógusainak a műszeres képességvizsgálatok pályaválasztással kapcsolatos tapasztalatait ismertetjük cikkünkben.

Pályaválasztási tanácsadást leggyakrabban az általános iskola 7. és 8. osztályos tanulóinál végeznek. Viszont szükség lehet pályaválasztási tanácsadásra a szakképző iskolák orientációs tanévében, és fogyatékos személyek, illetve hosszú, vagy súlyos betegség után a munkába visszatérő személyek esetében is. A pályaválasztási tanácsadás akkor a legsikeresebb, ha egy olyan munkacsoport végzi, amelynek tagja pszichológus, munkapszichológus, gyógypedagógus, foglalkozás-egészségügyi szakorvos, és ez a munkacsoport papírceruza tesztek mellett műszeres munkadiagnosztikai eszközökkel képességmérést is végez. Jelenleg az általános iskolások részére az iskolaorvosok és a Nemzeti Népegészségügyi és Gyógyszerészeti Központ (továbbiakban NNGYK) Munkahigiénés és Foglalkozás-egészségügyi Főosztálya végez, a fiatal felnőtteknek pedig Vácott a Piarista Kilátó Központ nyújt ilyen szolgáltatást.

A foglalkozási rehabilitáció része a komplex rehabilitációnak. A foglalkozási rehabilitáció során a betegség, baleset miatt a munkától hosszabb ideig távol lévő munkavállaló visszatérését segíti elő a klinikai gyógyulás után csapatmunkában, a foglalkozás-egészség-

ügyi alapellátás és szakellátás, a munkavédelem szakemberei, szükség esetén fejlesztő szakember. A munkába való visszatérés történhet a munkavállaló eredeti munkakörébe változatlan körülményekkel, vagy eredeti munkakörébe, de számára megfelelően adaptált munkakörnyezetbe, munkaeszközökkel, illetve az eredetitől eltérő, de képességeinek megfelelő munkakörbe. Gyakran szükség lehet átképzésre, pályamódosításra is. [8] A munkába visszatérő, új munkát vállaló és a munkaügyi központokban jelentkező álláskereső személyek részére kötelező a munkaköri, illetve szakmai orvosi alkalmassági vizsgálat elvégzése. [9] Kutatási tapasztalataink alapján úgy véljük, hatékonyabb és eredményesebb szolgáltatást nyújthatna a műszeres képességmérő eszközöket felhasználó foglalkozás-egészségügyi alapellátás, illetve szakellátás. A foglalkozás-egészségügyi szakorvos a munkaköri orvosi alkalmassági vizsgálat során fel tudja mérni, hogy szükséges-e munkadiagnosztikai mérést végezni a munkavállaló meglévő képességeinek objektív megítélése céljából és a munkavállaló egészségi állapota alapján tud dönteni, hogy elvégezhetőek-e a műszeres képességvizsgálatok (pl. fizikai terhelés az ErgoScope 0. és 2. paneljén szívbetegség esetén). A műszeres képességvizsgálatok után a mérési eredmények birtokában lehet dönteni a munkaköri, illetve szakmai alkalmasságról, illetve pontosítani lehet a korlátozásokat. Továbbá a munkakör adaptálásához is hasznos részletekkel szolgálnak a képességmérések eredményei. Foglalkozási rehabilitációs intézkedés keretében a bizottság (munkáltatóval szerződött foglalkozás-egészségügy alapellátás szakorvosa, munkavédelmi szakembere és a munkáltató képviselője) célja, hogy amennyiben lehetséges, az érintett munkavállalót cégen belül foglalkoztassák tovább. A rendszeresen (évente) elvégzett munkadiagnosztikai felmérések a munkavállaló egészségi állapotának objektív követését teszik lehetővé a szakemberek számára, valamint a munkavállalók egészségvédelme érdekében, betegségek kialakulásának megelőzésében válnak a munkáltatók és munkavállalók hasznára

Az iskolaorvosoknak és néhány nagy vállalat foglalkozás-egészségügyi alapszolgálatát kivéve a foglalkozás-egészségi szolgálatoknak jelenleg nincs lehetőségük munkadiagnosztikai mérésre küldeni a pácienseket.

A műszeres képességmérések jelentőségét a foglalkozási rehabilitációs eljárásban, az NNGYK Foglalkozás-egészségügyi Szakellátó Helyén elvégzett munkaköri orvosi alkalmassági vizsgálatok közül kiválasztott két példán keresztül mutatjuk be a cikkünkben.

## EREDMÉNYEK

### Munkadiagnosztikai mérések pályaválasztási tanácsadás során

A 2023 tavaszán a gödi Piarista Szakképző Iskola orientációs csoportvezetőjével készített interjúból kiderült, hogy a 2019-ben általunk elkezdett műszeres képességméréseket 2023-ig minden tanulónál elvégezték. A szakképzést előkészítő orientációs évfolyam diákjainál munkadiagnosztikai eszközökkel és kérdőívekkel is elvégzik a kompetenciák bemeneti mérését. (1. ábra) A kérdőíves méréseket az orientációs év után minden év szeptemberében és a tanév végén is elvégzik. Az orientációs évfolyam legfontosabb feladatai az egyéni kompetenciákat figyelembe vevő felzárkóztatás, és a képzési lehetőségek megismertetése a diákokkal, szakmaválasztás céljából. A szakképző iskolában 4 szakmát oktattak: asztalos, ács-állványozó, szerkezetlakatos és karosszérialakatos. Az iskola életében az idei volt az utolsó tanév, 2023 nyarán végleg bezárt az iskola.

*1.Ábra: ErgoScope munkaszimulátoron végzett vizsgálat a gödi Piarista Szakképző Iskola és Kollégium szakképzést előkészítő orientációs évfolyam diákjánál. Kép forrása: Munkadiagnosztikai mérésekkel a sikeres szakmaválasztásért – Piarista Kilátó Központ l*

Az orientációs évfolyamon végzett munkadiagnosztikai mérések célja a tanulók tanulási, személyes, szociális, szakmagyakorlási, kompetenciáik felmérése, a gyengébb képességek fejlesztése a tanév során. A szakmákhoz elvárt képességek elmaradása az átlagtól, mint kizáró, korlátozó tényező szerepel a szakmai orvosi alkalmasság elbírálása során. Így a munkadiagnosztikai mérések a szakma elsajátítására való alkalmasság megítélésében is jelentős szerepet töltenek be.

Az ErgoScope munkaszimulátorral és a hordozható munkapszichológiai képességmérő eszközökkel végzett méréseken a gödi Piarista Szakképző Iskola diákjai mindig szívesen vettek részt, komolyan vették a vizsgálatokat. Egyszer-egyszer versenyhelyzet is kialakult, főleg a stabilométer (egyensúlyvizsgáló) használatakor. Voltak kimagasló egyensúlyérzékkel bíró diákok, illetve egy fő esetében az átlagtól jelentősen gyengébb vizsgálati eredménye alapján a testnevelő tanárral egyeztettünk a mozgásfejlesztésével kapcsolatban és a tanév végén a szakmaválasztáskor megfontolásra javasoltuk az ács-állványozó szakma tanulását.

