ISSN 2676-9042

Vol 7, No 3, 2025.

2025, VII. 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 **Levitation II. (detail)** painting | A borítón **BORS Györgyi** painter/festőművész **Lebegés II. (részlet)** 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

Digital Object Identifier | Digitális ObjektumAzonosító
https://www.doi.org

| 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 7, No 3, 2025.** | **2025. VII. évf. 3. szám**

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

## BAKOSNÉ DIÓSZEGI Mónika

dioszegi.monika@bgk.uni-obuda.hu

Associate Professor and Deputy Director of the Institute of Natural Sciences and Fundamentals of Engineering at the Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University. She is an active supervisor at the Doctoral School on Safety and Security Sciences of Óbuda University. Her teaching and research areas include statics, ESG, and biogas and energy systems. She has led and contributed to numerous research and development projects, integrating the theoretical foundations of engineering sciences with the practical implementation of sustainable energy solutions.

Egyetemi docens, a Természettudományi és Alapozó Tantárgyi Intézet intézetigazgató-helyettese az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán. Témavezetőként aktívan közreműködik az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának munkájában. Oktatási és kutatási területei közé tartozik a statika, az ESG, valamint a biogáz- és energetikai rendszerek. Számos kutatásfejlesztési projekt szakmai irányítója és résztvevője, aki a mérnöki tudományok elméleti alapjait a fenntartható energetikai megoldások gyakorlati alkalmazásával ötvözi.

## BENDIÁK István

bendiak.istvan@uni-obuda.hu

I graduated from Óbuda University, Kandó Kálmán Faculty of Electrical Engineering, with both BSc and MSc degrees in Electrical Engineering, specializing in control engineering. My main fields of expertise are electrical machines and drives, rotating machine diagnostics, and signal processing. Currently, I am a PhD student at the Doctoral School on Safety and Security Sciences at Óbuda University, while also working at the Institute of Automation and Power Systems, Department of Automation. I teach electrical machines and drives at both BSc and MSc levels. Since 2010, I have been engaged in various professional roles related to electrical machines, including maintenance, testing, design, diagnostics, and education. My research interests focus on improving the efficiency of electric drives, developing diagnostic methods, and applying intelligent systems in the field of electrical engineering.

Az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karán végeztem villamosmérnöki tanulmányaimat BSc és MSc szinten, irányítástechnika specializáción. Fő szakterületeim közé tartoznak a villamos gépek és hajtások, a forgógép diagnosztika és a jelfeldolgozás. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója vagyok, miközben az Automatizálási és Energiarendszerek Intézet Automatika Tanszékén dolgozom. Oktatási tevékenységem során BSc és MSc szinten tanítok villamos gépeket és hajtásokat. Pályafutásom 2010-ben indult, azóta többféle pozícióban szereztem tapasztalatot: karbantartás, tesztelés, tervezés, diagnosztika és oktatás területén. Kutatási érdeklődésem középpontjában az elektromos hajtások hatásfokának növelése, diagnosztikai módszerek fejlesztése és az intelligens rendszerek alkalmazása áll.

## BERÉNYI Csaba

berenyi.csaba@kgk.uni-obuda.hu

Csaba BERÉNYI was born in Cegléd in 1975. He obtained his first degree in technical computer engineering from the Gábor Dénes College of Information Technology (1999). Between 2020 and 2022, he obtained a degree in engineering education from Óbuda University, and in 2021–2022, he completed a course in digital regional development at Edutus University. In 2023–2024, he took the public education leader and teacher certification exam at the Department of Tech-

BERÉNYI Csaba, 1975-ben született Cegléden. Első diplomáját a Gábor Dénes Informatikai Főiskola műszaki informatikus mérnök szakán szerezte (1999). 2020 és 2022 között az Óbudai Egyetemen mérnöktanári végzettséget szerzett, 2021–2022-ben elvégezte az Edutus Egyetem digitális térségfejlesztés képzését. 2023–2024-ben a Budapesti Műszaki Egyetem Műszaki Pedagógia Tanszékén közoktatási vezető és pedagógus-szakvizs-

nical Pedagogy at the Budapest University of Technology. Since 2023, he has been a doctoral student at the Doctoral School of Security Sciences at Óbuda University, researching security risks arising from the use of artificial intelligence and awareness of these risks among young people – examining technical threats and information security responses. Since 2017, he has been a lecturer and business development consultant at the Cegléd Vocational Training Center, and from 2023, he will be an assistant professor and lecturer at the Keleti Károly Faculty of Economics at Óbuda University. According to the MTMT registry, his publications currently include two scientific journal articles, five professional studies, nine conference papers, and five abstracts.

gát tett. 2023-tól az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusza, kutatási témája: Mesterséges intelligencia használatából eredő biztonsági kockázatok és azok tudatosulása a fiatal korosztályok körében – technikai fenyegetések és információbiztonsági válaszreakciók vizsgálata. Szakmai pályafutása során 2017 óta a Ceglédi Szakképzési Centrum oktatója és üzletfejlesztési tanácsadója, 2023-tól pedig az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi tanársegédje és oktatója. Publikációs tevékenysége az MTMT nyilvántartása alapján jelenleg 2 tudományos folyóiratcikket, 5 szakmai tanulmányt, 9 konferenciaközleményt és 5 kivonatot foglal magában.

**BOTTYÁN Sándor**

bottyan.sandor@gmail.com

Sándor BOTTYÁN is an information security expert at Paks II Nuclear Power Plant Ltd., a law enforcement administration manager in Prison Studies, a certified cybersecurity specialist, and a doctoral student at the Military Engineering Doctoral School of the University of Public Service. He has been started artificial intelligence research since 2020 and cybersecurity since 2022. His doctoral dissertation focuses on the potential applications of large language models in strategic-level military cyber threat intelligence. As a former senior administration officer in the prison service, his previous innovative research has been conducted within the field of law enforcement science, specifically in the scientific study of corrections. He is a multiple-time recipient of the New National Excellence Program (ÚNKP) scholarship, a recipient of the University of Public Service's Professional Scholarship (2022), and a member of the Scientific Association for Infocommunications and Information Technology (HTE). He holds certifications in ISO/IEC 42001 (Artificial Intelligence Management System) and ISO/IEC 27001 (Information Security Management System).

BOTTYÁN Sándor a Paks II. Atomerőmű Zrt. információbiztonsági szakértője, rendészeti igazgatásszervező, okleveles kiberbiztonsági szakértő, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának doktorandusza. 2020 óta foglalkozik a mesterséges intelligencia kutatásával, 2022 óta kiberbiztonsággal, doktori értekezésének témája a nagy nyelvi modellek alkalmazásának lehetőségei a stratégiai szintű katonai kiberfenyegetés hírszerzésben. Volt büntetés-végrehajtási főtisztként eddigi innovatív kutatásait a rendészettudomány, azon belül kifejezetten az büntetés-végrehajtás tudományos területén végezte. Többszörös ÚNKP ösztöndíjas hallgatói kutató, az NKE Szakmai Ösztöndíjasa (2022) a Hírközlési és Informatikai Tudományos Egyesület tagja. ISO/IEC 42001 (mesterséges intelligencia irányítási rendszer) és ISO/IEC 27001 (információbiztonsági irányítási rendszer) képesítésekkel rendelkezik.

**BRAUN András**

braun.andras92@stud.uni-obuda.hu

András BRAUN graduated from the Faculty of Military and Security Engineering of the National University of Public Service in 2016 with a specialization in radar engineering. In 2022, he graduated from Óbuda University with an MSc in Security Engineering. He participated in the operation and operation of military radars in service in Hungary for nearly 7 years. He is currently a doctoral student at the Doctoral School of Safety and Security Sciences, his field of research is the safety assessment of the operation of radar systems.

BRAUN András 2016-ban a Nemzeti Közszolgálati Egyetem Had- és Biztonságtechnikai mérnöki Karán végzett radar mérnök specializáción. 2022-ben az Óbudai Egyetem Biztonságtechnikai mérnöki MSc szakon szerzett diplomát. Közel 7 éven keresztül vett részt a Magyarországon hadrendben álló katonai radarok üzemeltetésében, működtetésében. Jelenleg a Biztonságtudományi Doktori Iskola doktorandusz hallgatója, kutatási területe, tanulmányain belül, a radarok alkalmazásának biztonságtechnikai vizsgálata.

## CSISZÁRIK-KOCSIR Ágnes

kocsir.agnes@kgk.uni-obuda.hu

Prof. Dr. Ágnes CSISZÁRIK-KOCSIR is a full-professor at the Keleti Károly Faculty of Business and Management at Óbuda University. Prior to her university career, she was responsible for the financial management of numerous European Union-funded projects, in addition to her general project management duties. She has been working at Óbuda University's predecessor institution since 2007, first as a teaching assistant and later as an assistant professor. She has been an associate professor at the Keleti Károly Faculty of Business and Management at Óbuda University since 2013 and a professor since 2025. She was habilitated in 2017, has been working as institute director since 2018, and as deputy dean of research at the faculty since 2020. Since 2004, he has published nearly 700 articles in the MTMT. Her Hirsh index is 24. She is a member of the editorial board of several professional organizations and domestic and international journals, a reviewer, and a member of the scientific and organizing committees of several domestic and international scientific conferences. She is a committed advocate of project thinking and building financial, digital, and consumer awareness, which is also reflected in her research.

Prof. Dr. CSISZÁRIK-KOCSIR Ágnes az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi tanára. Egyetemi munkássága előtt számos Európai Unió által finanszírozott projekt pénzügyi menedzsmentjét látta el az általános projektvezetői feladatok mellett. Az Óbudai Egyetem jogelőd intézményében 2007 óta dolgozik először tanársegédként, később adjunktusként. 2013-tól az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense, 2025-től egyetemi tanára. 2017-ben habilitált, 2018-tól intézetigazgatóként, 2020-tól pedig a Kar kutatási dékánhelyetteseként dolgozik. 2004-től az MTMT-ben a mai napig rögzített publikációinak száma közel 700. Hirsh-indexe 24. Több szakmai szervezet, hazai és nemzetközi folyóirat szerkesztőbizottságának tagja, lektora, valamint több hazai és nemzetközi tudományos konferencia tudományos és szervezőbizottságának tagja. Elkötelezett híve a projektszemélet és a pénzügyi, digitális és fogyasztói tudatosság építésének, amit kutatási is igazolnak.

## GULYÁS Olivér

gulyaso@gmail.com

Oliver GULYÁS, PhD student. I studied at the Foreign School of Economics in Budapest and the University Paris 1 Panthéon – Sorbonne. I started my PhD studies at the Óbudai University Doctoral School for Safety and Security Sciences in 2021. After finishing MSc. studies, I was working in the banking sector, after more than 15 years I started to work as an advisor. In my role as an advisor, I did not left the financial sector, I am still working with banks or for banks. As an advisor I was involved in the "creation" of a unified new bank when I had the opportunity to have an insight into the vulnerability of the organisation more than before and I experienced the everyday operational problems. It was at the final phase of this transformation when the COVID-19 pandemic broke out, this imposed new threats to the still fragile system. It was then I decided to deep dive in the subject. With the guidance of Dr. habil. Gabor Kiss I am trying to identify the current issues of cybersecurity, in particular its impact on the financial sector.

GULYÁS Olivér, PhD tanuló. A Külkereskedelmi Főiskola, majd azt követően a Paris 1 – Panthéon Sorbonne egyetemen tanultam. 2021-ben kezdtem el PhD tanulmányaimat az Óbudai Egyetem Biztonságtudományi doktori iskolájában. Egyetemi tanulmányaim elvégzése után a bankszektorban helyezkedtem el, majd több mint 15 év után tanácsadással kezdtem el foglalkozni. Tanácsadóként nem távolodtam el a pénzügyi szektortól, továbbra is bankoknak vagy bankokkal dolgozok. Már tanácsadóként egy egyesített, új bank „létrehozásában" vettem részt, amikor az addiginál jobban beleláttam a szervezet sérülékenységébe, megtapasztalhattam a mindennapos működési problémákat. Ennek az átalakulásnak a végén tört ki a COVID-19 járvány, ami újabb problémákat keletkeztetett a még törékeny rendszerben. Ekkor fogalmazódott meg benne annak az igénye, hogy mélyebben is beleássam magam a témába. Az egyetemen Dr. habil. Kiss Gábor útmutatása mellett próbálom feltérképezni a kiberbiztonság aktuális kérdéseit, különös tekintettel a pénzügyi szektorra gyakorolt hatásait.

## HERÉNYI Zoltán

zoltan.herenyi@gmail.com

Following the completion of his electrical engineering degree, the author worked for 17 years as an occupational safety inspector within the national labour safety authority. His earlier industrial experience and hands-on knowledge gained during his inspections led him to realize that new, more effective solutions are needed in the prevention and investigation of workplace accidents. In pursuit of this goal, he earned an MSc in Computer Science from the University of Miskolc, with a thesis focused on the image-based detection of personal protective equipment and hazardous zones. He is currently enrolled in the occupational safety engineering postgraduate program at Óbuda University, and is also a state-funded PhD student at the Doctoral School of Safety and Security Sciences. His research explores the applicability of artificial intelligence in preventing occupational diseases and workplace accidents.

A szerző villamosmérnöki diplomáját követően 17 éven át dolgozott munkavédelmi felügyelőként az állami munkavédelmi hatóságnál. Korábbi ipari tapasztalatai és felügyelői munkája során szerzett gyakorlati ismeretei vezették el annak felismeréséhez, hogy a munkahelyi balesetek megelőzése és kivizsgálása területén új, hatékonyabb megoldásokra van szükség. Ennek jegyében informatika MSc diplomát szerzett a Miskolci Egyetemen, diplomamunkáját a munkavédelmi felszerelések és veszélyzónák képfeldolgozáson alapuló felismeréséről írta. Jelenleg munkavédelmi szakmérnök hallgató az Óbudai Egyetem levelező képzésén, valamint állami ösztöndíjas doktorandusz a Biztonságtudományi Doktori Iskolában. Kutatási területe a mesterséges intelligencia foglalkozási megbetegedések és munkabalesetek megelőzésében való alkalmazhatósága.

## KISS Gábor

kiss.gabor@bgk.uni-obuda.hu

Dr. habil. Gabor KISS is associated professor and the Head of the Institute of Safety Science and Cybersecurity at the Óbuda University. He received the PhD. degree in Mathematics and Computer Science from Debrecen University in 2013 and the Habilitation in Safety and Security Science from Óbuda University in 2020. Dr. Kiss was a guest scientist in the Faculty of Computer Science Freie Universität Berlin in 2003 and Universität Paderborn in 2006. Dr. Kiss has published more than 210 refereed papers in Journals and Proceedings. He serves as an Editorial board member more Journals. He has been a Keynote speaker, Panelist speaker, Publicity chair, Program Committee or Organizing Committee member for more than 230 international conferences. Dr. Kiss is a member of the Hungarian Academy of Sciences, and more Hungarian and International Societies in Computer Science. Dr. Kiss is an external expert of Bureau of Education, Hungary; National Research, Development and Innovation Office of Hungary; Romanian Agency for Quality Assurance in Higher Education (ARACIS). Dr. Kiss is the director of College for Advanced Studies in Safety Science and Cybersecurity. His research interests include Artificial Intelligence in the Computer Science Education, Information Security Awareness, AI in self-driving vehicles, AI in Healthcare.

Dr. habil. KISS Gábor egyetemi docens, az Óbudai Egyetem Biztonságtudományi és Kiberbiztonsági Intézetének vezetője. A Debreceni Egyetem matematika-informatika szakán 2013-ban szerzett PhD. fokozatot, az Óbudai Egyetemen pedig 2020-ban habilitált biztonságtudományi és biztonságtechnikai szakon. Dr. Kiss Gábor 2003-ban a Freie Universität Berlin, 2006-ban pedig az Universität Paderborn németországi egyetemeknek Informatika Karán volt vendégkutató. Dr. Kiss Gábor több mint 210 referált tanulmányt publikált folyóiratokban és folyóiratokban. Több folyóirat szerkesztőbizottsági tagja. Több mint 230 nemzetközi konferencián volt Keynote speaker, Panelist speaker, Publicity chair, Program Committee vagy Organizing Committee Member. Dr. Kiss Gábor tagja a Magyar Tudományos Akadémiának, valamint több magyar és nemzetközi számítástechnikai társaságnak. Dr. Kiss Gábor külső szakértője az Oktatási Hivatalnak, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatalnak; a Romániai Felsőoktatási Minőségbiztosítási Ügynökségnek (ARACIS). Dr. Kiss Gábor a Biztonságtudományi Szakkollégium igazgatója. Kutatási területei közé tartozik a mesterséges intelligencia az informatikai oktatásban, az információbiztonsági tudatosság, a mesterséges intelligencia az önvezető járművekben, a mesterséges intelligencia az egészségügyben.