Négy tanév orientációs évfolyamán végzett műszeres munkadiagnosztikai vizsgálatok adatai:

- 2019/2020. tanév: 48 gyereket vettek fel, 3 gyerek ment el, mert nem voltak alkalmasak a tanított szakmákra, de tanulmányi eredményeik jók voltak, gimnáziumban folytatták a tanulmányaikat.
- 2020/2021. tanév: 48 gyereket vettek fel, 3 fő ment el, mert mégis más szakmát akartak tanulni (szépségipar, vendéglátás), 1 fő nem alkalmas a választott szakmára, hallássérülés miatt a szerkezetlakatos szakmát nem tanulhatta.
- 2021/2022. tanév: 48 gyereket vettek fel, 5 fő nem volt alkalmas egyik szakmára sem, 2 fő másik iskolába ment tovább tanulni inkább.
- 2022/2023. tanév: 13 gyereket vettek fel (a 2023. augusztusi iskola megszüntetés miatt) 1 fő megy át gimnáziumba, a többiek az itt tanított szakmák közül választanak, de másik szakképző intézményben folytatják tanulmányaikat.

Minden diák, aki az orientációs tanév után maradt a szakképző intézmény, a választott szakmát, amelyre alkalmasnak is bizonyult megtanulta és a szakképző iskolát befejezte.

A műszeres munkadiagnosztikai felméréseket az orientációs tanév elején és végén végezték el a szakemberek. Úgy véljük, hogy fontos lett volna a szakiskolai képzés során és végén kontroll, kimeneti méréseket elvégezni. Az ilyen módon rögzített adatsorok a diákok többéves fejlődését mutathatják ki és emellett a fejlesztésben résztvevő szakemberek munkáját objektív adatokkal támogathatják.

**Foglalkozási rehabilitációs esetbemutatások**

Az alábbiakban bemutatott két esetben véleményünk szerint fontos lett volna műszeres képességméréssel kiegészíteni a munkaköri alkalmassági vizsgálatokat annak érdekében, hogy a szakember objektív adatokra támaszkodhasson szakvéleményében.

- 1. eset

Fiatal nő jobb keze gyermekkorában, balesetben sérült és könyök fölött amputálták. Könyvesbolti eladóként, illetve könyvesbolt áruátvevő raktárában foglalkoztatnák a munkavállalót. A kérdés az volt, hogy mind a két munkakört elláthatja-e.

A műszeres munkadiagnosztikai vizsgálathoz első lépésben a munkakörök betöltéséhez elvárt képességeket és a vizsgálat során használható munkadiagnosztikai eszközöket határozzuk meg. Ezeket az 1. táblázatban mutatjuk be.

| ***Könyvesbolti eladó, áruátvevő raktáros*** | | | | | |
|---|---|---|---|---|---|
| **A munkakör ellátásához szükséges képességek** | | | A munkakör ellátáshoz szükséges képességek vizsgálatához **használható képességmérő eszközök, vizsgálatok.** | | **A leírt eset kapcsán, az elváltozás miatt fontos lett volna** |
| **kizáró,** | **korlátozó** | **tényezők** | **Műszer megnevezése** | **Feladat megnevezése** | |
| tartós állás, | | | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés, munkabírás | |
| járás | | | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés, munkabírás | |
| könnyű fizikai munka | | | ErgoScope 0. és 2. panel | Dinamikus emelés szék magasságra két kézzel<br>Összetett feladat: monotonitás tűrés, munkabírás | |

| ***Könyvesbolti eladó, áruátvevő raktáros*** | | | |
|---|---|---|---|
| kézi tehermozgatás 20 kg alatt | ErgoScope 0. és 2. panel | Dinamikus emelés szék magasságra két kézzel<br>Összetett feladat: munkabírás | Szükséges lett volna, megvizsgálni, hogy képes-e a kézianyagmozgatásra |
| karok, kezek használata (könyvek pakolása, rendszerezése) | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés | Az ErgoScope munkaszimulátotor a monotonítás tűrés feladat jól szimulálja a könyvesbolti aruátvevő munkakört. A Bogen-Lipmann kalitkával elvégzett vizsgálat alapján képes a kezek-karok használatát igénylő feladatok elvégzésére. |
| | Bogen-Lipmann kalitka | kéz-kar mozgás, szem-kéz koordináció, feladat/probléma megoldás | |
| ujjak használata (számítógép használata, kézzel írás) | ErgoScope 1. panel | Billentyűzet kezelés egy kézzel<br>ceruza használat egy kézzel | Valószínűleg képes kalviatúrán gépelni, de jó lett volna a gyorsaságot és pontosságot megmérni és összehasonlítani a két kezes standard értékekkel. |
| ujjakkal fogás (számla, fuvarlevél megfogása) | ErgoScope 1. panel | Kulcsfogás ujjal<br>Három pontos fogás ujjal | A standard orvosi vizsgálat során egyedül vette elő, tette el a dokumentumait, de fontos lett volna megmérni standardizált körülmények között, és összehasonlítani a referencia értékekkel. |
| jó közellátás | Csapody olvasótábla (orvosi vizsgálat) | | |

| *Könyvesbolti eladó, áruátvevő raktáros* | | | |
|---|---|---|---|
| kommunikáció | orvos és mérésvezető megfigyelése | | |
| figyelem | ErgoScope 1. és 2. panel | Billentyűzet kezelés egy kézzel ceruza használat egy kézzel Kapcsolók és a nyomógombok használata | |
| | Tachisztoszkóp | Teljes feladatsor | |

*1.Táblázat: Könyvesbolti eladó, áruátvételi raktáros munkakör betöltéséhez elvárt képességek és vizsgálatukra alkalmas munkadiagnosztikai eszközök (saját szerkesztés).*

Az alkalmassági vizsgálat során csak a Bogen-Lipmann szem-kéz koordinációt vizsgáló kalitkát volt lehetőségünk használni, melynél egyénre szabott, speciális feladatot adtunk (nem a műszerkönyvben leírt feladatsort) a munkavállalónak, annak érdekében, hogy megbizonyosodhassunk, hogy az amputált karjának csonkját biztonsággal tudja használni alátámasztásra, így kisebb súlyú csomagokat képes biztonsággal mozgatni. A vizsgálat során megfigyeltük a munkavállaló mozgását, feladatmegoldását. Feltételeztem, hogy használja az amputált karját alátámasztásra, amikor tárgyakat kell megfognia, a standard orvosi vizsgálat során megfigyeltem és dokumentumok, táska, kabát megfogásakor használta alátámasztásra a felkarcsonkot. A Bogen-Lipmann kalitkával elvégzett vizsgálat beigazolta, hogy a kezek, karok használatát igénylő feladatot jól végzi, ügyesen megoldja. Ezekből a vizsgálati eredményekből, csak kikövetkeztethettük, hogy kisebb terheket, ebben az esetben könyveket tud felemelni, cipelni. Javasoltuk a tovább foglalkoztatását, így maradhatott a könyvesboltban, munkáját el tudta látni. Nagy segítségünkre lett volna, ha az ErgoScope 1. paneljén a billentyűzetkezelést, a 2. panelen a monotóniatűrést tálcamozgatással vizsgálhattuk volna, ennek a feladatsornak az elvégzése jól szimulálja a könyvesbolti áruátvevő munkakört és mérhető lett volna az könnyű fizikai munka, kézi anyagmozgatás közbeni fáradás. Az ErgoScope munkaszimulátoron elvégzett vizsgálatok objektív adatokkal támasztották volna alá, hogy képes a kézi anyagmozgatást végezni a munkavállaló jobb alkar hiánnyal is és elég pontosan és gyorsan képes a számítógép klaviatúráján gépelni, mert a mért értékeket össze lehet vetni a referencia adatokkal.

- 2. eset

Középkorú nő sokízületi gyulladás betegségben szenved, minden ízülete érintett. Gerince folyamatosan fáj, gerinc és láb érintettsége miatt állni csak pár percet tud, járni tud, de néha megszédül, lépcsőn biztonsággal nem tud közlekedni, karok nagy mozgásai megtartottak, de a kéz kis ízületei deformáltak, fájdalmasak, erőtlenek, így fogni, szorítani, tárgyakat megtartani nem tud egyik kezében sem. Munkaköre laboratóriumi asszisztens, mely részben álló, részben ülő, esetenként kézi anyagmozgatással járó munka. Megrendeléstől

függően akár egész munkanapot állva kell töltenie, illetve precíz ujjmozgásokat, biztos fogást igénylő feladatot kell végeznie.

Műszeres munkadiagnosztikai vizsgálat esetén a munkakör betöltéséhez elvárt képességek és a vizsgálat során használható munkadiagnosztikai eszközök az 2. táblázatban találhatók.

| ***Laboratóriumi asszisztens*** | | | |
|---|---|---|---|
| **A munkakör ellátásához szükséges képességek** | A munkakör ellátáshoz szükséges képességek vizsgálatához **használható képességmérő eszközök, vizsgálatok.** | | **A leírt eset kapcsán, az elváltozás miatt fontos lett volna** |
| **kizáró, korlátozó tényezők** | **Műszer megnevezése** | **Feladat megnevezése** | |
| tartós állás, | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés, munkabírás | A munkaidő kis részében szükséges képesség, munkaszervezéssel rövidebb időszakokra megoldható (meg is oldották, amíg nem volt humán erőforrás hiány)<br>A beteg elmondása szerint cipekedni nem tud fájdalom és erőtlenség miatt, hosszan állni és járni nem tud, elsősorban szédülés miatt |
| járás | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés, munkabírás | |
| könnyű fizikai munka | ErgoScope 2. panel | Dinamikus emelés szék magasságra két kézzel | |
| kézi tehermozgatás 20 kg alatt | ErgoScope 0. és 2. panel | Dinamikus emelés szék magasságra két kézzel<br>Összetett feladat: monotonitás tűrés, munkabírás | |
| kényszertesttartásban munkavégzés: hajlás, állás | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés, munkabírás | |
| karok, kezek használata | ErgoScope 2. panel | Összetett feladat: monotonitás tűrés | A munkakör minden feladatához szükséges.<br>A munkavállaló elmondása szerint fájdalom miatt, időszakosan a karok |
| | Bogen-Lipmann kalitka | kéz-kar mozgás, szem-kéz koordináció, feladat/probléma megoldás | |

| *Laboratóriumi asszisztens* | | | |
|---|---|---|---|
| | | | nagymozgásai korlátozottak |
| ujjak használata (számítógép használata, laboreszközök biztos fogása) | ErgoScope 1. panel | Kulcsfogás ujjal<br>Hárompontos fogás ujjal<br>Billentyűzet kezelés egy kézzel, két kézzel | A felajánlott új munkakörhoz a billentyűzethasználat viszgálata szükséges csak. |
| ujjak, kezek pontos használata | Ricossay ujjügyesség vizsgáló | Mindegyikoszlop kirakása | Egyes részfeladatok ellátásához (pipettával mérés, nagyon kis tárgyak pontos fogása, áthelyezése) nélkülözhetetlen<br>A munkavállaló elmondása szerint gyakori kontraktúra miatt sokszor egy papír lapot nem tud megfogni. Az orvosi alkalmassági vizsgálat során többszöri próbálkozás után tudott csak tollal írni |
| | Crawford munkapróba | Teljes feladatsor | |
| szem-kéz koordináció | ErgoScope 2. panel | Forgatás domináns kézzel | |
| | Tanulás-emlékezet vizsgáló (labirintus) | Teljes feladatsor | |
| jó közellátás | orvosi vizsgálat | Csapody olvasótábla (orvosi vizsgálat) | |
| figyelem | ErgoScope 1. és 2. panel | Összetett feladat: monotonitás tűrés kapcsolók és nyomógombok használata | |
| | Tanulás-emlékezet vizsgáló (labirintus) | Teljes feladatsor | |
| | Tachisztoszkóp | Teljes feladatsor | |

*2.Táblázat:.Laboratóriumi asszisztens munkakör betöltéséhez elvárt képességek és vizsgálatukra alkalmas munkadiagnosztikai eszközök (saját szerkesztés).*

A rutin munkaköri orvosi alkalmassági vizsgálat alapján is javasolt a munkavállaló képernyős munkakörbe való áthelyezése, a munkakörváltást a közvetlen felettese támogatta, a munkáltatóval egyeztetve megvalósítható, de a munkavállaló nehezen fogadta el. A munkadiagnosztikai eszközökkel történő mérések segítettek volna a munkavállalót a helyzet megértésében, elfogadásában, a foglalkozás-egészségügyi szolgálat pedig pontosabban le tudta volna írni, hogy mely részfeladatokat tudja gyorsan, fáradás nélkül, elfogadható legalább közepes, de inkább jó teljesítménnyel elvégezni. A műszeres képességmérések nélkül is javasoltuk a munkavállaló képernyős munkakörbe való áthelyezését, de csak reméltük, hogy a kéz és kézujjak érintettsége nem akadályozza a gépelésben. Ezt a feltételezésünket erősítette volna meg a billentyűkezeléses feladatok elvégzése az ErgoScope munkaszimulátoron. Az eredmények kiértékelése és a munkavállalóval történő megbeszélés, hogy mennyire fárasztó számára a billentyűkezelés, milyen módon lehetne segíteni, (pl. kézfej, könyök megtámasztása) lehetőséget biztosított volna a személyes adaptációs lehetőségek feltárására és javaslattételre a munkáltató felé. A munkakörváltás megtörtént, a munkavállaló titkárságon dolgozik, képes a munkáját ellátni.