## KOVÁCS Károly

kovacs.karoly@kvk.uni-obuda.hu

Dr. Károly KOVÁCS, certified electrical engineer, holds a Candidate of Technical Sciences degree (equivalent to Ph.D.). Since 2010, he has held a senior position at the Hungarian subsidiary of DEHN, a German company. He also works part-time as an Assistant Professor at the Kandó Kálmán Faculty of Electrical Engineering, Óbuda University. He lectures in Lightning Protection, a subject offered in both English and German, and teaches the course on Energy Informatics. Dr. Kovács is a board member of the Electrical Engineering Division of the Hungarian Chamber of Engineers, as well as a board member of EMOSZ, the National Association of Electrical Industry Private Entrepreneurs. He holds official design licenses in the field of building electrical engineering, including a specialized license for lightning protection system design. Within the Hungarian Chamber of Engineers, he serves as an instructor for both the preparatory course for lightning protection (Vn) certification exams and the mandatory professional continuing education program, specifically in the field of lightning protection.

Dr. KOVÁCS Károly, okleveles villamosmérnök, a műszaki tudomány kandidátusa. 2010 óta a DEHN németországi cég magyarországi leányvállalatának vezető beosztású alkalmazottja, félállásban az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar adjunktusa, a Villámvédelem választható angol és német nyelven futó tárgyak előadója, valamint az Energetikai Informatika tárgy oktatója. A Magyar Mérnöki Kamara Elektrotechnikai Tagozatának elnökségi tagja, valamint az EMOSZ Elektromosipari Magánvállalkozók Országos Szakmai Egyesületének elnökségi tagja. Épületvillamossági területen kamarai tervezői jogosultsággal rendelkezik ill. külön jogosítása van Villámvédelem tervezésére. A Magyar Mérnöki Kamarában a Vn jogosítási vizsgára felkészítő tanfolyam és a kötelező szakmai továbbképzési rendszerben a villámvédelem téma oktatója. Szakterülete a villámvédelemi és túlfeszültség-védelmi rendszerek tervezése, létesítése, valamint a villámvédelmi elméleti kutatások bevezetése a napi gyakorlatba.

## KÚN Gergely

kun.gergely@kvk.uni-obuda.hu

Gergely KÚN is electrical engineer and assistant lecturer at the Department of Telecommunications, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University. His teaching activities cover the fields of telecommunications, mobile communication, and fundamental topics in electrical engineering. His research focuses on modern telecommunication systems. In addition to his academic work, he is involved in certification activities in the field of railway control-command and signalling at the Institute for Transport Sciences.

KÚN Gergely okleveles villamosmérnök, egyetemi tanársegéd az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karának Híradástechnika Tanszékén. Oktatási tevékenysége a híradástechnika, mobilkommunikáció és villamosmérnöki alapismeretek területeire terjed ki. Kutatási témája a modern telekommunikációs rendszerekhez kapcsolódik. Egyetemi munkája mellett a Közlekedéstudományi Intézetben tanúsítási tevékenységet végez a vasúti ellenőrző-irányító és jelző szakterületen.

## MÁRKOS Szilárd Attila

markos.szilard@bgk.uni-obuda.hu

I completed my higher education studies at the Bánki Donát Faculty of Mechanical and Safety Engineering at Óbuda University. I obtained my bachelor's degree (BSc) in 2011, specializing in mechanical engineering and machine design, and then in 2015 I completed my master's degree (MSc) in mechatronics engineering, specializing in intelligent equipment. During my professional career, I have worked on numerous industrial projects as a mechanical designer, regularly consulting

Felsőfokú tanulmányaimat az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán végeztem. Alapszakos (BSc) diplomámat 2011-ben szereztem meg Gépészmérnök Gépszerkesztő tervező szakirányon, majd 2015-ben Mechatronikai mérnökként végeztem el a mesterképzést (MSc) az Intelligens berendezések szakirányon. Szakmai pályám során számos ipari projektben dolgoztam gépészeti tervezőként, amelyek működtetése közben rendszeresen

with electrical engineers and automation specialists during their operation. As a result, I have gained an increasingly deeper insight into the design of complex, multidisciplinary systems. After that, my interest turned to modern building engineering, in the context of which I designed several systems related to the topic. Nowadays, hot and cold water networks and artificial ventilation require a number of auxiliary devices, and electrical networks are becoming increasingly complex. Control is essential for the coordinated operation of all these systems. Home automation offers a solution to these tasks, which is how I came into contact with this field of science.

egyeztettem villamosmérnök és automatizálási szakemberekkel. Ennek köszönhetően egyre mélyebb rálátásom alakult ki a komplex, több szakterületet átfogó rendszerek tervezésére. Ezek után az érdeklődésem a modern épületgépészet felé fordult, melynek keretében több, a témához kapcsolódó rendszert is terveztem. Napjainkban már a hideg-meleg vízhálózatok és a mesterséges szellőztetés is számos segéd berendezést igényel, a villamos hálózatok pedig egyre összetettebbé válnak. Mindezek összehangolt működéséhez elengedhetetlen a vezérlés. Ezen feladatok elvégzésére kínál megoldást a domotika, így kerültem kapcsolatba ezzel a tudományággal.

**MÓDNÉ TAKÁCS Judit**

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

Judit MÓDNÉ TAKÁCS is a PhD candidate who has passed the required courses at the Doctoral School of Security Sciences, Obuda University. Her main research areas include engineering education, cybersecurity awareness, the role and development of soft skills in engineering education, the methodology of adult education, as well as the study of methods that encourage and motivate students to learn and practically apply STEM subjects.

MÓDNÉ TAKÁCS Judit az Óbudai Egyetem Biztonságtudományi Doktori Iskola abszolvált PhD hallgatója. Fő kutatási területe a mérnökképzés, a kiberbiztonsági tudatosság, a puha készségek szerepe és fejlesztése a mérnökképzésben, a felnőttképzés módszertana, a hallgatókat a STEM tantárgyak tanulására és gyakorlati alkalmazására inspiráló és motiváló módszerek kutatása.

**MORVAY László**

morvay.laszlo@phd.uni-obuda.hu

László MORVAY (1967) electrical operating engineer in the medical technology sector (KKVMF, 1989) and MSc in safety engineering (ÓE-BGK, 2023). He is currently the managing director of HOLL & MOOR Health Service and Consulting Ltd. He specializes in soft laser therapy, as well as compiling professional material for research and development projects supported from EU and domestic funds, and monitoring and documenting the professional progress of projects. Contract tender assessor of the National Research, Development and Innovation Office. Continuous learning is the key to professional development, so he is currently a doctoral student at Óbuda University's Doctoral School on Safety and Security Sciences. His field of research is the investigation of medical devices used in musculoskeletal disorders, which covers the safety issues of soft laser therapy (light), ultrasound therapy (mechanical) and electrotherapy (electric current).

MORVAY László (1967) villamos-üzemmérnök orvostechnikai ágazaton (KKVMF, 1989) és biztonságtechnikai mérnök-tervező MSc (ÓE-BGK, 2023). Jelenleg a HOLL & MOOR Egészségügyi Szolgáltató és Tanácsadó Kft ügyvezetője. Szakterülete a lágylézer terápia, valamint uniós és hazai forrásból támogatott kutatás-fejlesztési projektek szakmai anyagának összeállítása, a projektek szakmai előrehaladásának ellenőrzése, dokumentálása. A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal szerződéses pályázati bírálója. A szakmai fejlődés kulcsa a folyamatos tanulás, ezért jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza. Kutatási területe a mozgásszervi megbetegedések során alkalmazott orvostechnikai eszközök vizsgálata, amely a lágylézer terápia (fény), az ultrahang terápia (mechanikai) és az elektroterápia (elektromos áram) biztonsági kérdéseire terjed ki.

**OLÁH Róbert**

olah.robert0721@gmail.com

My name is Róbert Oláh, and I am a computer engineer and artificial intelligence researcher. I hold a

Oláh Róbert vagyok, mérnökinformatikus és mesterséges intelligencia kutató. Tanulmányaimat az Óbudai

BSc in Computer Engineering, an MSc in Software Engineering, and an MSc in Engineering Education from Óbuda University. I am an active member of the Artificial Intelligence Research Group at the Bánki Donát Faculty of Mechanical and Safety Engineering, where my research focuses on the application of artificial intelligence in security systems, machine learning algorithms, and network monitoring solutions. My specific areas of interest include the use of AI in network security, as well as applying machine learning and deep learning techniques to the detection of cyber threats.

Egyetemen végeztem, ahol Mérnök informatika BSc, Programtervező MSc és Mérnöktanári MSc szakokon szereztem diplomát. Jelenleg az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Karán működő Mesterséges Intelligencia Műhely tagjaként veszek részt kutatási projektekben. Fő kutatási területeim közé tartozik a mesterséges intelligencia biztonságtechnikai alkalmazása, különös tekintettel a hálózati biztonságra, a gépi tanulási algoritmusokra és a hálózati megfigyelő rendszerek fejlesztésére. Érdeklődésem kiterjed a gépi tanulás és a deep learning módszerek alkalmazására a kiberfenyegetések detektálásában.

## PETŐ Richárd

peto.richard@bgk.uni-obuda.hu

Dr. Richárd PETŐ is a supervisor at the Doctoral School of Security Sciences at Óbuda University. He earned his PhD in Military Sciences from Óbuda University in 2017. His research discipline is military engineering with a focus on Devices and options for protecting objects against criminal/terrorist bombings.

Dr. PETŐ Richárd az Óbudai Egyetem Biztonságtudományi Doktori Iskola témavezetője. Tudományos, PhD, fokozatát az Óbudai Egyetem, katonai műszaki tudományok ágon szerezte 2017-ben. Kutatási területe az Objektumok védelmének eszközei és lehetőségei a bűnös célú/terror jellegű robbantásokkal szemben.

## POGÁTSNIK Monika

pogatsnik.monika@amk.uni-obuda.hu

Monika POGÁTSNIK is a habilitated associate professor at Óbuda University, vice dean for education and head of institute at the Alba Regia Faculty. Her research focuses on engineering pedagogy, with special emphasis on work-based learning, the development of non-cognitive skills, and career orientation attitudes. She has authored over 130 scientific publications, which have received more than 300 citations. Her academic and educational work places particular emphasis on supporting the digital competencies and resilience of young generations, especially engineering students. In recognition of her high-quality professional contributions, she was awarded the Knight's Cross of the Hungarian Order of Merit (civil division) in 2025.

POGÁTSNIK Monika az Óbudai Egyetem habilitált egyetemi docense, az Alba Regia Kar oktatási dékánhelyettese és intézetigazgatója. Kutatási területe a mérnökpedagógia, különös tekintettel a munkaalapú tanulásra, a nem kognitív készségek fejlesztésére és a pályaorientációs attitűdök vizsgálatára. Több mint 130 tudományos publikációja jelent meg, amelyekre több mint 300 hivatkozás érkezett. Oktatási és kutatási tevékenysége során kiemelt figyelmet fordít a fiatal generációk, különösen a mérnökhallgatók digitális kompetenciáinak és ellenállóképességének fejlesztésére. Magas színvonalú szakmai munkájának elismeréseként 2025-ben a Magyar Érdemrend lovagkereszt polgári tagozat kitüntetésben részesült.

## RÁCZ Ervin

racz.ervin@kvk.uni-obuda.hu

Full Professor and Director of the Institute of Electrophysics at the Kandó Kálmán Faculty of Electrical Engineering, Óbuda University. Under his academic leadership, the teaching of mathematics and physics is carried out at the faculty. His research interests include laser physics, solar energy systems, advanced photovoltaic technologies, nuclear power plants, distributed parameter networks, and the methodological development of physics education. As a PhD supervisor, he

Egyetemi tanár, Az Óbudai Egyetem – Kandó Kálmán Villamosmérnöki Karon működő Elektrofizikai Intézet, intézetigazgatója igazgatója. Szakmai felügyelete alatt zajlik a matematika és fizika tantárgyak oktatása. Kutatási területei közé tartozik a lézerfizika, a napelemes energiarendszerek, a speciális napelemek, atomerőművek és az elosztott paraméterű hálózatok, valamint a fizikaoktatás módszertani fejlesztése. Témavezetőként aktívan részt vesz az

actively contributes to the work of the Doctoral School on Safety and Security Sciences, promoting the integration of multidisciplinary research with industrial applications.

Óbudai Egyetem Biztonságtudományi Doktori Iskolájának munkájában, támogatva a multidiszciplináris kutatások és az ipari alkalmazások közötti kapcsolat erősítését.

**REZSABEK Nándor**

rezsabek.nandor@stud.uni-nke.hu

The author, REZSABEK, N. (1972–), is a certified geographer (specialization in resource and risk analysis) (MSc); an applied environmental researcher (specialization in environmental safety management) (BSc); an organizational plant engineer (BSc); student of the Ludovika University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering (PhD). Operations Support Department Manager of the Hungarian Economic Development Agency Public Benefit Nonprofit Ltd. (MGFÜ, formerly IFKA); member of the WJLF Department of Environmental Security. Vice president of the Hungarian Meteoritic Society (MMT) and head of the Meteorite Craters and Impactites Section; secretary general and member of the Board of the Scientific Journalists' Club (TÚK); member of the Hungarian Association of Military Science and its Geoinformation Section. Founder and editor-in-chief of the planetary science portal Planetology.hu; author of the Rezsabek Nándor ScienceBlog.

A szerző, REZSABEK N. (1972–) okleveles geográfus (erőforrás- és kockázatelemző specializáció) (MSc); alkalmazott környezetkutató (környezetbiztonsági menedzser specializáció) (BSc); szervező üzemmérnök (BSc); a Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola hallgatója (PhD). A Magyar Gazdaságfejlesztési Ügynökség Közhasznú Nonprofit Kft. (MGFÜ, korábban IFKA) működéstámogató osztályvezetője; a WJLF Környezetbiztonsági Tanszékének munkatársa. A Magyar Meteoritikai Társaság (MMT) alelnöke, illetve Meteoritkráterek és Impaktitok tagozatának vezetője; a Tudományos Újságírók Klubjának (TÚK) főtitkára, illetve elnökségi tagja; a Magyar Hadtudományi Társaság és Geoinformációs Szakosztályának tagja. A Planetology.hu bolygótudományi portál alapító-főszerkesztője; a Rezsabek Nándor ScienceBlog szerzője.

**SIMON Mátyás**

matyas.simon86@gmail.com

I graduated from the Faculty of Natural Sciences of the University of Pécs in 2011 as a graduate environmental researcher, and from 2017 I also have the qualification of an environmental expert. Subsequently, I supplemented my studies with a secondary qualification in occupational safety and fire protection. In 2020, I also successfully completed the training of a senior occupational safety specialist at the Budapest University of Technology. I started my professional career at Semmelweis University in 2013 as an environmental lecturer, and then I was appointed head of department, deputy director, and is currently headed by the Semmelweis University Directorate of Security Technology. During my career so far, I have had the opportunity to gain extensive experience in the fields of environmental, work, fire, property protection and dangerous goods transport (ADR). I am currently pursuing my studies as a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda.

A Pécsi Tudományegyetem Természettudományi Karán végeztem 2011-ben, mint okleveles környezetkutató, 2017-től környezetvédelmi szakértői jogosultsággal is rendelkezem. Ezt követően tanulmányaimat középfokú munkavédelmi és tűzvédelmi szakképesítéssel egészítettem ki. 2020-ban a Budapesti Műszaki Egyetem felsőfokú munkavédelmi szakember képzését is sikeresen elvégeztem. A szakmai pályafutásomat 2013-ban a Semmelweis Egyetemen kezdtem meg környezetvédelmi előadóként, majd megbízást kaptam osztályvezető, igazgatóhelyettes pozícióra, jelenleg a Semmelweis Egyetem Biztonságtechnikai Igazgatóság vezetésével bíztak meg, mint igazgató. Eddigi pályafutásom során alkalmam volt széleskörű tapasztalatokat szerezni a környezet-, munka-, tűz-, vagyonvédelem és veszélyes áruszállítás (ADR) szakterületén. Tanulmányaimat jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatójaként folytatom.

## SZÉN István

szen.istvan@kvk.uni-obuda.hu

Electrical Engineer and Electrical Engineering Teacher. He is currently a PhD candidate at the Doctoral School on Safety and Security Sciences of Óbuda University, and serves as Deputy Head of the Department of Hydrogen Technologies and Industrial IoT Systems at the Kandó Kálmán Faculty of Electrical Engineering. His teaching and research activities focus on energy systems and hydrogen technologies. He actively participates in research and development projects and has contributed to the establishment of several professional organizations. He is a member of IEEE and the Hungarian Electrotechnical Association.

Villamosmérnök, villamosmérnök-mérnöktanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója, valamint a Kandó Kálmán Villamosmérnöki Karon működő Hidrogéntechnológiák és Ipari IoT Rendszerek Tanszék tanszékvezető-helyettese. Oktatási és kutatási területe az energetika és a hidrogéntechnológia. Aktívan részt vesz kutatás-fejlesztési projektekben, valamint több szakmai szervezet alapításában is közreműködött. Tagja a IEEE-nek és a Magyar Elektrotechnikai Egyesületnek.