## ÖSSZEFOGLALÁS

Betegség, sérülés vagy fogyatékosság miatt hátrányos helyzetbe került pályakezdők, aktív munkavállalók esetében fontos a minél többfajta, objektív és szubjektív adatokat is szolgáltató vizsgálat lehetőségének biztosítása akár pályaválasztási tanácsadásról, akár foglalkozási rehabilitációról van szó. Javasolt vizsgálat a pszichológiai felmérés, tanácsadás, műszeres munkadiagnosztikai mérések; kötelező vizsgálat a foglalkozás-egészségügyi orvos által elvégzett szakmai, munkaköri orvosi alkalmassági vizsgálat.

A gödi Piarista Szakképző Iskolában a szakképzés megkezdése előtt, az orientációs évfolyam elején elvégezték a műszeres képességméréseket és pszichológiai teszteket a tanulóknál. Ennek köszönhetően az elindult négy orientációs évfolyam mindegyik tanulója, aki a műszeres képességvizsgálatok alapján alkalmasnak bizonyult a választott szakmára, be is fejezte az iskolát (illetve az iskola bezárás miatt másik iskolában, de a választott szakmát tanulja tovább). Kimeneti mérési adatok sajnos nem állnak rendelkezésünkre, de a bemeneti mérések eredményeire úgy tekinthetünk, hogy igazolták, alátámasztották a szakmai alkalmasságot.

A foglalkozási rehabilitáció két ismertetett példája bizonyította, hogy a munkadiagnosztikai vizsgálatoknak az orvosi alkalmassági vizsgálat részét kellene képezniük. Sikeres volt mind a két foglalkoztatás, azonban mind a munkáltató, mind a munkavállaló, valamint a vizsgálatban véleményt formáló orvos számára is objektív adatokat szolgáltatna a műszeres munkadiagnosztika és az abban felhasznált értékelési protokoll. A könyvesbolti eladó, áruátvevő munkakör esetében, ha nem is a legspecifikusabb képességvizsgálatot lehetett elvégezni, de megtörtént a műszeres képességvizsgálat, enélkül nehéz lett volna döntést hozni. A laboratóriumi asszisztens munkakör esetében az alkalmatlanság egyértelmű volt a munkakör minden feladatának és a munkakörnyezetnek pontos ismeretében. Az új munkakörre való alkalmasságot a munka kipróbálása támasztotta alá. Ebben az esetben meg volt az esély arra, hogy az új munkakört sem tudja ellátni a munkavállaló, biztosak csak a műszeres képességvizsgálatok elvégzése után lehettünk volna. Az ehhez hasonló esetekben a műszeres munkadiagnosztikai mérések alkalmazásával elkerülhető, hogy a munkavállalót

olyan munkakörbe és munkakörnyezetbe irányítsák, amely számára egészségügyi vagy baleseti kockázatot rejt vagy teljesítménykudarcot jelent.

A szakmaválasztás, munkakörváltás megtörténhet és megtörténik munkadiagnosztikai eszközös mérések nélkül is, de a műszeres mérések során kapott objektív eredmények segítik a foglalkozás-egészségügyi orvost a döntésben, a pályakezdő fiatal, vagy munkavállaló könnyebben dönt, könnyebben fogadja el a váltást, ha megtapasztalja képességeit egy-egy munkaszituációban és eredményeit teljesítménynormákhoz viszonyítva értékelheti. A műszeres képességvizsgálatok rávilágíthatnak eddig rejtve maradt kimagasló részképességekre, és a referencia adatok alátámaszthatnak, gyengébb funkciókat.

## KÖVETKEZTETÉS

A bemutatott alkalmazási példák alátámasztják törekvéseinket, hogy az ErgoScope munkaszimulátor és a hordozható munkapszichológiai képességmérő eszközök esetében folyamatosan bővíteni kell az sztenderd értékeket adó mérési adatbázist és folyamatosan fejleszteni kell, igény szerint kiegészíteni a módszertani útmutatókat, valamint minél előbb elérhetővé tenni legalább konzultációs lehetőséggel a foglalkozás-egészségügyi szolgálatok számára a műszeres képességmérést.

A pályaválasztási, pályamódosítási tanácsadás és a foglalkozási rehabilitáció folyamatába, illetve a foglalkozás-egészségügyi alap- és szakellátás feladatai közé könnyen beilleszthetők a munkadiagnosztikai vizsgálatok, a műszeres képességmérések objektív eredményeinek értékelése és az ezek alapján történő javaslattétel a munkaköri/szakmai alkalmasságról, foglalkoztatásról.

## FELHASZNÁLT IRODALOM

[1] S. Nagy, „Munkadiagnosztikai mérőeszközök és az FNO együttes használata a munkavédelemben (első lépések)”*Biztonságtudományi szemle,* vol. 4, no.4, 2022, pp. 145-154, 2022. Elérhető: Teljes szám - 2022. IV. évf. 4. szám megtekintése (uni-obuda.hu)

[2] 11.2011. évi Népszámlálás KSH, *Fogyatékossággal élők,* Budapest, 2014. Letöltve: https://www.ksh.hu/docs/hun/xftp/idoszaki/nepsz2011/nepsz_11_2011.pdf

[3] Piarista Kilátó Központ https://www.kilato.piarista.hu/szolgaltatasok/eletpalya-tanacsadas-2/

[4] E. Jókai, Sz. Smudla, A. Pálosi, *„Mérésvezetői instrukciók az ErgoScope munkaszimulátoros vizsgálatsorozat levezetéséhez”* 2018.

[5] S. Nagy, E. Jókai, „Pályaorientációs központ fejlesztése során végzett pilot vizsgálat munkadiagnosztikai méréseinek tapasztalatai és módszertana” In: *K. Németh, Tavaszi Szél 2019 Konferencia. Nemzetközi Multidiszciplináris Konferencia, Absztraktkötet,* Budapest, Doktoranduszok Országos Szövetsége (DOSZ), 2019, 742 p. pp. 454-454.

[6] E. Jókai, S. Nagy, „The raison d’etre of work diagnostic tests in the work safety of disabled employees”, *Biztonságtudományi szemle* vol. 2, no. 1. Különszám, pp. 15-23, 2020. Elérhető: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/89/85

[7] E. Jókai, „Munkaszimulátorok alkalmazása sérülékeny munkavállalók munkahelyi biztonsága és egészségvédelme érdekében” *Bánki Közlemények* vol.2. no. 2. pp.46-52, 2019. Elérhető: http://bk.bgk.uni-obuda.hu/index.php/BK/article/view/102/72
[8] A. Horváth, G. Stierné szenes, J. Szellő szerk. „Bevezetés a komplex rehabilitációba” ELTE Bárczi Gusztáv Gyógypedagógiai kar, Budapest, 2009.
[9] 33/1998 (VI.24.) NM rendelet, Elérhető: https://njt.hu/jogszabaly/1998-33-20-3D

# NOISE EXPOSURE DETERMINATION AND PERSONAL PROTECTIVE EQUIPMENT ALLOCATION FOR MAINTENANCE STAFF WITH SNR AND OCTAVE BAND METHOD

# MUNKAHELYI ZAJEXPOZÍCIÓ MEGHATÁROZÁSA ÉS EGYÉNI VÉDŐESZKÖZ JUTTATÁS KARBANTARTÓ MUNKAKÖRBEN SNR ÉS OKTÁVSÁV MÓDSZERREL[1]

ZAKARIÁS Rebeka[2]

**Abstract**

In my current position, I am responsible for occupational safety. According to my daily experience, managing health risks related to workplace noise is a challenge for both the employer, and the employees. I often encounter the problem that workers are provided with personal hearing protection devices that are not justified. The management of workplace noise protection risks is my passion, so the aim of my thesis was to determine the workplace noise exposure within the examined workplace's employees working in the maintenance workshop. Furthermore, during the risk assessment I reviewed the necessity and adequacy of the provided, individual hearing protection device. In the case of possible inappropriateness, the recommendation of suitable individual hearing protection devices according to the SNR and octave band methods.

**Keywords**

Noise exposure determination, risk assessment, personal protective aquipment allocation, SNR and Octave band method

**Absztrakt**

Mindennapi tapasztalatom, hogy a munkahelyi zajjal kapcsolatos egészségügyi kockázatok kezelése kihívást jelent a munkáltató és a munkavállaló részére is. Gyakran találkozom azon problémával, hogy a dolgozók számára olyan egyéni hallásvédő eszközök vannak szolgáltatva, amelyek alkalmazása nem indokolt. Ezen érvek alapján publikációmban beszeretném mutatni egy az általam vizsgált ipari létesítmény Karbantartó műhelyében különböző munkakörben dolgozó munkavállalókat érő munkahelyi zajexpozíció meghatározását, kockázatértékelés során felülvizsgálni a számukra szolgáltatott egyéni hallásvédőeszköz szükségességét, valamint nem megfelelőségét. Esetleges nem megfelelőség esetén a megfelelő egyéni hallásvédő eszközök kiválasztása az SNR és oktávsáv módszerek szerint.

**Kulcsszavak**

munkahelyi zajexpozíció meghatározása, kockázatértékelés, egyéni védőeszközjuttatás, SNR és Oktávsáv módszer

[1] Jelen tanulmány a szerzőnek az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán készült „Munkahelyi zajexpozíció meghatározása és egyéni védőeszköz juttatás karbantartó munkakörben SNR és Oktávsáv módszerrel" című szakdolgozata alapján íródott.

[2] zakarias.rebeka@gmail.com | ORCID: 0009-0002-0577-8367 | HSE Expert | HSE szakértő

## BEVEZETÉS

Napjainkban több millió európai munkavállaló van a munkahelyén kitéve a zaj által okozott károsító hatásoknak és körülbelül 7 % szenved munkavégzéshez köthető halláskárosodásban. Zajnak nevezünk minden olyan hangot, amely zavaró, káros hatást, kellemetlen érzetet kelt. [1]

A munkahelyi zaj egyik legnagyobb kockázata és legkellemetlenebb hatása a halláskárosodás. A zaj okozta hallásvesztés a leggyakrabban előforduló munkahelyi megbetegedés az EU-ban, a munkahelyi megbetegedések mintegy 1/3-át teszi ki, megelőzve a bőrbetegségeket és a légzőszervi problémákat. A zaj okozta halláskárosodás, hallásvesztés mellett a zaj más károsító, kellemetlen hatásokat is okoz, hiszen csökkenti a koncentráció képességet, feszültséget, stresszt eredményez, ezzel is csökkentve a munkahelyi termelékenységet, hatékonyságot. Ezen negatív hatások elkerülése érdekében az Európai Parlament és a Tanács 2003-ban elfogadta a munkavállalókat érő fizikai tényezők (zaj) hatására vonatkozó egészségügyi és biztonsági minimumkövetelményekről szóló 2003/10/EK irányelvet, melyet a tagállamoknak kötelezően át kellett ültetniük a nemzeti jogszabályokba. Az irányelv 5. cikke kimondja, a kockázatértékelés, a műszaki fejlődés és a kollektív védelem szükségességét, a kockázatot okozó zajexpozíciót a forrásnál kell megszüntetni. Valamint az említett irányelv, minimum követelményeket is meghatároz a munkavállalókra ható zajexpozícióból eredő egészségügyi és biztonsági kockázatokkal szembeni védelmére, valamint bevezetésre kerülnek az expozíciós és a beavatkozási határértékek és kötelezi a munkáltatót, hogy a dolgozók zajterhelését szükséges mérni és meghatározni. [2]

Mindennapi tapasztalatom, hogy a munkahelyi zajjal kapcsolatos egészségügyi kockázatok kezelése kihívást jelent a munkáltató és a munkavállaló részére is. Gyakran találkozom azon problémával, hogy a dolgozók számára olyan egyéni hallásvédő eszközök vannak szolgáltatva, amelyek alkalmazása nem indokolt.

Ezen érvek alapján publikációmban beszeretném mutatni egy az általam vizsgált ipari létesítmény Karbantartó műhelyében különböző munkakörben dolgozó munkavállalókat érő munkahelyi zajexpozíció meghatározását, kockázatértékelés során felülvizsgálni a számukra szolgáltatott egyéni hallásvédőeszköz szükségességét, valamint nem megfelelőségét. Esetleges nem megfelelőség esetén a megfelelő egyéni hallásvédő eszközök kiválasztása az SNR és oktávsáv módszerek szerint.

## A MUNKAKÖRÖK BEMUTATÁSA ÉS TEVÉKENYSÉGÜK LEÍRÁSA

A karbantartó műhelyben dolgozók a kétemeletes műhelyben, külső raktárokban, külső épületű műhelyben, valamint a gyár alapanyaggyártó üzemeinek területén látnak el karbantartási, javítói tevékenységet.

A karbantartó műhely kétemeletes főépülete magában foglalja, a hegesztő, műanyag hegesztő, lakatos és lemezhajlító műhelyt, valamint egy kétemeletes belső raktárhelységet, öltözőt, mosdókat, étkezőt és egy művezetői irodát. A főépület kiegészül továbbá két külső megközelítésű raktárral, ahol a műhely mindennapi munkájához szükséges alkatrészeket, nyersanyagokat tárolnak. A karbantartó műhely főépületétől távolabb helyezkedik el még egy a műhely fennhatósága alá tartozó hegesztő műhely, ahol a dolgozók hegesztési és plazmavágási folyamatokat végeznek.