## SZIJÁRTÓ Gábor

szijarto.gabor@phd.uni-obuda.hu

Gábor SZIJÁRTÓ is an electrical engineer, an assistant lecturer at the Kandó Kálmán Faculty of Electrical Engineering of Óbuda University, and a PhD student at the Doctoral School of Safety Sciences. He teaches "Energy Networks" and "Protection Against Electric Shock." He works at MVM Émász Áramhálózati Ltd. as a network strategy expert, primarily on substation and medium-voltage development projects. He holds design, technical management, technical inspection, and expert licenses (including lightning and surge protection). His industrial experience includes the electrical design and commissioning of gas-engine small power plants and the coordination of service work. He is a member of IEEE and the Hungarian Electrotechnical Association (MEE), a regular contributor to Elektroinstallateur (7 articles) and Villanyszerelők Lapja (21 articles), and co-author of the lightning and surge protection chapter in the "Handbook for Electrical Industry Professionals." He placed third in the Challenge.on engineering competition and in the MEE thesis competition.

SZIJÁRTÓ Gábor okleveles villamosmérnök, az Óbudai Egyetem Kandó Karának egyetemi tanársegédje, a Biztonságtudományi Doktori Iskola PhD-hallgatója. Az „Energia hálózatok" és az „Áramütés elleni védelem" tárgyakat oktatja. Az MVM Émász Áramhálózati Kft.-nél hálózati stratégiai szakértőként dolgozik főként alállomási és középfeszültségű fejlesztési projektekben. Tervezői, műszaki vezetői, műszaki ellenőri és szakértői jogosultságokkal rendelkezik (többek között villám- és túlfeszültség-védelem), ipari tapasztalata kiterjed gázmotoros kiserőművek villamos tervezésére és üzembe helyezésére, valamint szervizmunkák koordinálására. Az IEEE és a MEE tagja, az Elektroinstallateur (7 cikk) és a Villanyszerelők Lapja rendszeres szerzője (21 cikk), társszerző az „Elektromosipari szakemberek kézikönyve" villám- és túlfeszültség-védelem fejezetében, a Challenge.on mérnökverseny és a MEE szakdolgozat pályázat III. helyezettje.

## SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Endre SZŰCS (1963) PhD degree in military science, certified security engineer, mechanical engineer, engineering teacher. Currently, he is a doctoral supervisor and advisor at Óbuda University's Doctoral School on Safety and Security Sciences, Instructor of the course "Review and analysis of the history and events of security technology", and he is also a lecturer at the Institute of Mechanical Engineering and Technology and Institute of Safety Science and Cybersecurity at Óbuda University, Bánki Donát Faculty of Mec-

SZŰCS Endre (1963) a hadtudomány PhD fokozatosa, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető és témakiíró, „A biztonságtechnika történetének, eseményeinek áttekintése, elemzése" című tantárgyat oktató, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi és Kibervédelmi Intézet

hanical and Security Engineering. His research interests are "The possibilities of the use of renewable energy sources in safety and security technology", "Investigation of the history of safety and security technology".

óradója. Kutatási területe A megújuló energiaforrások alkalmazásának lehetőségei a biztonságtechnikában. A biztonságtechnika történetének vizsgálata.

**VIKTOR Patrik**

viktor.patrik@uni-obuda.hu

My name is Patrik VIKTOR. I am a lecturer and PhD student at Óbuda University. My doctoral research focuses on self-driving vehicle technology, with particular attention to the economic, technical, and social impacts. I study the role of artificial intelligence, sensor fusion, and reliability in the development of autonomous systems. Since August 2022, I have been teaching at the university, with the goal of providing students with modern, practice-oriented training and fostering their openness to new technologies. My degrees in technical management and economics allow me to combine engineering, economic, and educational perspectives. I have been actively involved in university life as a demonstrator and president of a professional college, and I have gained professional experience in fleet management and quality assurance. I have achieved success in several academic competitions and have presented at domestic conferences. I believe the future of transportation will be shaped by safe and sustainable autonomous systems, and I aim to contribute to this as both a researcher and lecturer.

VIKTOR Patrik vagyok. Az Óbudai Egyetem oktató és PhD-hallgató vagyok. Doktori kutatásom az önvezető járművek technológiájára irányul, különös tekintettel a gazdasági, műszaki és társadalmi hatásokra. Vizsgálom a mesterséges intelligencia, a szenzorfúzió és a megbízhatóság szerepét az önvezető rendszerek fejlesztésében. 2022 augusztusa óta tanítok az egyetemen, célom a hallgatók modern, gyakorlatias képzése és az új technológiákra való nyitottságuk erősítése. Végzettségeim műszaki menedzsment és közgazdaságtan területéről származnak, így mérnöki, gazdasági és oktatási szemléletet ötvözők. Aktívan részt vettem az egyetemi közösségben demonstrátorként és szakkollégiumi elnökként, szakmai tapasztalatot szereztem flottamenedzsmentben és minőségirányításban. Több tudományos versenyen értem el eredményeket és hazai konferenciákon tartottam előadásokat. Hiszem, hogy a jövő közlekedését a biztonságos, fenntartható autonóm rendszerek határozzák meg, ehhez szeretnék kutatóként és oktatóként hozzájárulni.

**WÜHRL Tibor**

wuhrl.tibor@kvk.uni-obuda.hu

Tibor WÜHRL is electrical engineer and associate professor at the Department of Telecommunications, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University. His teaching activities cover the fields of telecommunications, and digital signal processing. His research interests focus on modern telecommunication systems and advanced signal processing methods. In addition to his aca-demic work, he is engaged in certification in the field of railway control-command and signaling activities at the Institute for Transport Sciences.

WÜHRL Tibor okleveles villamosmérnök, egyetemi docens az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karának Híradástechnika Tanszékén. Oktatási tevékenysége a híradástechnika, tele-kommunikáció, digitális jelfeldolgozás területeire terjed ki. Kutatási témái a modern telekommunikációs rendszerekhez és a korszerű jelfeldolgozó eljárásokhoz kapcsolódnak. Egyetemi munkája mellett a Közlekedéstudományi Intézetben tanúsítási tevékenységet végez a vasúti ellenőrző-irányító és jelző szakterületen.

| 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 |

**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 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.

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 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 7, No 3, 2025.** | **2025. VII. évf. 3. szám**

## CONTENT | TARTALOM

| 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 in General column | Munkabiztonság rovat

DOI: https://doi.org/10.12700/btsz.2025.7.3.1

# A HISTORICAL OVERVIEW OF BATTLEFIELD WOUNDED CARE IN THE LIGHT OF TODAY'S MODERN TOOLS

# A HARCTÉRI SEBESÜLTELLÁTÁS TÖRTÉNETI ÁTTEKINTÉSE NAPJAINK MODERN ESZKÖZEINEK TÜKRÉBEN

MORVAY László[1] – SZŰCS Endre[2]

**Abstract**

Every major military conflict has contributed to the advancement of wound treatment techniques and equipment. From the primitive surgical interventions of ancient times to the advanced medical procedures used in modern warfare, numerous innovations have emerged that have improved the survival chances of the wounded. In the modern era, technological innovations have revolutionized casualty care. Portable ultrasound and CT devices have made it possible to diagnose injuries quickly and accurately, even under battlefield conditions. The use of robotics and telemedicine has further increased the effectiveness of treatments. Innovative tools aimed at reducing blood loss and stabilizing injuries have significantly improved survival rates. This study, following these lines of development, presents how lessons from the past have contributed to today's technological innovations, and how future advancements may impact military medical care.

**Keywords**

phased battlefield casualty care, portable diagnostic devices, non-invasive therapies, LLLT, ultrasound therapy, electrotherapy

**Absztrakt**

Minden jelentős katonai konfliktus hozzájárult a sebellátási technikák és eszközök fejlődéséhez. Az ókori primitív sebészi beavatkozásoktól a legújabb kori háborúk során használt fejlett orvosi eljárásokig számos innováció született, amelyek a sebesültek túlélési esélyeit javították. A modern korban a technológiai újítások forradalmasították a sebesültellátást. A hordozható ultrahang- és CT-berendezések lehetővé tették a sérülések gyors és pontos diagnosztizálását, még harctéri körülmények között is. A robotika és a telemedicina alkalmazása tovább növelte a kezelések hatékonyságát. A vérveszteség csökkentésére és a sérülések stabilizálására használt szorító kötések és vérzéscsillapító szerek jelentős mértékben javították a túlélési arányt. A jelen tanulmány ezen fejlődési vonalak mentén haladva mutatja be, hogy a múlt tanulságai hogyan járultak hozzá a jelenkor technológiai újításaihoz, illetve a jövőbeli fejlesztések milyen hatást gyakorolhatnak a katonai orvosi ellátásra.

**Kulcsszavak**

szakaszos harctéri sebesültellátás, hordozható diagnosztikai eszközök, nem invazív terápiák, lágylézer terápia, ultrahang terápia, elektroterápia

[1] morvay.laszlo@phd.uni-obuda.hu | ORCID: 0009-0004-2064-8856 | doctoral student, Óbudai University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X | senior lecturer, Óbudai University Doctoral School on Safety and Security Sciences | egyetemi oktató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

## INTRODUCTION

Battlefield casualty care has played a vital role in the success of military operations for centuries. In modern warfare, the immediate treatment of injuries and the rapid evacuation of the wounded have a direct impact on the efficiency and morale of military units. Providing timely and context-appropriate medical care significantly increases survival rates, reduces the number of battlefield fatalities, and improves long-term health outcomes. The development of battlefield medical care has been a major military and scientific challenge in every significant war. Innovations such as the use of disinfectants, anaesthesia, portable medical equipment, and basic first aid have brought fundamental changes. On today's battlefield, telemedicine, drone-based transport, and AI-powered diagnostic systems have further revolutionized casualty care, enabling military medical personnel to treat the wounded more effectively.

The aim of the present research is to provide an overview of the historical development of battlefield casualty care and to demonstrate how modern technological advances have improved the survival chances of the injured and the overall efficiency of medical treatment. The study explores how historical contexts interact with modern medical technologies and how past experiences influence current practices. It also analyses to what extent technological innovations, such as portable therapeutic devices, have transformed casualty care and impacted soldiers' chances of survival. This topic is particularly relevant today, as modern warfare presents new challenges to medical practice. Asymmetric conflicts, the evolution of military technology, and varying battlefield conditions demand new and unique solutions. Moreover, developments in military medical science may also benefit civilian disaster response and emergency medical services.

## MATERIALS AND METHODS

For the writing of this publication, a secondary research method was applied. This involved systematically organizing and reanalysing existing data, including relevant academic literature, publications, records, and online journals related to the topic. Throughout the research process, particular attention was paid to ensuring that the sources used were verifiable, reliable, and accurate. The secondary literature review was concluded on November 5, 2024, at which time all downloaded materials were accessible online.

## THE HISTORICAL DEVELOPMENT OF BATTLEFIELD CASUALTY CARE

The treatment of injuries sustained during combat has a history spanning thousands of years, with the methods used in each era reflecting the level of technological advancement in weaponry, transportation capabilities, the effectiveness of disinfection procedures, and the development of surgical techniques.

### Wound Treatment in Antiquity

The ancient Egyptians employed wound treatment methods that can be considered precursors to modern disinfection principles. To clean wounds, they used wine and seawater. The alcohol in wine aided in cleansing the wound, while the salt content of seawater accelerated wound contraction. Based on their observations, they realized that purulent wounds needed to be drained. Rather than closing discharging wounds, they treated them

with a mixture of honey, fat, and plant fibres. As shown in *Figure 1*, wounds were covered with linen or woollen fabrics, which helped prevent contamination and reduced the risk of infection. Egyptian physicians and priests developed their healing techniques based on practical experience and documented them in writing in the collection known as the *Ebers Papyrus*, which served as the primary source of medical knowledge of the time. [1]

*1.Figure: Ancient Egyptian bandage [1, 27.p.]*

According to ancient papyri, the Egyptians between 3000 and 2000 BCE were familiar with approximately 700 medicinal substances, and by 1500 BCE this number had risen to 876. Of the 349 drugs used between 1850 and 1350 BCE, around 70% were still in use at the end of the 20th century, and several are still being manufactured today. [1]

*2. Figure: Depiction of surgical instruments on the wall of the temple at Kom Ombo [1, 28.o.]*

Depictions from ancient Egypt also confirm the presence of surgical practices. As shown in *Figure 2*, a stone carving on the wall of the temple in Kom Ombo illustrates tools that bear a remarkable resemblance to modern surgical instruments. [1]

In ancient Egypt, healing was closely intertwined with religion. Their medical practices often reflected the constant struggle between demons and gods, which was a central theme in their worldview. [1]


*3. Figure: Red figure aryball 480-470 BC [3, Figure 1.]*

The earliest known reference to wound treatment in ancient Greece is found in Homer's Iliad, written around 700 BCE, which recounts the Trojan War that took place roughly 500 years earlier. In addition to traditional long-range weapons like the bow, the opposing armies engaged in close combat using spears (dory), swords (xiphos), and sabers (kopis), often inflicting severe injuries. [2]

In Book IV of the Iliad, a surgeon named Machaon extracted an arrow from the abdomen of the Spartan king Menelaus, sucked out the poison from the wound, and applied medicinal ointments. In Book XI, Achilles' friend Patroclus cut out an arrow from the thigh of Eurypylus, king of Thessaly, washed the blood with warm water, and applied healing balms. One of the longest-standing principles of wound treatment, which remained influential for centuries, comes from the works of Hippocrates (ca. 460–377 BCE). His writings introduced key innovations such as chest tubes for draining bodily fluids, external fixation for properly aligning broken bones, and important observations on head injuries. Hippocrates believed that wounds should be kept dry, irrigated only with clean water or wine, and that suppuration (pus formation) was a natural part of healing, helping to expel "corrupted" blood. [2]

*Figure 3* features a small red-figure vase dated around 480–470 BCE, depicting outpatient care in ancient Greece. In image "A," a physician is treating a patient. The young doctor is making an incision in the right arm vein of a standing man using a lance. The man leans on a stick and watches the procedure with a frightened expression. [3]

## Casualty Care in Medieval Europe and Hungary

*4. Figure: Medieval barber surgeon during surgery [5]*

During the Middle Ages, physicians held a higher social status than surgeons, which meant that scientific writings on wound treatment were scarce. Nevertheless, the surgeon Guy de Chauliac (1298–1368) recorded five foundational principles of wound care: the prompt removal of foreign objects, the reunification of damaged tissues, the preservation of tissue continuity, the conservation of bodily materials, and the prevention of complications. Projectiles from firearms caused severe tissue destruction and, passing through the heavily contaminated clothing of soldiers, introduced pathogens into wounds, leading to serious infections. Since contemporary healers were unaware of bacteria, they poured boiling oil into wounds to destroy what they assumed were poisons from black powder. However, during the Siege of Turin in 1536, the French surgeon Ambroise Paré achieved remarkable anti-inflammatory success using an alternative ointment made of egg yolk, rose oil, and turpentine in the absence of hot oil. [2]

In Hungary, battlefield casualty care remained an unresolved issue for centuries. Historical records credit Tamás Esze with being the first to articulate the need for treating injured and disabled soldiers on the battlefield and for employing military physicians. In Europe and Hungary, organized care for war invalids began with the French in 1674, followed by the Habsburgs in 1692. Prior to this, military science made no mention of tactics for mass casualty care, logistics, or sustained medical support. Though these aspects were absent from theoretical officer training, their importance became immediately evident in battlefield practice. During campaigns or sieges, barber-surgeons, such as those shown working in *Figure 4*, were contracted to serve the army for a specified duration, number, and salary. These barber-surgeons provided their own surgical instruments, medicines, and dressings, which they brought to the battlefield. At the time, the roles and duties of barbers and surgeons were still distinct, but as anatomical knowledge advanced, surgery became linked to internal medicine. With the subsequent boom in medical education and the constant state of warfare, both technical and mechanical development accelerated. As previ-

ously mentioned, Ambroise Paré (1510–1590), serving as a military surgeon, designed functional limb prostheses and palatal replacements made from precious metals. By the 17th century, surgical advances were largely driven by military medicine, especially in the treatment of burns and gunshot wounds. [4]

**Innovations of the Great Wars**

*5. Figure: Minié projectile [6]*

During the American Civil War, the Minié ball, which emerged in the 1850s and is shown in *Figure 5*, caused such devastating injuries that abdominal and thoracic gunshot wounds had a mortality rate of 87%. [2]

The nature of a gunshot wound is influenced by the characteristics of the projectile, the direction of the shot, and the shooting distance. Anatomically, a gunshot wound is divided into three parts: the entry wound, often featuring burn marks from close-range shots; the bullet track, the internal path taken by the projectile; and the exit wound, which may not always be present. Determining the bullet track helps identify internal damage, locate the lodged projectile, and facilitate its removal. [7]

At the start of the Civil War, gunshot wounds were treated primarily with cauterization and tourniquets. Over time, practical experience led to the widespread use of pressure dressings, which significantly reduced primary haemorrhage. However, due to secondary bleeding occurring on the third or fourth day, the mortality rate remained above 62%. [2]

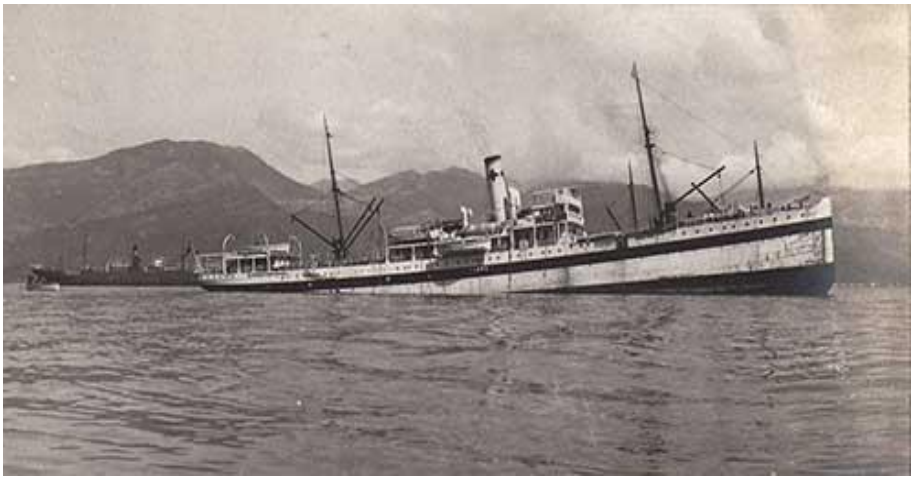
*6. Figure: Wounded people waiting to be loaded into wagons [8]*

In World War I, femoral fractures had a mortality rate exceeding 80%, which was reduced to 20% through immediate external splinting and immobilization. Medical personnel were trained to perform procedures blindfolded, enabling treatment in the dark or low-visibility conditions. Surgeons also discovered the benefits of delayed wound closure; they would take swabs from the wound and base the decision to close it on the presence of pathogens. Triage systems were used to classify the wounded based on injury severity. [2] As seen in *Figure 6*, severely wounded soldiers were gathered and evacuated by road, rail, or ship to military hospitals farther from the combat zone.