A műhelyben dolgozókat három munkakörbe tudjuk sorolni, végzettség és ezáltal ellátott munkafolyamatok, felelőségek szerint. Az említett három munkakörbe tartozik a hegesztő lakatos, képernyős lakatos, valamint a művezető beosztás. Mind a három munkakörbe tartozó munkavállalók végeznek munkát az alapanyaggyártó üzemek területén, így esetükben számításba került az alapanyaggyártó üzemek átlaga a heti zajexpozíció meghatározásánál, de a valóságot reprezentálva különböző időarányban, hiszen a hegesztő lakatos jóval több időt tartózkodik az üzemekben javítási feladatok közben, mint a művezető, aki felügyeli, valamint ellenőrzi a dolgozói által nyújtott munkát. A lakatos képernyős munkakörben dolgozó munkavállaló – aki idejének jelentős hányadát a kétemeletes belső és a kívülről megközelíthető külső raktárban tölti – mindennapi feladatai közé tartozik, az alapanyagok, nyersanyagok raktárkészletének ellenőrzése, lerendelése külső beszállítóktól, valamint a művezető távollétében ő felügyeli a műhely mindennapi munkáját, de szükség esetén képes mindennemű javítási, karbantartási munkát végezni a műhely és üzemek területén is. A művezető – hasonlóan az előbb említett képernyős lakatos munkavállalóhoz – sem látja el napi szinten a javítási tevékenységeket, hanem ellenőrzi azokat, de szükség esetén ő is be tud vonódni azokba. Az idejének nagy részét az emeleten található irodában tölti, ahol ellátja a műhelyhez kapcsolódó adminisztratív feladatokat, valamint irányítja dolgozói munkáját.

**A vizsgált dolgozókat érő általános kockázatok ismertetése**

Az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeinek biztosítása a munkáltató feladatai közé tartozik, amelyet a *89/391/EGK keretirányelv* ír elő, valamint kötelezi továbbá, hogy ezen követelmények biztosítása során keletkező költségeket, illetve egyéb terheket nem háríthatja a munkavállalóra. A feltételek biztosításának egyik fő eszköze a kockázatértékelés, melynek segítségével a foglalkoztató megfelelő megelőzési intézkedési stratégiát képes létrehozni. A kockázatértékelés elvi alapja a veszélyek, a veszélyeztetettek azonosítása és a kockázatok minőségi és mennyiségi értékelése. [3]

Ilyen mennyiségi értékelésnek tekinthető a publikációmban taglalt zajexpozíciós vizsgálat is, melyet az egészségkárosító hatás elkerülése végett szükséges elvégezni, ha feltételezhető, hogy a beavatkozási határérték túllépésre került. Veszélynek tekintünk minden olyan eszközt, felszerelést, anyagot/keveréket, módszert, gyakorlatot vagy munkakörnyezeti hatást, amely egy lehetséges sérülés vagy egészségkárosodás forrása lehet [4], valamint kockázatnak nevezünk valamely cselekvéssel, vállalkozással járó veszélyt, kárt, bajt és kellemetlenség lehetőséget. [3]

A kockázatértékelés alapján meghatározható, hogy a felmért veszélyek elkerülhetőek-e, valamint, hogy milyen intézkedések szükségesek az elkerülhetőséghez.

A munkavédelem szempontkából kiemelten fontos a munkavállalók hallásvédelme, hiszen a munkahelyi baleset, megbetegedés hátterében zajexpozíciós hallászcsökkenés is állhat, melynek következtében a dolgozó nehezebben észleli a munkakörnyezetében előforduló hanghatásokat, figyelmeztető jelzéseket. Az előbb említett okokból eredően, a hallásvédelem megvalósulása a kockázatértékelés mellett, a műszaki, kollektív, szervezési és egyéni védelemből, oktatásból, kockázatok ismertetéséből, munkavédelmi oktatásból és felügyeleti orvosi vizsgálatokból tevődik össze. [5]

Az általam vizsgált munkavállalókra, leginkább az állás, járás és ülés kockázatainak vannak kitéve mindennapi munkájuk során, valamint karbantartási munkájuk végett, kiegészül a kézi anyagmozgatással, a magasban végzett munkával, beszorulással, becsípéssel, vágással és egyéb mechanikai hatásokkal. A lakatos képernyős munkakörben a képernyős munka végett jelentkező optikai sugárzás veszélye is fellelhető. Mind a műhelyben, mind az üzemekben több munkavégzési ponton nem megfelelő, görnyedt, csavart testhelyzetben tudják munkájukat ellátni, így megállapítható, hogy jelentős a dolgozókra ható ergonómiai kockázat. A dolgozók többnyire zajos munkakörnyezetben látják el mindennapi feladataikat, melyek erednek a telepített berendezésekből, valamint az általuk használt kézi eszközökből, szerszámokból.

## MUNKAHELYI ZAJEXPOZÍCIÓ VIZSGÁLAT

A szervezett munkavégzés keretében, a munkavégzés során a munkavállalókat érő zajterhelés műszeres vizsgálatát és a munkavállalókat érő zajexpozíció meghatározását a 66/2005. (XII. 22.) EüM rendelet 1. mellékletének előírásai szerint végeztem el [6], hiszen feltételezhető, hogy a Karbantartó műhelyben a zajexpozíció túllépi a beavatkozási határértékeket.

A vizsgálat megkezdése előtt konzultáltam a karbantartó műhely művezetőjével, valamint a műhely dolgozóival is, hogy megismerjem a mindennapi munkájuk részfolyamatait, valamint a különböző munkakörökhöz tartozó feladatokat. A mérésem során prioritásként kezeltem, hogy a mérési eredmények a valóságot reprezentálják minél jobban, ezáltal üzemszerűek legyenek. Úgy határoztuk meg a vizsgálati pontokat a karbantartó műhely munkavállalóival karöltve, hogy azok között a legkedvezőtlenebb zajterhelésnek kitett dolgozók és munkahelyek is szerepeljenek. A dolgozók segítségével felvilágosítást kaptam arról, hogy egyes vizsgálati pontokon pontosan milyen munkát végeznek és mennyi időt töltenek el. A nem munkafolyamatból származó, de rendszeresen jelentkező, illetve ki nem küszöbölhető zajokat (pl. más üzemrész zaja) a mérés során figyelembe vettem, de a kizárható zajokat (rádió), a mérés idejére kikapcsolásra kerültek, hogy ne befolyásolja a mérési eredményeket. Azon nyílászárók a vizsgálati időtartamra becsukásra kerültek, melyek nem üzemszerűen, szellőzés céljából voltak nyitva, így is reprezentálva az üzemszerűséget. A műhely művezetőjétől felvilágosítást kaptam, hogy a dolgozók számára jelenleg is van egyéni hallásvédőeszköz juttatva, mégpedig SNR=31 dB zajcsillapítási értékű Peltor Optime II fültok, illetve azon pontok is meg vannak határozva, ahol ezen eszköz használata szükséges.

A mért 45 mérési pont a munkavállaló fülétől 50 cm-en belül, illetve a munkavállaló szokásos tartózkodási helyén, álló munkavégzés esetén 1,5 m, ülő munkavégzés esetén 1,25 m magasságban jelöltem ki. Amennyiben a munkahelyen a zajterhelés független volt a munkavállaló tevékenységétől, akkor a mérést a munkavállaló távollétében végeztem el.