In the Austro-Hungarian Empire, medical trains and hospital ships were introduced to speed up treatment. Hospital trains were designated for the severely injured, while transport carriages, such as those in *Figure 7*, were used for lighter cases. By March 1915, 128 mobile medical rail units were in operation, increasing to 151 by the end of the war in 1918. These units had a combined capacity of 39,334 beds, and nearly 8 million wounded soldiers were transported during the conflict. [9]

In the First World War, the three best-known hospital ships of the Austro-Hungarian Monarchy were the 3199-ton Elektra, launched in 1884 and accommodating 355 wounded, the 879-ton Metkovich, commissioned in 1893, capable of caring for 135 wounded, and the 2836-ton steamers Tirol, completed in 1901, which provided accommodation for 300 wounded, shown in *Figure 8*. In addition to the naval staff doctor serving as military commander, the ships were staffed by a field chaplain, a naval officer, three non-commissioned officers and 6-12 nurses. [10]

*7. Figure: Medical train at Villach, 1916 [9]*



*8. Figure: The Tirol hospital ship that hit a mine [10]*

In World War II, American surgeon Edward D. Churchill (1895–1972) developed a wound closure approach based on the wound's appearance. In 1944 in northern Italy, he closed 25,000 soft tissue wounds where tissue appeared healthy and free of debris or oedema, achieving a 5% mortality rate. [2]

During the Korean War (1950–1953), frontline surgeons used compression dressings to stop bleeding and resorted to tourniquets only when necessary. If immediate evacuation was impossible, they began antibiotic therapy and blood transfusions on site. [2]

In the Vietnam War, American forces encountered complex, multiple injuries caused by AK-47s, SKS rifles, and explosive traps used by North Vietnamese and Viet Cong troops. Due to combat conditions, it was rare for the wounded to receive surgical treatment within 1–2 hours; the average evacuation time was 4–6 hours. In such cases, patients were given Ringer's lactate to counter blood loss and began antibiotic therapy. Wounds were cleaned, irrigated, and dressed. In field hospitals, vascular and orthopaedic surgeons treated the injured. Fractures were managed through bone alignment, traction, or plastering. [2]

In Iraq and Afghanistan, suicide bombers and improvised explosive devices (IEDs) changed the nature of warfare. These caused extensive and complex tissue damage, often necessitating limb amputations. In many cases, resuscitation began on-site and continued during aerial or ground evacuation. [2]

**Phased Battlefield Casualty Care**

According to the principle of phased care, wounded soldiers on the battlefield are treated in stages, based on the severity and location of their injuries. The first phase of care is battlefield first aid, provided either by the injured soldier themselves (self-aid) or by fellow soldiers (buddy aid) using a standardized personal first aid kit. This kit typically includes sterile dressings, bandages, pressure dressings, a Velcro tourniquet, adhesive bandages, tape, nasal and mouth masks, scissors, tweezers, and a user manual. [11]

*9. Figure: The tools of the field surgeon [12]*

The second level of care - referred to as advanced buddy aid - is provided at a relatively safe area near the frontline. Here, a better-trained soldier equipped with more advanced medical tools stabilizes the wounded before they are transported to higher-level treatment facilities. [11] *Figure 9* shows the tools used by a field surgeon at this stage.

Beyond basic first aid, treatment continues at increasingly advanced echelons of care, defined as:

- ROLE 1: Medical aid post
- ROLE 2: First field hospital
- ROLE 3: Civilian or military hospital in the operational area
- ROLE 4: Specialized hospital in the home country or rear area [11]

**The Role of Modern Rehabilitation Devices in Phased Battlefield Casualty Care**

The primary objective of battlefield casualty care is the rapid rehabilitation of injured soldiers, so they can return to duty and continue combat operations. [11] Following traditional wound dressing or surgical treatment, electrotherapy, low-level laser therapy (LLLT), and ultrasound therapy are recommended rehabilitation methods across all echelons of care of ROLE 1 through ROLE 4.

*Electrotherapy* is a therapeutic technique that uses electric currents to treat various diseases, relieve pain and injuries, and regenerate tissue. Widely used in physiotherapy and rehabilitation, this method enhances cellular function through controlled electrical impulses that stimulate healing processes. [13] *Figure 10* depicts a modern electrotherapy device.

Electrotherapy supports pain relief, nerve and muscle stimulation, reduced inflammation, and improved blood circulation. Its non-invasive nature makes it an appealing alternative to drug therapy, reducing side effects and accelerating recovery. The microvolt (μV) and millivolt (mV) ranges used ensure gentle, regulated effects on cells, minimizing the risk of tissue damage. [13]


*10. Figure: PhySys SD electrotherapy device (author's own photo)*

This therapy enhances cell metabolism, oxygen uptake, and nutrient absorption, while optimizing membrane potential and promoting neural communication. Controlled muscle stimulation also supports rehabilitation of weakened or injured muscles, improving mobility, tissue regeneration, and preventing muscle atrophy due to inactivity. [13]

*11. Figure: Modern soft laser therapy device [author's own photo]*

*LLLT, or soft laser therapy*, is a low-energy laser treatment used to stimulate cellular regeneration, relieve pain, and reduce inflammation in damaged tissues. During treatment, low-intensity laser light penetrates the tissue, energizing cells and supporting healing processes. [14] *Figure 11* depicts a modern electrotherapy device.

Commonly applied for musculoskeletal issues, inflammation, and pain, LLLT uses light wavelengths of 810 nm and 980 nm, which effectively reach deep tissue layers. The 810 nm wavelength penetrates muscles and ligaments, reducing inflammation and pain,

while 980 nm light stimulates blood flow, enhancing regeneration and nutrient delivery. Benefits of LLLT include faster tissue healing, pain reduction, and improved joint mobility. It enhances cell metabolism and oxygen intake, which helps restore function to injured areas. Because it naturally supports the body's healing processes, it contributes to both symptomatic relief and long-term recovery. [14]


*12. Figure: Modern ultrasound therapy device [author's own photo]*

*Ultrasound* began to be used in medicine in 1938 and has since been used in many medical fields, including diagnostic, surgical and therapeutic purposes. It is a form of medical treatment in which human tissues are stimulated with high-frequency sound waves, which promotes healing processes and reduces pain. Its purpose is to stimulate blood circulation and metabolism by penetrating into the deeper layers of tissues, which contributes to cell regeneration, reducing inflammation and relaxing muscles. *Figure 12* shows a modern ultrasound therapy device. Ultrasound waves with a frequency of 0.8 to 2.4 MHz are particularly suitable for penetrating deep into muscle and joint tissues. The lower frequency waves (0.8 MHz) penetrate deeper layers, so they exert their healing effect on the deep areas of the joints and muscles, while the higher frequencies (2.4 MHz) affect the surface tissues. During therapy, sound waves create microscopic massage movements between cells, which increase the oxygen supply and nutrient uptake of cells and help to remove waste products accumulated there. The heat effect created by ultrasound relaxes the muscles, reduces pain and increases the flexibility of the affected areas. [13]

In the case of ultrasound treatments, a triple energy transformation occurs: the electrical energy in the ultrasound hand head is converted into mechanical energy, and then it becomes thermal energy when it enters the human tissue. With the help of the artificially produced polycrystalline ceramic material of the ultrasonic heads, the treatment unit converts electrical energy into mechanical energy. The energy emitted is a longitudinal mechanical wave, where the alternating condensation and rarefaction of the particles of matter in the direction of sound propagation occurs. When two different tissues reach the border,

some of the ultrasound waves are reflected and only the other part penetrates the new medium, this is called interface reflection. At the border of muscle and bone tissue, the degree of reflection can reach 30%. The effect induced by ultrasound irradiation is based on the absorption capacity of the tissues. As a result of absorption, the ultrasonic intensity used on the tissue surface, measured in $W/cm^2$, decreases exponentially with depth in the direction of propagation. As the depth decreases, the frequency values also change. In human tissues, ultrasound acts both superficially and deeply. It exerts its beneficial biological effects at a depth of 8 cm, the half-life layer is 4 cm. Due to the absorptions, the intensity of radiation is reduced by half between 4 and 8 cm. Compared to the energy absorption capacity of muscle tissue, fat tissue absorbs half as much, ligaments and tendon tissue absorb four times as much, and bone tissue absorbs ten times as much energy. The more energy a tissue absorbs, the more it heats up. The order of tissue warming: bones, tendons and ligaments heat up the most, followed by nerves, muscles, skin, internal organs and least of all adipose tissue. [13]

In the phased battlefield casualty care system, electrotherapy, low-level laser therapy, and ultrasound therapy are most effectively used at the echelon of care highlighted in yellow in Table 1.

| Level | PHASED BATTLEFIELD CASUALTY CARE LEVELS | | | Required competency |
|---|---|---|---|---|
| | Designation / Location | | Content | |
| | Battlefield | **Battlefield First Aid** | first aid<br>Self-aid or buddy aid using a standardized first aid kit (sterile dressings, bandages, pressure dressing, tourniquet, etc.) | |
| | Battlefield<br>in a safe location further away from the forward edge of the battle-area | **first special help** | first aid<br>medically trained personnel using basic medical tools | |
| | theatre of operations<br>further away from the forward edge of the battle-area<br>first medical aid station | **ROLE 1** | specialist (surgeon, orthopaedist) | |
| | theatre of operations,<br>further away from the forward edge of the battle-area<br>first field hospital | **ROLE 2** | Emergency traumatology care<br>Modular healthcare facility | |
| | theatre of operations,<br>further away from the forward edge of the battle-area<br>civil- or military hospital | **ROLE 3** | triage and emergency care, outpatient care, inpatient care, pharmacy, clinical laboratory, blood bank, radiology, physiotherapy, medical logistics, operative dental care (emergency and basic), oral and maxillofacial surgery, nutritional care, patient administration services. | |
| | hospital in the hinterland | **ROLE 4** | General hospital care | |

*Table 1. Phased Battlefield Casualty Care (own compilation based on referenceses [11] and [12])*

## CONCLUSIONS AND SUMMARY

The use of electrotherapy, low-level laser therapy (LLLT), and ultrasound therapy is well justified in battlefield casualty care, where rapid and effective methods are essential for treating injured soldiers. Due to their tissue-regenerating and anti-inflammatory effects, these modalities support the treatment of injuries such as muscle damage, dislocations, surgical wounds, and oedemas, which are common in combat environments.

Modern therapeutic devices are now available in compact and portable forms, making it feasible to apply these treatments even in field conditions. This significantly contributes to faster and more efficient care for battlefield casualties, which is critical to avoid further complications and ensure that soldiers can return to duty as soon as possible.

As non-invasive treatment options, these therapies often serve as effective alternatives to pharmacological interventions, especially in field settings where access to medications may be limited. The combined use of these three therapeutic methods offers a fast, efficient, and natural-healing-supportive approach, which is particularly advantageous for mobile and field-based medical services.

## REFERENCES

[1] Szabóné Révész, E.: Sebkezelés az ókori Egyiptomban. Kaleidoscope Művelődés-, Tudomány- és Orvostörténeti Folyóirat, 2022. Vol. 12. No. 24., ISSN 2062-2597, DOI: 10.17107/KH.2022.24.24-34

[2] M. M. Manring et al.: Treatment of War Wounds. Clinical Orthopaedics and Related Research, Vol. 467, No. 8, August 2009, pp. 2168-2191, DOI 10.1007/s11999-009-0738-5

[3] G. Samonis et al.: Outpatient Clinic in Ancient Greece. Maedica, 2021 Dec;16(4):700–706. doi: 10.26574/maedica.2020.16.4.700, PMCID: PMC8897778 PMID: 35261674

[4] Kincses, Katalin Mária (2005) A hadi sebesültellátás kérdései Magyarországon (XVI. század - XVIII. század eleje). In: Az értelem bátorsága. Tanulmányok Perjés Géza emlékére. Argumentum, Budapest, pp. 359-386. ISBN 963 446 329 0

[5] Diósi, Sz.: Ők műtöttek a középkorban: a gyógyító szerzetesek nem vállalták a véres beavatkozásokat. https://divany.hu/vilagom/kozepkor-mutet/ (Downloaded: 29.10.2024.)

[6] .58 kaliberű unionista Minié-lövedék a Gettysburgi-csata helyszínéről. [Online]. Available: https://www.worthpoint.com/worthopedia/58-caliber-union-minnie-ball-bullet-3888407397 (Downloaded: 29.10.2024.)

[7] Szemerédi, V.: Nyílt, mechanikus sebek tünetei és kezelése. Published: 23.09.2006. Revised: 28.02.2018. [Online]. Available: https://www.hazipatika.com/betegsegek_a_z/nyilt_mechanikus_sebek (Downloaded: 10.29.2024.)

[8] Harctéri sebesült ellátás. [Online]. Available: https://www.kvmkl.hu/kiallitasvezeto/sebesult-ellatas-a-fronton (Downloaded: 10.29.2024.)

[9] Kiss, G.: Vasúti egészségügyi vonatok az osztrák–magyar haderőben. Published: 28.04.2017. [Online]. Available: https://nagyhaboru.blog.hu/2017/04/28/vasuti_egeszsegugyi_vonatok_az_osztrak_magyar_haderoben (Downloaded: 10.29.2024.)

[10] Kiss, G.: Kórházhajók az Adrián. Published: 09.05.2024. [Online]. Available:

https://nagyhaboru.blog.hu/2024/05/09/korhazhajok_az_adrian (Downloaded: 31.10.2024.)
[11] Pápai, T.: A harctéri elsősegélynyújtás helye a hadszíntéri ellátásban és annak oktatás módszertani irányvonalai. Hadmérnök, Vol. VI. No. 4. December 2011, pp. 111-120., ISSN 1788-1929
[12] Meixner, Z.: Így működnek a frontkórházak. Published: 28.02.2022. Revised: 10.08.2022. [Online]. Available: https://www.hazipatika.com/napi_egeszseg/egeszsegugy/cikkek/igy_mukodnek_a_frontkorhazak (Downloaded: 05.11.2024.)
[13] Diricziné, B.Gy.: Elméleti és gyakorlati fizioterápia. Kádix, Budapest, 2013, 330 pages · ISBN: 9789638901545
[14] Sandra S.: Lágylézer terápia I. San-Ergonómia Kft, Budapest, 2016, ISBN 978-963-12-5067-1

DOI: https://doi.org/10.12700/btsz.2025.7.3.15

# CYBERSECURITY PROFILES AMONG GENERATION Z AND ALPHA

# KIBERBIZTONSÁGI PROFILOK A Z ÉS ALFA GENERÁCIÓ KÖRÉBEN

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

**Abstract**

Due to the increased online presence of Gen Z and Alpha, their cybersecurity awareness is a critical social issue. The aim of this research was to assess the cybersecurity awareness of Gen Z and Alpha, identify influencing factors, and uncover user profiles. The study employed a quantitative survey methodology with a sample of 3275 young individuals from Fejér County, Hungary. Data were analyzed using descriptive and inferential statistics, alongside K-means cluster analysis. Results indicated no significant difference in overall awareness levels between the generations. Average daily internet usage was found to be negatively correlated with awareness. Cluster analysis identified five distinct profiles: "Proactive Protectors," "Average Users," "Technologically Confident," "Passively Cautious," and "Vulnerable Novices." Higher parental educational attainment was significantly associated with membership in more aware profiles. Cybersecurity awareness exhibits complex patterns. The identified profiles allow for the development of targeted prevention strategies to address the specific risks of each group.

**Keywords**

cybersecurity awareness, user profiles, Generation Z, Generation Alpha

**Absztrakt**

A Z és Alfa generációk fokozott online jelenléte miatt kiberbiztonsági tudatosságuk kritikus társadalmi kérdés. A kutatás célja a Z és Alfa generációk kiberbiztonsági tudatosságának felmérése, a befolyásoló tényezők azonosítása és felhasználói profilok feltárása volt. Kvantitatív kérdőíves vizsgálatban 3275 Fejér vármegyei fiatal vett részt. Az adatokat leíró és következtető statisztikai módszerekkel és K-means klaszteranalízissel elemeztük. Az eredmények alapján generációk között nem volt szignifikáns különbség az átlagos tudatossági szintben. Az átlagos napi internethasználat negatívan korrelált a tudatossággal. A klaszteranalízis öt profilt tárt fel: Proaktív védelmezők, Átlagfelhasználók, Technológiai magabiztosak, Passzív óvatosak és Sebezhető kezdők. A magasabb szülői iskolázottság tudatosabb profilokkal járt együtt. A kiberbiztonsági tudatosság komplex mintázatokat mutat. A feltárt profilok lehetővé teszik célzott prevenciós stratégiák kidolgozását az egyes csoportok specifikus kockázatainak kezelésére.

**Kulcsszavak**

kiberbiztonsági tudatosság, felhasználói profilok, Z generáció, Alfa generáció

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

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

## BEVEZETÉS

A kiberbiztonság kritikus szerepet tölt be a 21. században, ahol a globális kiberbiztonsági szakemberhiány súlyosan érinti a vállalkozásokat, ipari szektort, ahol a hiányos, nem megfelelő védelmi rendszerek lassabb reagálást és gyengébb megelőzést eredményeznek [1]. Az információbiztonság területén a technikai tudás mellett egyre fontosabbá válnak releváns puha készségek (problémamegoldás, kritikus gondolkodás és együttműködési készségek), amelyek nélkülözhetetlenek a növekvő komplexitású kiberbiztonsági kihívások kezeléséhez[2]. A jövő munkavállalóinak oktatási folyamatában kritikus fontosságú a digitális kompetenciák fejlesztése, amely magában foglalja a biztonsági attitűdök formálását és a puha készségek erősítését a digitális munkakörnyezet elvárásainak megfelelően[3]. Bár a fiatalabb generációk technológiailag jártasak, gyakran hiányzik belőlük a kiberbiztonsági tudatosság és a preventív viselkedési stratégiák alkalmazása[4]. Az Alfa generáció technológiai fejlettsége nem párosul megfelelő érzelmi érettséggel, és tapasztalatlanságuk, könnyű manipulálhatóságuk akadályozza a kiberbiztonsági kockázatok helyes értékelését. A Z és Alfa generáció korai internethasználata eltérő tanulási stílusokat és viselkedési mintákat alakít ki [5], valamint eltérő online kockázatvállalási attitűdöket és biztonsági tudatosságot eredményez. Az Alfa generáció specifikus információbiztonsági tudatosságára vonatkozó empirikus adatok hiánya indokolja generációspecifikus vizsgálatukat a kiberbiztonsági kutatásokban.

A kutatás célja a Z és Alfa generációk jellegzetes kiberbiztonsági profiljainak azonosítása, valamint ezen profilok demográfiai és viselkedési hátterének feltárása.
A kutatás három fő kérdésre keresi a választ:

- K1: Milyen alapvető különbségek azonosíthatók a Z és Alfa generációk internethasználati és biztonsági szokásaiban?
- K2: Mely demográfiai és pszicho-szociális tényezők magyarázzák leginkább az egyes generációk tudatossági szintjét?
- K3: Milyen csoportok és profilok alakíthatók ki a kiberbiztonsági tudatossági dimenziók és befolyásoló tényezők alapján?

## IRODALMI ÁTTEKINTÉS

Ez a fejezet röviden bemutatja a kiberbiztonsági tudatosság fogalmát és dimenzióit, áttekinti a Z és Alfa generáció digitális kompetenciáival kapcsolatos magyarországi kutatásokat, valamint elemzi a generációs különbségeket az online térhasználatban és a kapcsolódó kockázati tényezőket.

### A kiberbiztonsági tudatosság fogalma és dimenziói

A szakirodalomban a kibertérnek számos meghatározása olvasható. A kibertér (*cyberspace*) kifejezés eredete a görög „*kyber*” szóból származik, amelynek jelentése hajózni vagy navigálni[6]. Maga a fogalom nehezen definiálható, hiszen ez egy összetett és folyamatosan változó digitális ökoszisztéma, amelyben az emberek és eszközök a hálózatokon keresztül kommunikálnak és működnek. A fogalmat Magyarország Nemzeti Kiberbiztonsági Stratégiája (2013) is definiálja[7], mely szerint a kibertér globális, összekapcsolt elektronikus rendszerek hálózata, ahol adatok és információk áramlanak, a társadalmi és

gazdasági folyamatainkat érintően. Magyarország kibertere ennek a globális hálózatnak az a része, ami hazánkban található vagy minket érint.

A kiberbiztonság (*cybersecurity*) a számítógépes rendszerek, hálózatok, programok és adatok védelmét jelenti a digitális támadások, illetéktelen hozzáférések, károkozások és lopások ellen. A célja a digitális eszközök, rendszerek és a rajtuk tárolt információk bizalmasságának (*confidentiality*), sértetlenségének (*integrity*) és rendelkezésre állásának (*availability*) biztosítása (*CIA elv*).[8]

A kiberbiztonsági tudatosság (*cybersecurity awareness*) egyrészt a kibertér és annak veszélyeivel kapcsolatos tudást, az ismeretek szerzésének, megértésének és feldolgozásának képességét, valamint annak gyakorlati megvalósításának igényét jelenti[9]. A kiberbiztonsági tudatosság képzésének, fejlesztésének célja az egyének felelős magatartásának biztosítása a kiberbiztonság terén, így fontos megérteni, a tudatosság, az egyéni jellemzők és az oktatás összefüggéseit a magatartásra gyakorlat hatásának szempontjából[10].

**Generációs különbségek az online tér használatában, kockázati tényezők**

A digitális kompetenciák és a kiberbiztonsági tudatosság nemcsak egyéni, hanem generációs szinten is jelentősen eltérnek. A fiatalabb generációk digitális bennszülöttként szocializálódtak, így számukra az online tér természetes közegként funkcionál. Ezzel szemben az idősebb generációk számára a digitális környezet inkább tanult, tudatosan elsajátított világ, amelyhez gyakran kritikusabb attitűddel közelítenek[11].

Ez a különbség azonban nem csupán az eszközhasználat gyakoriságában, hanem a digitális viselkedés minőségében is megmutatkozik. Ribble [12] modellje szerint a digitális állampolgárság nem redukálható technikai készségekre, hanem magában foglalja az etikus viselkedést, a jogi tudatosságot és a biztonsági attitűdöket is. A fiatalabb generációk technikai jártassága gyakran nem párosul megfelelő kiberbiztonsági tudatossággal: a jelszavak védelme, az adatkezelés, a közösségi média beállításainak tudatos használata vagy a forráskritika alkalmazása sok esetben hiányos. Ribble hangsúlyozza, hogy a digitális írástudás fejlesztése során nem elegendő a technológiai eszközök használatának oktatása, hanem szükséges a digitális viselkedés normáinak és kockázatainak tudatosítása is.

A digitális szocializáció eltérő mintázatai szintén hozzájárulnak a generációs különbségekhez. Smith, Hewitt és Skrbiš[13] kutatása alapján a fiatalabb generációk számára az online tér nemcsak információforrás, hanem identitásformáló közeg is, amelyben a közösségi elismerés és a vizuális tartalmak dominanciája gyakran háttérbe szorítja a biztonsági szempontokat. Ez a fajta szocializációs dinamika hozzájárulhat ahhoz, hogy a fiatalabb felhasználók kevésbé érzékenyek a digitális kockázatokra, például az adathalászatra, a személyes adatok kiszolgáltatására vagy a manipulált tartalmak felismerésére.

Boghosian[14] ezzel összhangban rámutat arra, hogy a digitális írástudás és a kiberbiztonsági tudatosság nem csupán technikai, hanem demokratikus kompetenciák is. A szerző szerint a digitális higiénia, azaz az online viselkedés tudatossága, a forráskritika, a jelszókezelés és a digitális lábnyom kontrollja alapvető feltétele a demokratikus részvételnek. A generációs különbségek nemcsak a technológiahasználat módjában, hanem az információkhoz való viszonyulásban is megmutatkoznak: a fiatalabb generációk gyakran kevésbé képesek felismerni a dezinformációt, és hajlamosabbak az adatvédelmi kockázatok alábecsülésére.

A generációk eltérő erősségei komplementer kapcsolatban állnak: a fiatalabbak technikai és szociális kompetenciái, valamint az idősebbek szabálytudatossága és kockázatkerülése együttesen előnyös lehet. A fejlesztési stratégiáknak a technikai készségek mellett a generációk közötti tudásmegosztásra is kell fókuszálniuk egy olyan digitális kultúra kialakítására, amelyben a kompetencia és tudatosság egyensúlyban van.

## A KUTATÁS MÓDSZERTANA

A Fejér vármegyei Z és Alfa generáció kiberbiztonsági tudatosságának felmérésére kvantitatív módszertant alkalmaztunk. A deduktív logikán alapuló, leíró és hipotézis-tesztelő vizsgálat adatgyűjtési eszköze egy korábban adaptált és validált kiberbiztonsági tudatosság kérdőív volt.

### Mintavétel és adatgyűjtés folyamata

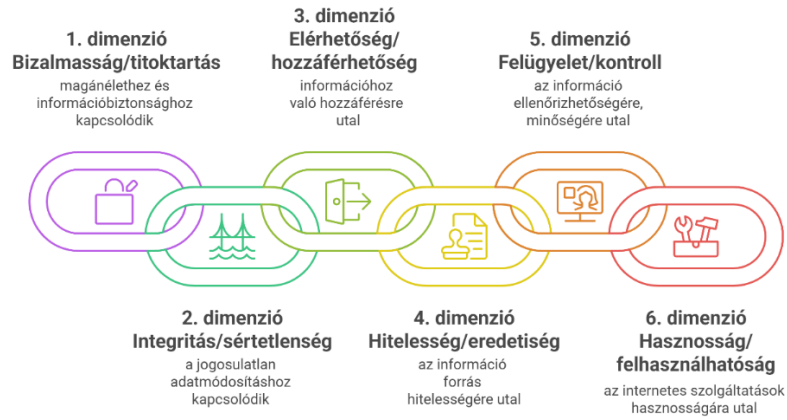
A résztvevők célzott kényelmi mintavétellel kerültek kiválasztásra. Az adatgyűjtés 2022 szeptembere és 2023 májusa között történt online és papíralapú kérdőívekkel. A kérdőíveket Fejér vármegye összes oktatási intézményéhez eljuttattuk, ahol pedagógusok és vezetők segítségével érték el a célcsoportot. A válaszadási arány intézményenként jelentősen változott (45 iskola, 1-444 válaszadó/iskola), ami korlátozhatja az általánosíthatóságot.

A részvétel önkéntes és anonim volt, etikai irányelveknek megfelelően. A résztvevők tájékozott beleegyezést adtak, az Alfa generáció tagjainál szülői hozzájárulással. A célcsoport a Z generáció (1995-2009) és az Alfa generáció (2010-2025, 5. évfolyamtól) tagjaiból állt. Az X és Y generáció tagjai, valamint a hiányos kitöltések kizárásra kerültek a 3473 fős mintából. Az adattisztítás során 198 kiugró értéket távolítottunk el. A végleges minta ($N$ = 3275) 74,4%-a Z generáció ($N$ = 2438), 25,6%-a Alfa generáció ($N$ = 837). A résztvevők 53,3%-a fiú ($N$ = 1746), 46,7%-a lány $N$ = 1529). Oktatási szintek szerint: általános iskola 37% ($N$ = 1215), középiskola 53% ($N$ = 1726), felsőoktatás 10% ($N$ = 334).

A minta Fejér vármegyei reprezentativitását $\chi^2$-próbákkal vizsgáltuk a KSH 2022-es referenciaadataival [15,16] összevetve. Nem találtunk szignifikáns eltérést a nemek arányában az általános iskolában ($\chi^2(1, N = 1215) = 1.40$, $p = .237$), a középiskolában ($\chi^2(1, N = 1726) = 1.25$, $p = .263$), és a 10-29 éves korcsoportban ($\chi^2(1, N = 3275) = 1.90$, $p = .168$). A generációs ($\chi^2(1, N = 3275) = 3.80$, $p = .051$), és a generációkon belüli nemi megoszlások is reprezentatívak voltak (Alfa: $\chi^2(1, N = 837) = 0.17$, $p = .680$, Z: $\chi^2(1, N = 2438) = 3.44$, $p = .064$). A felsőoktatásban azonban férfi dominancia mutatkozott ($\chi^2(1, N = 334) = 126.05$, $p < .001$), így ez az alcsoport nem reprezentatív. A kényelmi mintavétel miatt – a demográfiai illeszkedés ellenére is – az eredmények általánosíthatósága korlátozott.

### Kutatási eszköz és mérődimenziók

A végleges kérdőív az adaptált Kiberbiztonsági tudatosság kérdőív (CS-C-H)[17] tételeit, valamint demográfiai kérdéseket tartalmazott. A 25 kérdésből, 5 alskálából álló Cybersecurity Scale-t (CS-C) Arpaci és mtsai alkották meg 2021-ben[18]. A CS-C-H kérdőív a felhasználók kiberbiztonsági gyakorlatát és felfogását méri, valamint megfelelő validitással és megbízhatósággal rendelkezik[19]. A teljes skála Cronbach-alfa értéke .836, és a hat alskála belső konzisztenciája ($.621 < \alpha < .795$). A kérdőív hat dimenzión keresztül (1. ábra) vizsgálja a felhasználók kiberbiztonsággal kapcsolatos gyakorlatát, tudását és tudatosságát.




*1. Ábra: A Kiberbiztonsági tudatosság kérdőívhez tartozó dimenziók [forrás: saját szerkesztés]*

### Adatfeldolgozás és elemzés

A kvantitatív adatok kódolására, tisztítására és feldolgozására az SPSS 27, Excel és Python 3.11.13 szoftverkörnyezetek kerültek alkalmazásra. Az adatelemzés leíró statisztikákat (átlag, szórás), Pearson-korrelációt, lineáris regressziót, megbízhatósági vizsgálatot (Cronbach's α) tartalmazott. A közvetítő hatások mediációs útelemzéssel kerültek vizsgálatra. A csoportok közötti különbségek vizsgálatára a változók típusától függően különböző teszteket alkalmaztunk: két független csoport esetén független mintás t-próbát, nem normális eloszlás esetén Mann-Whitney U tesztet, több csoport összehasonlítására ANOVA, illetve nem parametrikus esetben Kruskal-Wallis H tesztet. Kategorikus változók esetén $\chi^2$-próbát használtunk. Homogén alcsoportok azonosítására K-means klaszterelemzést végeztünk. A statisztikai szignifikancia szintje $p < 0,05$.[20]

## KUTATÁSI EREDMÉNYEK

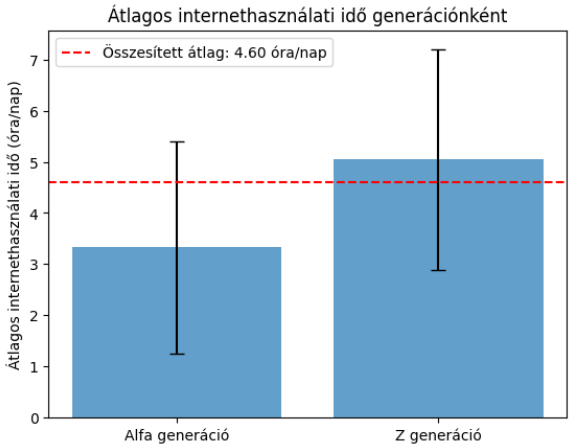
Ez a fejezet a kvantitatív elemzések eredményeit mutatja be. Először a leíró statisztikákat és korrelációkat ismertetjük, majd az alcsoportok közötti különbségeket vizsgáljuk. Ezt követően a kiberbiztonsági tudatosságot befolyásoló tényezők regressziós modelljeit, végül a biztonságtudatosság, attitűdök és viselkedésmintázatok alapján képzett klasztereket mutatjuk be.