A vizsgálat során rögzítettem a mérési pontok egyenértékű A- C- és a maximális C-hangnyomásszintjét. A munkavállalók segítségével és a vizsgálat során tapasztaltak alapján lett meghatározva a mérési pontokon a dolgozók tartózkodási ideje. A mért adatok segítségével és a meghatározott időmennyiségek segítségével számítással határoztam meg a $L_{EX,8h}$ zajexpozíciót decibelben, egyheti időtartamra. A munkahét egyes napjain a munkavállalók zajterhelése jelentősen eltérő (és ez a munkavállalókat érő zaj minősítése szempontjából lényeges), ezért heti zajexpozíciót vettem figyelembe. [6] [8]

Az általam végzett vizsgálat során egy hitelesített Brüel & Kjaer 2250 típusú műszert használtam. A használt műszeren a mérések előtt és után kalibrálást végeztem.

## A JELENLEG ALKALMAZOTT EGYÉNI HALLÁSVÉDŐESZKÖZ FELÜLVIZSGÁLATA

Az egyéni védőeszköz juttatást az MSZ EN 458:2016 szabvány szerint vizsgáltam felül, az SNR és az Oktávsáv módszer segítségével. Az SNR módszer egy egyszerű, elterjedt módszer, amelynél az egyszerűsített zajcsillapítási értéket határoztam meg eszközönként, míg az Oktávsáv módszer egy összetettebb, pontosabb eljárás, amelynél frekvenciánkként határoztam meg az eszközök elfogadott csillapítási értékeit. [7]

Valamint az MSZ EN 458:2016 szabvány meghatározza a hallásvédőeszköz használat mellett a munkavállalók fülét érő effektív hangnyomásszintek besorolásait:

| Fület érő effektív hangnyomásszint [dB] | Minősítő besorolás |
|---|---|
| nagyobb, mint 85 | elégtelen |
| 85 és 80 közötti | elfogadható |
| 80 és 75 közötti | jó |
| 75 és 70 közötti | elfogadható |
| 70 alatti | túlcsillapít |

*1. táblázat: MSZ EN 458:2016 szabvány A.4 táblázata [7]*

A 66/2005 (XII.22.) EüM rendelet értelmében azon mért 18 mérési pont esetén vizsgáltam felül az egyéni hallásvédő eszköz megfelelőségét, ahol a zajexpozíció meghaladja a felső beavatkozási határértéket. [6]

A mérési pontokhoz tartozó vizsgálati eredményekből egyértelműen látható, hogy a jelenleg használt és szolgáltatott SNR=31 dB zajcsillapítási értékű Peltor Optime II fültok egyik mérési pont esetén sem indokolt, hiszen minden esetben túlcsillapít. A munkavállalók panaszai így alátámasztásra kerültek, hiszen jelezték a munkáltatójuk felé, hogy az említett fültok használata során többször nem hallották a figyelmeztető jelzéseket, valamint a dolgozók közötti kommunikáció is megnehezítette. A túlcsillapítás elkerülése azért mellőzendő, hiszen ezzel kivédhetővé válnak az esetlegesen ebből következő balesetek, veszélyek, valamint biztosítja a gyorsabb kommunikációt, érzékelési és reagálási időt a munkavállalók számára, nem csak a veszélyes élethelyzetekben. [9]

## AZ SNR ÉS AZ OKTÁVSÁV MÓDSZER EREDMÉNYEI MÉRÉSI PONTONKÉNT

### Eredmények különböző SNR értékű hallásvédő eszközök használata mellett

Különböző csillapításértékű egyéni védőeszközök, amelyeket megvizsgáltam:

- 3M Peltor Optime II. SNR=31 dB csillapítás értékű fültok
- 3M E-A-RSoft összesodorható; 3M Ultratech előre megformált; 3M E-A-RBand pántos; 3M Caboflex pántos SNR=21 dB csillapítás értékű füldugók

- 3M Ultrafit 20 előre megformált; 3M ClearE-A-R 20 előre megformált; 3M E-A-RFlex 20 pántos; 3M Tracer 20 előre megformált SNR=20 dB csillapítás értékű füldugók
- Alpha Sota L1 fültok; Alpine Partyplug és NoNoise SNR=19 dB csillapítás értékű előre megformált füldugók
- 3M EAR Ultrafit 14 előre megformált; 3M Flex 14 pántos SNR=14 dB csillapítás értékű füldugók

| Mérési pont | Mért és kerekített $L_{Ceq}$ [dBC] hang-nyomásszint | Különböző csillapítás értékű egyéni védőeszközök használata mellett számított és kerekített $L_{AM}$ [dBA] hangnyomásszint | | | | |
|---|---|---|---|---|---|---|
| | | SNR=31 dB | SNR=21 dB | SNR=20 dB | SNR=19 dB | SNR=14 dB |
| M2 | 92 | 61 | 71 | 72 | 73 | 78 |
| M5 | 93 | 62 | 72 | 73 | 74 | 79 |
| M8 | 90 | 59 | 69 | 70 | 71 | 76 |
| M10 | 91 | 60 | 70 | 71 | 72 | 77 |
| M11 | 95 | 64 | 74 | 75 | 76 | 81 |
| M12 | 92 | 61 | 71 | 72 | 73 | 78 |
| M13 | 93 | 62 | 72 | 73 | 74 | 79 |
| M14 | 102 | 71 | 81 | 82 | 83 | 88 |
| M17 | 89 | 58 | 68 | 69 | 70 | 75 |
| M23 | 92 | 61 | 71 | 72 | 73 | 78 |
| M24 | 91 | 60 | 70 | 71 | 72 | 77 |
| M25 | 97 | 66 | 76 | 77 | 78 | 83 |
| M28 | 101 | 70 | 80 | 81 | 82 | 87 |
| M31 | 88 | 57 | 67 | 68 | 69 | 74 |

| Mérési pont | Mért és kerekített $L_{Ceq}$ [dBC] hang-nyomásszint | Különböző csillapítás értékű egyéni védőeszközök használata mellett számított és kerekített $L_{AM}$ [dBA] hangnyomásszint | | | | |
|---|---|---|---|---|---|---|
| | | SNR=31 dB | SNR=21 dB | SNR=20 dB | SNR=19 dB | SNR=14 dB |
| M32 | 94 | 63 | 73 | 74 | 75 | 80 |
| M34 | 95 | 64 | 74 | 75 | 76 | 81 |
| M36 | 97 | 66 | 76 | 77 | 78 | 83 |
| M45 | 94 | 63 | 73 | 74 | 75 | 80 |

*2. táblázat: Vizsgálati eredmények különböző SNR csillapítás értékű hallásvédő eszközök használata mellett*

**Eredmények frekvenciaszint szerint (oktávsáv módszer)**

Frekvencia szerinti különböző csillapításértékű egyéni védőeszközök, amelyeket megvizsgáltam:

- 3M Peltor Optime II. fültok {1}
- 3M E-A-RSoft összesodorható füldugó {2}
- 3M Ultratech előre megformált füldugó {3}
- 3M E-A-RBand pántos füldugó {4}
- 3M Caboflex pántos füldugó {5}
- 3M Ultrafit 20 előre megformált; 3M ClearE-A-R 20 előre megformált; 3M E-A-RFlex 20 pántos; 3M Tracer 20 előre megformált füldugók (ezen típusoknál megegyezik a frekvencia szerinti zajcsillapítás érték) {6}
- Alpha Sota L1 fültok {7}
- Alpine Partyplug előre megformált füldugó {8}
- NoNoise előre megformált füldugó {9}
- 3M EAR Ultrafit 14 előre megformált; 3M Flex 14 pántos füldugók (ezen típusoknál megegyezik a frekvencia szerinti zajcsillapítás érték) {10}

| Mérési pont | Frekvenciaszint szerinti különböző csillapítás értékű egyéni védőeszközök használata mellett számított és kerekített $L'_{p,A}$ [dBA] hangnyomásszint | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | {1} | {2} | {3} | {4} | {5} | {6} | {7} | {8} | {9} | {10} |
| M2 | 57 | 74 | 73 | 73 | 74 | 71 | 72 | 74 | 74 | 76 |
| M5 | 62 | 71 | 74 | 70 | 70 | 70 | 70 | 75 | 77 | 76 |

| Mérési pont | Frekvenciaszint szerinti különböző csillapítás értékű egyéni védőeszközök használata mellett számított és kerekített $L'_{p,A}$ [dBA] hangnyomásszint | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | {1} | {2} | {3} | {4} | {5} | {6} | {7} | {8} | {9} | {10} |
| M8 | 59 | 71 | 69 | 72 | 71 | 71 | 73 | 73 | 72 | 79 |
| M10 | 60 | 69 | 73 | 68 | 68 | 68 | 68 | 73 | 74 | 72 |
| M11 | 64 | 70 | 76 | 67 | 68 | 70 | 68 | 75 | 78 | 72 |
| M12 | 61 | 70 | 73 | 69 | 69 | 69 | 69 | 73 | 73 | 73 |
| M13 | 61 | 71 | 73 | 71 | 71 | 71 | 70 | 74 | 74 | 77 |
| M14 | 69 | 83 | 82 | 83 | 83 | 82 | 83 | 85 | 85,4 | 90 |
| M17 | 57 | 67 | 69 | 66 | 66 | 66 | 67 | 69 | 70 | 71 |
| M23 | 60 | 69 | 72 | 68 | 69 | 69 | 68 | 73 | 73 | 72 |
| M24 | 61 | 70 | 70 | 70 | 70 | 71 | 73 | 72 | 71 | 78 |
| M25 | 66 | 73 | 77 | 72 | 72 | 73 | 71 | 77 | 79 | 75 |
| M28 | 70 | 77 | 83 | 76 | 77 | 77 | 76 | 82 | 85 | 80 |
| M31 | 59 | 68 | 66 | 67 | 67 | 69 | 71 | 69 | 68 | 75 |
| M32 | 66 | 68 | 68 | 67 | 67 | 73 | 72 | 71 | 71 | 77 |
| M34 | 64 | 73 | 77 | 73 | 73 | 73 | 73 | 77 | 77 | 77 |
| M36 | 64 | 72 | 76 | 71 | 71 | 72 | 72 | 76 | 79 | 76 |
| M45 | 64 | 70 | 75 | 68 | 68 | 71 | 70 | 75 | 77 | 74 |

*3. táblázat: Vizsgálati eredmények frekvenciaszint szerinti különböző zajcsillapítás értékű hallásvédő eszközök használata mellett*

## ÖSSZEGZÉS

A szolgáltatott egyéni hallás védőeszköz helyett a vizsgálati pontok többségénél a 3M EAR Ultrafit 14 előre megformált vagy a 3M Flex 14 pántos füldugók valamelyike

alkalmazandó munkavégzés és működő zajforrás esetén, melyeknél a kialakításban különbözőek egymástól, de a frekvencia szerinti zajcsillapítás értékük azonos. Az M10 (pneumatikus kézi maró, marás), az M11 (kézi sarokcsiszoló, csiszolás), az M23 (kézi körfűrész, fűrészelés) és az M45 (plazmavágó berendezés, plazmavágás) mérési pontok esetén munkavégzés közben, működő zajforrásnál a NoNoise előre megformált füldugó használata az optimális, az M14 (kézi ütvefúró, fúrás) mérési pont esetén pedig a 3M Ultrafit 20 előre megformált; a 3M ClearE-A-R 20 előre megformált; a 3M E-A-RFlex 20 pántos vagy a 3M Tracer 20 előre megformált füldugók közül valamelyik típus alkalmazása elfogadható, melyek szintén kialakításban különbözőek, a frekvencia szerinti zajcsillapítási értékük azonban megegyező. Az előző pontban szemléltetett különbségek a két módszer összehasonlítása során jól látható, hogy az oktávsáv módszerrel meghatározott védőeszköz juttatás sokkal pontosabb és részletesebb, hiszen több esetben is felfedezhető volt az SNR módszerhez képest a túl vagy az alulcsillapítás megléte, így indokolttá válik, hogy lehetőség szerint az egyéni hallásvédőeszközök kiválasztásánál mind a két módszer alkalmazásra kerüljön.

## FELHASZNÁLT IRODALOM


[1] J. Maue, Noise, 2016 https://oshwiki.eu/wiki/Noise, (Utolsó letöltés: 2022.11.17.)

[2] Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség, A munkahelyi zaj hatása, The impact of noise at work, Facts 57 kiadás, https://osha.europa.eu/hu/publications/factsheet-57-impact-noise-work, (Utolsó letöltés: 2022.11.17.)

[3] Faragó F., Kockázatértékelés előadás, Óbudai Egyetem 2021/22 II. félév

[4] Dr. Nagy K. J., Munkahigiéne előadás, NNK 2019, https://www.nnk.gov.hu/attachments/article/108/01_Nagy_Karoly_forum_2019-05-08.pdf, (Utolsó letöltés: 2022.06.24.)

[5] Bán Cs., Kockázatbecslés előadás, Óbudai Egyetem, 2020/21 II. félév

[6] 66/2005. (XII. 22.) EüM rendelet a munkavállalókat érő zajexpozícióra vonatkozó minimális és biztonsági követelményeiről és melléklete, https://net.jogtar.hu/jogszabaly?docid=a0500066.eum, (Utolsó letöltés: 2022.11.17.)

[7] MSZ EN 458:2016 Hallásvédők. Ajánlások a kiválasztáshoz, a használathoz, a gondozáshoz és a karbantartáshoz. Útmutató dokumentum, Hearing protectors. Recommendations for selection, use, care and maintenance. Guidance document. (Utolsó letöltés: 2022.01.11.)

[8] Módszertani útmutató a zaj-és rezgéstechnikai mérési gyakorlatokhoz, OMKT 2007, https://docplayer.hu/27578455-Modszertani-utmutato-a-zaj-es-rezgestechnikai-meresi-gyakorlatokhoz.html, (Utolsó letöltés: 2022.11.17.)

[9] DND honlap: https://www.dnd.hu/blog/hallasvedelmi-kisokos-avagy-amit-a-fuldugokrol-es-fultokokrol-tudnod-kell, (Utolsó letöltés: 2022.07.19)

**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