### Leíró statisztika és korreláció

A vizsgálati minta 3275 főt tartalmaz, ebből 837 fő (25,6%) az Alfa generációhoz (10-14 év), 2438 fő (74,4%) a Z generációhoz (15-29 év) tartozik. A nemek eloszlása: 1746 férfi (53,3%) és 1529 nő (46,7%). Lakóhely szerint a városi lakosok a legnagyobb csoportot alkotják ($N = 1220$, 37,3%), ezt követik a kistelepülési lakóhelyűek ($N = 1178$, 36%) és a megyeszékhelyi lakosok ($N = 819$, 25%). A budapesti válaszadók aránya alacsony ($N = 58$, 1,8%). A szülők legmagasabb iskolai végzettsége alapján a felsőfokú végzettségűek dominálnak ($N = 1515$, 46%), ezt követi az érettségizettek aránya ($N = 1212$, 37%), a szakmunkás végzettségűek ($N = 447$, 14%) és az általános iskolai végzettségűek $N = 101$, 3,1%).

A résztvevők átlagosan 4,6 órát ($SD = 2,27$) töltöttek naponta internetezéssel. A Z generáció szignifikánsan több időt töltött online, mint az Alfa generáció ($U = 579609,000$,

$p < ,001$; $r_s = .338$, $p < ,01$) (2. ábra). Az Alfa generáció átlagosan 3,33 ± 2,08, a Z generáció 5,05 ± 2,16 órát internetezett naponta. Az Alfa generációban az iskolatípus szignifikánsan befolyásolta az internethasználat idejét ($\chi^2(1, N = 837) = 8{,}81$, $p = ,003$), a 6-8 osztályos gimnáziumi tanulók több időt töltöttek online. A nem, lakóhely és szülői iskolai végzettség nem mutatott szignifikáns kapcsolatot az internethasználat mértékével.




*2. Ábra: Átlagos napi internethasználati idő generációnként [forrás: saját szerkesztés]*

A Z generációnál a napi internethasználattal több demográfiai változó is szignifikáns, bár gyenge kapcsolatot mutatott. A nők többet interneteztek, mint a férfiak ($U = 695566{,}00$, $p = ,011$). Szignifikáns különbségek mutatkoztak az iskolatípus ($\chi^2(2, N = 2438) = 56{,}19$, $p < ,001$), szakirány ($\chi^2(2, N = 2438) = 60{,}80$, $p < ,001$), tudományterület ($\chi^2(5, N = 2438) = 72{,}43$, $p < ,001$) és a szülői iskolázottság ($\chi^2(3, N = 2438) = 15{,}07$, $p = ,002$) szerint, míg a lakóhely nem volt releváns. A felsőoktatásban résztvevő hallgatók töltötték a legtöbb időt online ($M = 5{,}27$, $SD = 2{,}02$). Tudományterületenként a Z generáción belül, az informatika és gazdaságtudomány diákjai interneteztek legtöbbet (5,44 ± 2,14 óra). A Z generáción belül az általános iskolai végzettségű szülők gyermekei (5,37 ± 2,43 óra) töltik a legtöbb, a felsőfokú végzettségűek gyermekei a legkevesebb időt online (4,85 ± 2,14 óra).

A kiberbiztonsági tudatosság kérdőív elemzése alapján a válaszadók általánosan magas szintű tudatosságról számoltak be, a teljes pontszám átlaga magas volt ($M = 96{,}57$, $SD = 14{,}70$) a maximálisan elérhető 125 ponthoz képest. A legerősebb területeknek a hitelesség (20,96 ± 4,09), a felügyelet (20,72 ± 3,97) és a bizalmasság (16,86 ± 3,30) alskálák bizonyultak. Az egyedi tételek elemzése azt mutatja, hogy a válaszadók óvatosak a jelszavak megosztásával, az adataik láthatóságának korlátozásával és az ismeretlen forrásból származó e-mailekkel szemben ($4{,}35 < M < 4{,}51$).

Ezzel szemben a legalacsonyabb átlagpontszámot a sértetlenség alskálánál figyeltük meg (12,60 ± 3,86). Ez az eredmény ellentmondásos attitűdökre utal: míg a válaszadók egyértelműen elutasították azt az állítást, hogy az adatmegosztás kockázatmentes ($M = 2{,}37$), ami pozitív, addig mérsékelt bizalmukat fejezték ki a kibertérben való adattárolással kapcsolatban, hogy az adataik biztonságban vannak ($M = 3{,}19$) és nem veszhetnek

el (M = 3,69), ami potenciális sebezhetőségre utal. Hasonlóképpen, a proaktív védelmi eszközök használatát mérő hozzáférhetőség alskála (14,15 ± 4,35) és a hasznosság alskála (11,28 ± 2,73) pontszámai is alacsonyak voltak. Különösen a rendszeres vírusellenőrzésre (M = 3,35) és a letöltött fájlok vizsgálatára (M = 3,48) vonatkozó tételek kaptak alacsonyabb értékelést, ami arra utal, hogy a passzív óvatosság (pl. bizalmatlanság) erősebb, mint az aktív, rutinszerű védelmi cselekvések.

A magasabb internethasználat gyenge, de szignifikáns negatív kapcsolatot mutat a kiberbiztonsági óvatossággal. Ez különösen az elérhetőségek megosztásánál ($r_s$ = -,152, $p$ < ,001), az ismeretlen e-mailek megbízhatóságánál ($r_s$ = -,104, $p$ < ,001), és a vírusellenőrzésnél ($r_s$ = -,104, $p$ < ,001) nyilvánvaló. Az összesített pontszámmal is negatív a korreláció ($r_s$ = -,080, $p$ < ,001), jelezve, hogy több online idő alacsonyabb kiberbiztonsági tudatossággal jár.

Az Alfa generációnál ez a kapcsolat a legerősebb. Az internethasználat növekedése erősebb negatív korrelációt mutat a személyes adatok védelmével ($r_s$ = -,233, $p$ < ,001), jelszóerősséggel ($r_s$ = -,126, $p$ < ,001) és ismeretlen források kerülésével ($r_s$ = -,108, $p$ = ,002). Egyedül ennél a generációnál mutatott pozitív kapcsolatot a kibertéri adattárolás biztonságába vetett téves hit ($r_s$ = ,089, $p$ = ,010). Az összesített pontszámmal való negatív korreláció itt a legerősebb ($r_s$ = -,104, $p$ = ,003). A Z generációnál gyengébb korrelációk mutatkoztak. Szignifikáns negatív kapcsolat volt az internethasználat és a személyes adatok védelme ($r_s$ = -,102, $p$ < ,001), bankkártyaadatok kezelése ($r_s$ = -,066, $p$ < ,001) és vírusvédelem ($r_s$ = -,088, $p$ < ,001) között. Az összesített pontszámmal való kapcsolat szintén negatív, de gyengébb ($r_s$ = -,072, $p$ < ,001).

## Összehasonlító elemzések

Az egyutas varianciaanalízis szignifikáns különbségeket mutatott a napi átlagos internethasználati csoportok között a teljes kiberbiztonsági tudatosságban, $F(4, 3270)$ = 5,23, $p$ < ,001. A Tukey HSD post-hoc teszt szerint a napi 7+ órát internetező csoport szignifikánsan alacsonyabb tudatossági pontszámmal rendelkezett ($M$ = 93,92) a kevesebbet használó csoportokhoz képest ($M$ = 96,28–97,54). A hasznosság alskálán fordított mintázat jelentkezett ($p$ < ,001): a napi 0-1 órát internetezők mutatták a legalacsonyabb pontszámot ($M$ = 10,52), szignifikánsan elmaradva a többi csoporttól, mivel a kevésbé aktív internethasználók ritkábban használják a kibertér szolgáltatásait információkezelésre, problémamegoldásra és közösségi média alkalmazásokra.

A nemi különbségek vizsgálata a független mintás t-próba eredményei a kiberbiztonsági tudatosság szintjével kapcsolatban nem mutatott szignifikáns különbséget a férfiak és nők között, de az alskálákat vizsgálva a nők szignifikánsan magasabb pontszámot értek el a bizalmasság ($M$ = 17,07; $t(3273)$ = -3,46, $p$ < ,001) és a hitelesség ($M$ = 21,28; $t(3271,48)$ = -4,21, $p$ < ,001) alskálákon. Ezzel szemben a férfiak a proaktív védelmet mérő hozzáférhetőség alskálán értek el szignifikánsan magasabb pontszámot ($M$ = 14,39; $t(3273)$ = 3,39, $p$ < ,001).

Az egyutas ANOVA szignifikáns különbségeket mutatott a szülők iskolai végzettsége alapján képzett csoportok között a teljes kiberbiztonsági tudatosságban, $F(3, 3271)$ = 4,97, $p$ = ,002. A post-hoc Tukey HSD teszt igazolta ezt a pozitív kapcsolatot, ahol az általános iskolai végzettségű szülőkkel rendelkező válaszadók szignifikánsan alacso-

nyabb kiberbiztonsági tudatosság pontszámot értek el ($M$ = 93,02) a magasabb iskolai végzettséggel rendelkező szülők gyermekeihez képest. A hitelesség alskálán is a magasabb szülői végzettség fokozottabb óvatosságot eredményez az ismeretlen e-mailek, biztonsági tanúsítvány nélküli weboldalak és adathalász támadások kezelésében. A hozzáférhetőség dimenzióban szintén pozitív összefüggés mutatkozott, tehát a diplomás szülők gyermekei gyakrabban alkalmaznak proaktív védelmi intézkedéseket (vírusirtó programok, tűzfal). A bizalmasság alskálán is a diplomás szülőkkel rendelkezők mutatták a legmagasabb pontszámot ($M$ = 17,09), amely szignifikánsan meghaladta a többi csoport értékeit. Ez fokozott óvatosságot jelez a személyes adatok megosztásában és a privátszféra védelmével kapcsolatban.

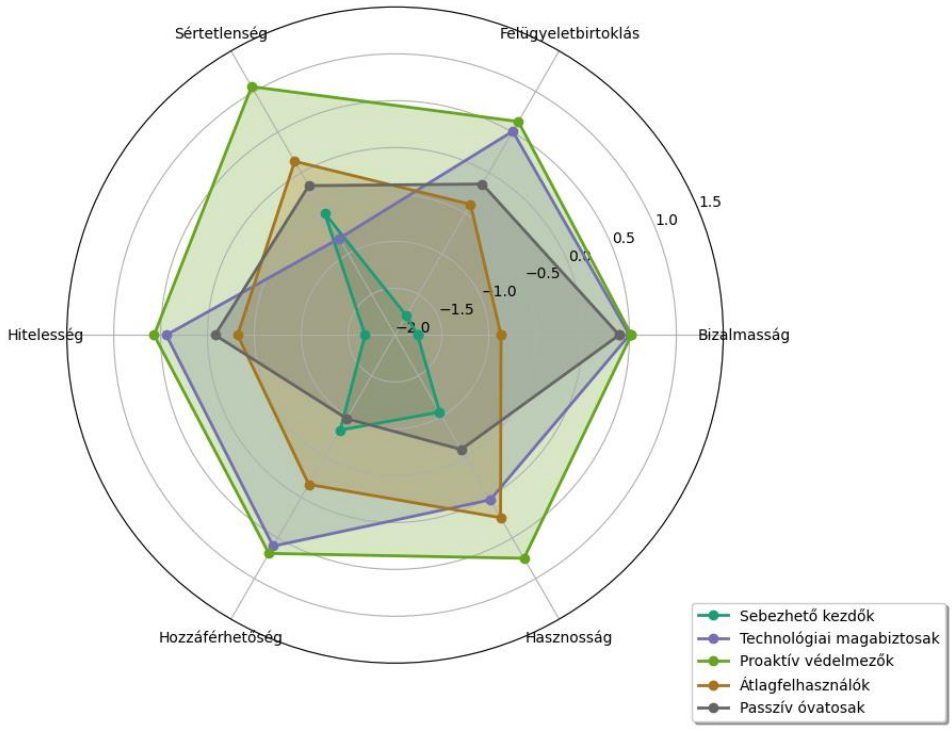
**Regressziós eredmények, összefüggések**

A kiberbiztonsági tudatosság szint jóslására lineáris regressziós modellt alkalmaztunk, független változókként a generációt, nemet, napi internethasználatot és szülői iskolázottságot bevonva. A modell szignifikáns volt, $F(4, 3270)$ = 5,69, $p$ < ,001, azonban alacsony magyarázó erővel ($R^2$ = ,007) rendelkezett. Egyedül a napi átlagos internethasználat bizonyult szignifikáns negatív prediktornak ($\beta$ = -,076, p < ,001), jelezve, hogy a több online töltött idő alacsonyabb kiberbiztonsági tudatossággal jár együtt.

A személyes adatok és privátszféra védelmét mérő bizalmasság alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 23.62, $p$ < ,001, $R^2$ = ,021, ahol a női nem magasabb ($\beta$ = ,065, $p$ < ,001), míg a fokozott internethasználat alacsonyabb adatvédelmi tudatosságot jelzett előre ($\beta$ = -,127, $p$ < ,001). Az online források és kommunikáció megbízhatóságának értékelését mérő hitelesség alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 9.72, $p$ < ,001, $R^2$ = ,009, ahol a női nem magasabb ($\beta$ = ,076, $p$ < ,001), míg a fokozott internethasználat alacsonyabb kritikai gondolkodást jelzett előre az ismeretlen e-mailek, bizonytalan weboldalak és potenciális fenyegetések kezelésében ($\beta$ = -,050, $p$ = ,004). A proaktív technikai védelmi eszközök (vírusirtó, tűzfal) használatát mérő hozzáférhetőség alskála lineáris regressziós modellje szignifikáns volt, $F(3,3271)$ = 12,81, $p$ < ,001, $R^2$ = ,012, ahol a férfi nem ($\beta$ = -,056, $p$ < ,001) és a kevesebb internethasználat ($\beta$ = -,087, $p$ < ,001) magasabb technikai biztonsági tudatosságot jelzett előre. A kibertér szolgáltatásainak (közösségi média, felhőalkalmazások) aktív használatát mérő hasznosság alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 8,38, $p$ < ,001, $R^2$ = ,008, ahol egyedül a fokozott internethasználat jelzett előre magasabb digitális eszközhasználatot ($\beta$ = ,083, $p$ < ,001).

**Kiberbiztonsági felhasználói profilok**

Annak érdekében, hogy a különböző pontszámtartományú alskálák egyenlő súllyal vegyenek részt a klaszterek kialakításában, a hat alskála nyers pontszámait Z-értékekké standardizáltuk (átlag = 0, szórás = 1). A klaszterezési eljárást ezeken a standardizált változókon hajtottuk végre, ami biztosította, hogy az algoritmus tisztán a tudatossági dimenziók közötti relatív mintázatok alapján képezze a csoportokat. A K-means klaszterelemzés a hat kiberbiztonsági alskála alapján öt, tartalmilag elkülönülő felhasználói profilt tárt fel ($N$ = 360–837). Az iterációs folyamat 52 lépésben stabil konvergenciát ért el, jelezve a klaszterek megbízhatóságát. Az azonosított csoportokat a 3. ábra szemlélteti a standardizált Z értékekkel.




*3. Ábra: Kiberbiztonsági klaszterek Z-értékei kiberbiztonsági alskálákon [forrás: saját szerkesztés]*

***1. Proaktív védelmezők*** ($N$ = 825)
Ez a csoport a legmagasabb és legkiegyensúlyozottabb kiberbiztonsági tudatossággal rendelkezik. Szinte minden dimenzióban átlag feletti, pozitív Z-értékeket értek el. Az ő profiljuk egy proaktív, felkészült és minden dimenzióban tudatos, óvatos felhasználói típust ír le.

***2. Átlagfelhasználók*** ($N$ = 591)
Középszintű tudatossággal jellemezhetők, a legtöbb pontszámuk enyhén átlag alatti (negatív Z-értékek). Ők a tipikus „nemtörődöm" felhasználók, akik a legtöbb területen alulmaradnak az átlaghoz képest.

***3. Technológiai magabiztosak*** ($N$ = 837)
Tagjaik átlag feletti tudatossággal rendelkeznek a legtöbb technikai és óvatossági dimenzióban, mint a felügyelet (jelszókezelés $Z$ = ,51) és a hozzáférhetőség (proaktív védekezés $Z$ = ,60). Ezzel szemben ők rendelkeznek a legalacsonyabb pontszámmal a sértetlenség alskálán ($Z$ = -,81). Ez a profil egy olyan felhasználói típust ír le, amelyik bár ért a technikai védelemhez, naivan azt hiszi, az adatai alapvetően biztonságban vannak, alábecsülik a valós kockázatokat.

***4. Passzív óvatosak*** ($N$ = 662)
Tagjai átlag feletti óvatosságot mutatnak a bizalmasság terén ($Z$ = ,39), tehát vigyáznak a személyes adataikra. Ezzel éles ellentétben ők rendelkeznek a legalacsonyabb pontszámmal a hozzáférhetőség alskálán ($Z$ = -,97). Egy olyan felhasználói típust ír le, amelyik

mentálisan óvatos és gyanakvó, de a gyakorlatban nem teszi meg a szükséges technikai lépéseket (pl. vírusirtó használata) a védelem érdekében.

***5. Sebezhető Kezdők*** (*N* = 360)

Különösen alacsony tudatosságot mutatnak a felügyelet (Z = -1,76), bizalmasság (Z = -1,76) és hitelesség (Z = -1,76) dimenzióban. A legkisebb és legveszélyeztetettebb csoport, általánosan felkészületlen, reaktív felhasználói típust, a legnagyobb kockázatot képviselik.

A $\chi^2$-próbák több demográfiai változó és klasztertagság között szignifikáns kapcsolatokat tártak fel. A szülői iskolázottság mutatta a legerősebb összefüggést ($\chi^2(12, N = 3275) = 31.26$, $p = .002$, *Cramer's V* = .056). Az általános iskolai végzettségű szülők gyermekei felülreprezentáltak a „*Sebezhető kezdők*" csoportjában (standardizált reziduális = 2,5), míg a diplomás szülők gyermekei alulreprezentáltak voltak ebben a csoportban (standardizált reziduális = -2,5). A napi internethasználat szintén szignifikáns kapcsolatot mutatott ($\chi^2(16, N = 3275) = 50,82$, $p < .001$, Cramer's V = ,062). A 7+ órát internetezők felülreprezentáltak a „*Sebezhető kezdők*" (standardizált reziduális = 3,0) és „*Átlagfelhasználók"* (standardizált reziduális = 2,4) csoportjaiban.. A tudományterület és a klasztertagság között is szignifikáns összefüggés volt kimutatható ($\chi^2(20, N = 3275) = 42,94$, $p = .002$, Cramer's V = ,057). Az informatika szakos hallgatók felülreprezentáltak a „*Technológiai magabiztosak*" profiljában (standardizált reziduális = 2,0), míg az általános tantervű képzésben résztvevők a „*Sebezhető kezdők*" csoportjában mutattak magasabb arányt (standardizált reziduális = 2,0). A generáció gyenge kapcsolatot ($\chi^2(4, N = 3275) = 10,50$, $p = .033$, Cramer's V = ,057), míg a *'nem'* nem mutatott szignifikáns összefüggés ($\chi^2(4, N = 3275) = 9,40$, $p = ,052$).

## KÖVETKEZTETÉSEK

Az eredmények generációs különbségeket tártak fel az átlagos napi internethasználatot érintően. A Z generáció tagjai (*M* = 5,05, *SD* = 2,16) szignifikánsan több időt töltenek online, mint a fiatalabb, Alfa generációba tartozók (M = 3,33, SD = 2,08), ami az életkori sajátosságokkal és az eltérő életszakaszokkal magyarázható. Az Alfa generáción belül az internethasználatot elsősorban az oktatási kontextus befolyásolja, ahol a magasabb követelményű, 6-8 osztályos gimnáziumokba járó diákok online aktivitása magasabb, amit valószínű az iskolai feladatok eltérő jellege, illetve a nagyobb szabadsággal járó középfokú oktatási intézmény befolyásoló hatása okozhat. Ebben a korcsoportban a demográfiai háttér (nem, lakóhely, szülők végzettsége) még nem képez szignifikáns különbséget, ami egy viszonylag homogén használati mintázatra utal. Ezzel szemben a Z generációnál egy sokkal összetettebb kép rajzolódik ki, ahol a digitális szokásokat számos szocio-demográfiai tényező árnyalja. A nemi különbségek mellett az iskolázottság szintje és iránya is kulcsfontosságúvá válik; szint szerint a felsőoktatásban, szakirány szerint az informatika és gazdaságtudományi területeken tanulók használják legintenzívebben az internetet. Különösen figyelemre méltó az a fordított kapcsolat, miszerint az alacsonyabb iskolai végzettségű szülők gyermekei töltik a legtöbb időt online, jelezve, hogy a szocio-ökonómiai háttér eltérő módon befolyásolhatja a digitális szokásokat a fiatal felnőttkorban.

A válaszadók magas kiberbiztonsági tudatosságról számoltak be (*M* = 96,57, *SD* = 14,70), különösen a jelszókezelés, adatvédelem és e-mail források ellenőrzése terén.

Tudatában vannak az adatmegosztás kockázatainak és nem bíznak a kibertérben tárolt adatok sértetlenségében, ami konzisztens óvatos attitűdöt tükröz. A proaktív védelmi intézkedések (vírusellenőrzés, fájlvizsgálat) azonban alacsonyabb értékeket mutattak, jelezve a passzív védekezési stratégiák dominanciáját. Ez összhangban van azzal, hogy a fiatalok önbizalma gyakran meghaladja tényleges tudásukat: bár úgy vélik, jobban eligazodnak az online térben, mint szüleik, ez a magabiztosság nem mindig párosul a kiberbiztonsági kockázatok megfelelő felismerésével [12,21,22].

Az eredmények alapján az internethasználat intenzitása és a kiberbiztonsági tudatosság kapcsolatban áll. A legaktívabb felhasználók (7+ óra/nap) alacsonyabb biztonsági tudatossággal rendelkeztek. Ez összhangban van korábbi kutatásokkal, amelyek szerint a túlzott internethasználat csökkentheti a kritikus gondolkodást online környezetben [23,24]. A nők magasabb bizalmasság- és hitelességtudatossággal rendelkeztek, míg a férfiak proaktívabb technikai védekezést alkalmaztak. A szülői iskolázottság pozitív hatása a kiberbiztonsági tudatosságra megerősíti a családi szocializáció jelentőségét a digitális kompetenciák fejlesztésében[25]. A magasabban iskolázott szülők valószínűleg tudatosabb digitális nevelést nyújtanak, ami a gyermekek fokozott kiberbiztonsági tudatosságában tükröződik.

A regressziós elemzések legfontosabb megállapítása, hogy a fokozott internethasználat alacsonyabb kiberbiztonsági tudatossággal járt együtt, kivéve a hasznosság dimenzióban, ahol ez a kapcsolat pozitív. A nők magasabb adatvédelmi és kritikai tudatossággal, a férfiak pedig jobb technikai védekezéssel rendelkeztek.

A klaszterelemzés öt elkülönülő kiberbiztonsági profilt tárt fel, amelyek meghaladják az egydimenziós tudatossági modelleket. A főbb megállapítás, hogy a tudatosság ellentmondásos mintázatokat mutat: a „*Technológiai magabiztosak*” gyakorlati tudásuk ellenére alábecsülik a kockázatokat, míg a „*Passzív óvatosak*” óvatosságuk dacára nem alkalmaznak megfelelő technikai védelmet. A szociokulturális háttér bizonyult a legerősebb prediktív tényezőnek: a magasabb iskolázottságú szülők gyermekei tudatosabb profilokhoz tartoztak, hangsúlyozva a családi szocializáció szerepét. Az internethasználat intenzitása paradox kapcsolatot mutatott: a legaktívabb felhasználók (7+ óra/nap) a legkevésbé tudatos csoportokban koncentrálódtak.

Az eredmények alátámasztják, hogy az univerzális prevenciós stratégiák helyett profil-specifikus, célzott beavatkozásokra van szükség az egyes csoportok egyedi sebezhetőségeinek kezelésére.

## ÖSSZEFOGLALÁS

A kutatás a Fejér vármegyei Z és Alfa generációk kiberbiztonsági tudatosságát vizsgálta, a generációs különbségekre, a befolyásoló tényezőkre és a jellegzetes felhasználói profilokra fókuszálva.

Bár a Z generáció szignifikánsan több időt tölt online, a két generáció átlagos kiberbiztonsági tudatossági szintje között nincs szignifikáns különbség. A különbségek a tudatosság jellegében mutatkoznak meg, az egyes aldimenziókban eltérő erősségekkel és gyengeségekkel(K1). Az elemzés kimutatta, hogy a demográfiai változók önmagukban gyenge bejósló erővel bírnak. A legerősebb és legkövetkezetesebb tényezőnek a napi átlagos internethasználat, mely szerint az intenzívebb online jelenlét következetesen alacsonyabb tudatossággal járt együtt. Emellett a szülői iskolai végzettség emelkedett ki kulcsfontosságú szociokulturális faktorként, ahol a magasabb végzettség szignifikánsan magasabb

tudatosságot jelzett előre (K2). A klaszteranalízis sikeresen azonosított öt, egymástól jól elkülönülő felhasználói profilt. Ezek a profilok – a „Proaktív védelmezők”-től a „Sebezhető kezdők”-ig, valamint a köztes csoportokig, mint a „Technológiai magabiztosak”, az „Átlag-felhasználók, és a „Passzív óvatosak” – bizonyítják, hogy a kiberbiztonsági tudatosság nem egy lineáris skála, hanem különböző attitűdök és viselkedésminták komplex mintázata. Ezen profilokhoz való tartozást szignifikánsan befolyásolta a szülői végzettség, a választott tudományterület és az internethasználati szokások, ami célzott, profil-specifikus oktatási és prevenciós stratégiák kidolgozásának szükségességét támasztja alá (K3).

A kapott eredmények különösen fontosak a digitális kompetenciák fejlesztése és az oktatási stratégiák szempontjából, hangsúlyozva a proaktív intézkedésekre, a helyes döntéshozatalra és a kritikus gondolkodásra nevelés fontosságát a kiberbiztonság területén.

## FELHASZNÁLT IRODALOM[3]


[1] D. Z. Tommaso, „Future Research on the Cyber Security Skills Shortage”, *Cyber Security Education: Principles and Policies*, 2020.

[2] Nemzeti Kibervédelmi Intézet: 2025-ös kiberfenyegetések új dimenziói. [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/2025-os-kiberfenyegetesek-uj-dimenzioi/ (utolsó megtekintés 2025.04.02)

[3] T. J. Módné, M. Pogátsnik, „A systematic review of human aspects in Industry 4.0 and 5.0: Cybersecurity awareness and soft skills”, *27th IEEE International Conference on Intelligent Engineering Systems (INES 2023)*, 2023, pp. 33–40, https://doi.org/10.1109/ines59282.2023.10297768

[4] J. Zarębska et al., „Research on students' perception of information technology security – a new era of threats”, *Zeszyty Naukowe, Politechnika Śląska*, 2023.

[5] F. T. Cimene, „Generation Alpha Students' Behavior as Digital Natives and their Learning Engagement”, *Psychology and Education: A Multidisciplinary Journal*, 2024, pp. 258–273, doi: 10.5281/zenodo.14007254.

[6] R. Mészáros, „A kibertér társadalomföldrajzi megközelítése”, *Magyar Tudomány*, 2001.

[7] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiá-járól; 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. melléklet, 1. §, 2013.

[8] Y.C. Kar, M.F. Zolkipli, „Review on Confidentiality, Integrity and Availability in Information Security”, *Journal of ICT in Education*, vol 8(2), 2021, pp. 34–42, https://doi.org/10.37134/jictie.vol8.2.4.2021

[9] S. Chaudhary et al, „Developing metrics to assess the effectiveness of cybersecurity awareness program”, *J Cybersecur*, köt. 8, sz. 1, 2022, doi: 10.1093/cybsec/tyac006.

[10] I. Corradini, „Developing Cybersecurity Awareness”, *Studies in Systems, Decision and Control,* köt. 284. 2020. doi: 10.1007/978-3-030-43999-6_6.

[11] E. J. Helsper, R. Eynon, “Digital natives: where is the evidence?,” *British Edu-cational Research Journal*, vol. 36, no. 3, 2010, pp. 503–520.

[12] M. Ribble, „Digital Citizenship in Schools: Nine Elements All Students Should Know”, *International Society for Technology in Education*, 2015.


[3] példák hivatkozásokra | REFERENCES examples of references

[13] J. Smith et al, "Digital socialization: young people's changing value orientations towards internet use between adolescence and early adulthood," *Information, Communication & Society*, vol. 18, no. 9, 2015, pp. 1022–1038.
[14] H. Boghosian, „Cyber Citizens: Saving Democracy with Digital Literacy", *Boston, MA: Beacon Press*, 2025.
[15] KSH, "Népszámlálási adatbázis – Központi Statisztikai Hivatal", [Online] Elérhető: https://nepszamlalas2022.ksh.hu/adatbazis/ (utolsó megtekintés 2025.06.02)
[16] KSH, "22.1.2.1. A lakónépesség nem, vármegye és régió szerint, január 1.", [Online] Elérhető: https://www.ksh.hu/stadat_files/nep/hu/nep0034.html (utolsó megtekintés 2026.06.02)
[17] J. Módné Takács és M. Pogátsnik, „A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education", *Acta Polytechnica Hungarica*, köt. 21, sz. 10, 2024, pp. 533–552, doi: 10.12700/APH.21.10.2024.10.32.
[18] I. Arpaci és K. Sevinc, „Development of the cybersecurity scale (CS-S): Evidence of validity and reliability", *Information Development*, köt. 38, sz. 2, 2022, pp. 218–226, doi: 10.1177/0266666921997512.
[19] J. Wim et al., „Marketing research with SPSS", *FT Publishing International*, 2010.
[20] L. Sajtos és A. Mitev, „SPSS Kutatási és adatelemzési kézikönyv", *Alinea Kiadó*, Budapest, 2007. ISBN:978 963 9659 08 7
[21] N. Calvin, „The Cyber Talent Gap and Cybersecurity Professionalizing", *International Journal of Hyperconnectivity and the Internet of Things*, vol 2(1), 2018, pp. 42–51.
[22] C. Berényi, Á. Csiszárik-Kocsir, "A digitális szocializáció hatása a középiskolás fiatalok eszközhasználatára," *Vállalkozásfejlesztés a XXI. században*, vol. 2023/2, 2023, pp. 241–254.
[23] B. Meggyesfalvi, "Kockázati tényezők a digitális térben – A gyerekek internet- és közösségi média használata és az online áldozattá válás," *Belügyi Szemle*, vol. 71, no. 12, 2023, pp. 2163–2178. https://doi.org/10.38146/BSZ.2023.12.3
[24] D. Szabó, E. Dani, "Smartphones and social media as status symbol of Gen Z," *Folia Toruniensia*, vol. 22, 2021.
[25] B. B. Budai, "Digitális készségfejlesztés," *Akadémiai Kiadó*, 2021. [Online] Letölthető: https://akademiai.hu/ptudx00468-digitalis-keszsegfejlesztes.html (utolsó megtekintés 2025.04.02)

DOI: https://doi.org/10.12700/btsz.2025.7.3.29

# INCREASING ENERGY EFFICIENCY WHILE MAINTAINING COMFORT: EXAMINING COMPROMISES AND ECONOMIC CONSIDERATIONS

# ENERGETIKAI HATÉKONYSÁG NÖVELÉSE A KOMFORT MEGTARTÁSA MELLETT: KOMPROMISSZUMOK ÉS GAZDASÁGOSSÁGI SZEMPONTOK VIZSGÁLATA

MÁRKOS Szilárd Attila[1]

**Abstract**

The aim of this study is to explore the extent to which energy efficiency can be increased in residential and smart buildings without reducing user comfort. Although numerous studies in various fields of building engineering have demonstrated significant energy-saving potential, they often apply optimizations that reduce user comfort. In contrast, this review seeks to identify the critical threshold at which comfort remains unchanged, while the system becomes more energy efficient. Energy suppliers using dynamic pricing offer significant financial incentives to consumers who are willing to make small changes to their consumption habits. Numerous studies show that smart home systems using artificial intelligence can achieve significant financial savings, and these processes take place automatically without users having to pay attention to them. The analysis can contribute to striking a balance between economic expectations and user needs.

**Keywords**

Efficiency, maintaining comfort level, savings, Demand response optimalization

**Absztrakt**

A tanulmány célja annak feltárása, hogy milyen mértékben növelhető az energetikai hatékonyság lakó- és intelligens épületekben anélkül, hogy csökkenne a felhasználói komfort. Bár az épületgépészet különböző területein számos tanulmány mutat be jelentős energia-megtakarítási lehetőségeket, ezek gyakran olyan mértékű optimalizációt alkalmaznak, amelyekkel csökkentik a felhasználói komfortot. Jelen áttekintés ezzel szemben azt a kritikus határt keresi, ahol a komfort változatlan marad, miközben a rendszer energiahatékonyabbá válik. A dinamikus árazást alkalmazó energiaszolgáltatók jelentős anyagi ösztönzőket nyújtanak a fogyasztási szokásaikon kis mértékben változtatni hajlandó fogyasztóknak. Számos tanulmány bemutatja, hogy mesterséges intelligencia segítségével az okosotthon rendszerekkel jelentős anyagi megtakarítás érhető el, ezek a folyamatok automatikusan zajlanak, anélkül, hogy a felhasználóknak figyelmet kellene erre fordítaniuk. Az elemzés hozzájárulhat a gazdaságossági elvárások és felhasználói igények közötti egyensúly megteremtéséhez.

**Kulcsszavak**

Hatékonyságnövelés, komfortmegőrzés, megtakarítás, keresletválasz optimalizáció

[1] markos.szilard@bgk.uni-obuda.hu | ORCID: 0009-0007-1044-6099 | university intern, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi gyakornok, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## BEVEZETÉS – AZ OKOSOTTHON-TECHNOLÓGIÁK TÉRNYERÉSE

Az aktuális trendek azt mutatják, hogy az okosotthonok térnyerése egyre szélesebb körű a modern világban. Az Internet of Things (IoT) azaz a dolgok internete megjelenése óta lehetőség nyílt a különböző okosotthon eszközök központi vezérlésére, felügyeletére és valós idejű monitorozására. Ezen eszközök elsősorban okostelefonokon és táblagépeken keresztül vezérelhetők, de lehetőség van számítógépen és egyéb (okos kapcsoló, termosztát, központi vezérlő egység, stb.) perifériákon keresztül irányítani az eszközöket. Az emberi beavatkozások volumenének csökkentésével növelhető a fel-használói komfort, ami az okosotthon rendszerek vezérlésében megjelenő mesterséges intelligencia segítségével érhető el. A felhasználóknak vannak szokásaik és különböző sémák szerint élnek ezért a klasszikus „jelenetekkel" beavatkozás nélkül viszonylag jól elérhetőek a kívánt körülmények, azonban mindig akad egy-két a szokásostól forgatókönyvtől eltérő igény, amit a mesterséges intelligencia (AI) fellhasználó monitorozásából kinyert adatok segítségével ki tud szolgálni, oly módon, hogy döntéseket tud hozni és megtenni a szükséges beavatkozásokat. Az okosotthonok potenciálja a technológia egyre szélesebb körű elterjedésével markánsan emelkedik.

Az okosotthon rendszerek az élet több területén is javítják az életminőséget, fokozzák a komfortot azáltal, hogy önműködően szabályozzák a szellőztetést a belső levegő minőség függvényében, így megfelelő gázösszetételű, VOC (formaldehid) mentes, porszűrt levegő lesz a lakásban és ezzel a rendszerrel elkerülhető a túlszellőztetés, ezáltal csökkentve az energiaveszteséget.[25] Továbbá időjárás követő módon szabályozzák a fűtést-hűtést, fényérzékelő alkalmazásával a belső megvilágítás konstans fényerősségre állítható a természetes megvilágítástól függetleníthető. Vezérlik a különböző árnyékolókat (redőnyök, zsaluziák, fényvédő rolók stb.) ezáltal tudják szabályozni a szoláris nyereséget/vesztességet, ami kedvező energetikai szempontból és a mesterséges megvilágítás is csökkenthető. Hatással vannak a hideg és melegvíz hálózatra is, a cirkulációs meleg vízhálózat csak akkor üzemel amikor a mozgásérzékelők az ingatlanban aktivitást érzékelnek ezáltal energia spórolható a komfort megtartása mellett. A körvezetékes hidegvíz rendszer automatikus előre meghatározott időközönkénti öblítését is elvégzi az okosotthon rendszer ezáltal biztosítható a higiénikus ivóvíz. Nem utolsó sorban a fenntarthatóság iránt elkötelezett emberek igényeit is kielégíti.

## PIACI KILÁTÁSOK ÉS NÖVEKEDÉSI TRENDEK

A globális intelligens otthoni eszközök piaca 2024-ben elérte a 150 milliárd USD-t, és a jelenlegi előrejelzések szerint ez az érték 2025-re 165 milliárdra, 2034-re pedig 360 milliárd dollárra emelkedik. A 2019–2034 közötti időszakra vetített összetett éves növekedési ráta (CAGR) 9,11%-os dinamikát jelez.[22]

A piaci növekedés legfőbb hajtóereje az elköteleződés a környezettudatos meg-oldások irányába, a személyes komfort növelése és a gazdaságos üzemeltetés igénye. Ezt a folyamatot tovább erősíti a különböző országok energetikai szolgáltatói által kialakított árazás, ami premizálja az energiatermelés szempontjából völgy időszakba eső fogyasztást. A végfelhasználói energia fogyasztás mintázat amplitúdójának csökkentése érdekében számos szolgáltató olyan kedvező díjazást szab a völgyidőszaki energiafel-használás serkentésére, hogy a megfelelő arányú a korábbinál magasabb fogyasztás esetében is kevesebbet kell fi-

zetnie a felhasználónak. Az okosotthonok kialakítása után nem jellemző az energia szükséglet növekedése, mivel ezen rendszerek hatékonysága jelentősen meghaladja a korábbi rendszer hatékonyságát. A szolgáltatóknak annak ellenére gazdaságos ez a díjszabás, hogy úgy tűnik fajlagosan kevesebb a bevételük, ugyan-is nem képesek valós időben szabályozni a termelésüket, így a megtermelt energia jelentős része veszteséggé alakulna, és egy ilyen díjszabással ezt az energiát tudják a hálózatba táplálni, és ezzel a teljes energiaráfordítás jóval alacsonyabban tartható.

Az Egyesült Államokban a háztartások 70%-a rendelkezik legalább egy okosotthon-eszközzel, szemben a 2018-as 33%-os aránnyal, ami jelentős előrelépést eredményez az okosotthonok összekapcsolásában és az okosvárosok kialakításának irányába. A Statista előrejelzései szerint 2025-re a világon működő intelligens otthoni eszközök száma meghaladja az 1,5 milliárdot – ez a szám egyértelmű indikátora a kereslet folyamatos növekedésének.[22]

**Az okosotthon-technológia bevezetésének motivációi**

Az okosotthon rendszerek alkalmazásának számos motivációja lehet, azonban csoportosítás szempontjából ezeket négy egymástól jól elkülönülő területre oszthatóak:

*Hatékony energiagazdálkodás*

Az első motiváció az energiahatékonysághoz kapcsolódik. Az okosotthonok nagy potenciállal rendelkeznek a háztartási energiafelhasználás ütemezése és csökkentése szempontjából, ezzel nagy mértékben hozzájárulva a szén-dioxid kibocsátás visszaszorításához [6],[7],[8]. Az integrált okoseszközök monitorozása és az eredmények vizualizálása lehetővé teszi a felhasználó számára, hogy különböző szokásaihoz költség vonzatot rendeljen. Az egyes tevékenységek vagy szokásokhoz tartozó költségek tudatában lehetőségük van megváltoztatni szokásaikat, hogy kényelem megtartása mellett energiát takarítsanak meg [6],[9] ,[11].

Ezek a technológiák fontos szerepet játszanak a kereslet oldali szabályozásban, mivel lehetővé teszik a háztartások és az energia szolgáltatók közötti adatcserét. Ez hozzájárul a fogyasztási szokások optimalizálásához és az energiatermelés tervezhetőbb időzítéséhez.

A környezettudatosság igénye egyre jobban megmutatkozik az emberek hozzáállásában. Olyan okosotthon eszközöket vásárlását részesítik előnyben, amivel energiát takaríthatnak meg és közben még az otthonuk komfortját is képesek emelni. Azt, hogy ez a megtakarítás mekkora mértékű lesz, előre nem lehet megmondani, mivel minden környezet eltér egymástól és az épület energetikájának és perifériáinak ismerete nélkül erre nincs lehetőség.

Az Egyesült Államok Energiaügyi Minisztériuma szerint az energiahatékony eszközök jelentősen csökkenthetik a háztartások energiafogyasztását, ami 10% és 50% közötti megtakarítást eredményezhet az energiaszámlákon. [22]A statisztikai adatok alapján megállapítható, hogy bármilyen okosotthon eszköz, aminek fókuszában az energia megtakarítás áll, rendkívül rövid megtérülési idővel rendelkezik, még abban az estben is, ha az energia szolgáltatási árazás nem sávos. Ha az árazás differenciált, akkor a megtérülési idő tovább apad. A kormányzati támogatások és ösztönző intézkedések elősegítik a technológia egyre szélesebb körben történő elterjedését.

A szabályozó szervek döntő szerepet töltenek be az energiahatékonysági szabványok lefektetésében és érvényesítésében. A Nemzetközi Energiaügynökség (IEA) ösztönzi

a gyártókat az innovációra és hozzájárul a szabályozási követelmények fokozatos szigorításához, ami növeli a versenyt a piaci résztvevők között. A technológiai fejlődés és a fogyasztók környezettudatosságának erősödése várhatóan tovább fokozza az okosotthon eszközök és rendszerek iránti keresletet. [22]

*Jobb otthoni egészségügyi szolgáltatások*

A második motiváció az egészségügyi szolgáltatások fejlesztése. Az idősödő fejlett társadalmakban egyre nagyobb kihívást jelent az idősek saját otthonukban történő gondozása. A mesterséges intelligenciával támogatott okosotthon rendszerek képesek monitorozni a felhasználók igényeit és megtenni a szükséges beavatkozásokat, mielőtt az adott személy valamilyen periférián keresztül felülírná a szokásos forgatókönyvet az aktuális igényi kielégítése céljából. Ennek kiemelt nagy jelentősége van az idősek és a testi vagy szellemi fogyatékossággal élők számára, akik nem biztos, hogy saját erőből be tudnának avatkozni az adott jelenet lefutásába. [16][17] Ez különösen előnyös az idősek számára, mert az okos egészségügyi funkciók nagymértékben hozzájárulnak az önállóság hosszabb fenntartásához. Ezzel javítva az életminőséget és megőrizve annak a lehetőségér, hogy rosszabb egészségi állapotban is a jól megszokott, ismert környezetben maradhasson. Egészségügyi probléma esetén riaszthatja az előre beállított kontakt személyt, így szükség esetén a segítség időben érkezhet. [13][14][15][17]

*Pénzügyi megtakarítás és gazdasági előnyök*

A harmadik motiváció a pénzügyi megtakarításokhoz és előnyökhöz kapcsolódik. A technológia lehetővé teszi, hogy akár minden a hálózatba integrált eszköz fogyasztását valós időben monitorozzuk és azt különböző szemléltetési módokon a felhasználó elé tárjuk. Az egyes folyamatokhoz, szokásokhoz tartozó költség vonzat ismeretében a felhasználó képes változtatni szokásain, finomhangolhatja a rendszere beállításait, például a sávos energia árazás esetében optimalizálhatja a fogyasztási görbéjét, módosíthat a fűtésvezérlő beállításain, új árnyékolás technikai beállításokat eszközölhet [9][11][19][18]. Csak néhány példát emeltem ki, azonban a megtakarításokra számtalan lehetőség kínálkozik. Ezen finomhangolások az ésszerű kereteken belül tartva is jelentős megtakarításokat eredményezhetnek, miközben a felhasználó komfortja nem sérül. Számos tanulmány keresi a megtakarítási maximumot, azonban ehhez olyan beállítások szükségesek, amik drasztikusan rontják a felhasználók életkörülményit, ilyenkor a költségcsökkentés jellemzően többszöröse, mint a komfortérzet megtartása mellett.

*Javított életminőség/növekvő kényelem*

Végül, de nem utolsósorban, az okosotthon-technológiák hozzájárulnak a felhasználók életminőségének javításához. Az okosotthon technológiák elterjedésével egyre több eszköz vezérelhető direkt módon. Korábban például egy kávéfőző az áramellátás kapcsolásával volt indítható és megállítható, azonban napjainkra elértünk oda, hogy egyre több készüléket közvetlenül tudunk vezérelni, ami egy jóval szofisztikáltabb működtetést tesz lehetővé[7][9][21]. A mesterséges intelligencia terjedése is nagy mértékben növeli a kényelmet azáltal, hogy minimálisra csökkenti a felhasználói beavatkozások szükségességét. Rengeteg fejlődési potenciál van még az AI vezérelt okosotthonok működtetésében, ami a generatív algoritmusok alkalmazása révén rohamosan fejlődik [20].

# IRODALMI ÁTTEKINTÉS

## Egyszerűbb okosotthon eszközök használatának hatása

A világméretű villamos energia ellátási problémák tovább fokozzák az energiahatékonysági, fentarthatósági törekvéseket. Az energia generálási deficit több dologra vezethető vissza. Egyrészt a megnövekedett ipari energia igény, másrészt a megújuló energiát hasznosító energiatermelés várakozásoktól elmaradó térnyerése, és a hagyományos erőművek visszaszorítása. Ezért egyre nagyobb hangsúlyt kap a háztartási energiafelhasználás mérséklése, melyben a fogyasztó kényelmének megőrzése mellett csak az okosotthon technológia képes jelentős eredményeket elérni. A következőkben bemutatott példák különböző földrajzi, társadalmi és technológiai kontextusban mutatja be a rendszerek hatékonyságát.

Ukpene és szerzőtársai [2] által készített tanulmányban a szerzők az okosotthon-technológiák bevezetésének hatását vizsgálták a nigériai otthonok energiafogyasztása, költségcsökkentése és környezeti előnyei szempontjából. Öt nagyobb nigériai városban (Lagosban, Abujában, Kanóban, Port Harcourtban és Enuguban) található okosotthonban gyűjtötték az elemzéshez szükséges adatokat. Az okosotthon rendszerek elemeit, mint például okos termosztátok, világítási rendszerek, fogyasztásmérők stb. a következő kategóriák alapján értékelték: Energiamegtakarítás (%), CO2 kibocsátás csökkenés és havi költség (NGN). Ebben a tanulmányban azt mutatják be, hogy egy hagyományos élettér okosotthonná alakítása milyen változásokat eredményez az energia igény és a gazdaságosság területén. Mérések alapján a modernizált otthonok energia fogyasztása jellemzően 15-25%-kal visszaesett az átalakítás előtti eredményekhez képest. A fogyasztáscsökkenés nem csak a modernizáció mértékétől függ, hasonlóan nagy jelentősége van annak, hogy az átalakítás előtt milyen volt a kiindulási állapot és hogy az épület milyen energetikai jellemzőkkel rendelkezik. Ebben a tanulmányban a megtakarítást nem a kereslet válasz vagy a fogyasztói szokások változása adta, hanem az, hogy egy okostermosztát segítségével csak akkor szükséges adott hőmérsékleten tartani a lakást, amikor a lakók otthon tartózkodnak, illetve időzíthető konnektorokkal manuálisan be lehet állítani a háztartási gépek üzemidejét, ezzel csökkentve a készenléti fogyasztást. A tanulmány bemutatja, hogy háztartásonként havi 4000 Nigériai niarás (~1000 Forint) megtakarítás érhető el, és háztartásonként az éves CO” kibocsátás 500-700 kg-mal csökken, ami számottevő környezeti előnnyel jár.

Malysheva és társai [4] a tanulmányában részletesen megvizsgálta az intelligens otthoni technológiák energiahatékonyságát különböző energiahatékonysági beállítások mellett.

Választottak egy alkalmas lakást, amelyet felszereltek okosotthon eszközökkel például napelemek, energia menedzsment rendszer, világítás vezérlés, okos termosztátok, okos energia fogyasztás mérők, és egyéb okos eszközök. Minden okos és nem okos fogyasztó elé okos fogyasztásmérőt kötöttek, így mérni tudták az eszközök valós idejű energia fogyasztását. Valós mérési körülmények reprodukálása érdekében, a rendszert valós otthoni környezetben kezdték el használni.

A mérések spektruma túlmutatott az energiafelhasználás mérésén, kiterjedt egészen a felhasználói interakciók figyeléséig. A rendszert úgy állították be, hogy előre meghatározott diszkrét időközönként (15 percenként) rögzítsen mérési eredményeket. Különböző eseteket vizsgáltak, két különböző beállítást alkalmaztak, először mértek a standard és utána az energiahatékonyságra optimalizált beállításokkal.

A hőmérséklet szabályozás hatékonyságának megítélése érdekében, feljegyezték a külső, a belső és az okostermosztáton beállított hőmérsékleteket egyaránt.

A kutatási eredmények kiértékelése után az alábbi összefüggéseket állapították meg, az okosotthon technológiák energiahatékonyságával kapcsolatban.:

1. Az okos készülékek energia fogyasztásának mérésénél megállapították, hogy jelentős 10-15%-os átlagos megtakarítás érhető el a teljesítmény és a komfort feláldozása nélkül.
2. A hőmérséklet szabályozással sikerült elérni, hogy a lakókörnyezet hőmérsékletét átlagosan 1°C-kal lehessen csökkenteni. Ezt úgy érték el, hogy komfortosnak tartott hőmérsékletet akkora érje el a lakás, amikor a felhasználó megérkezett az otthonába, és addig tartották ameddig el nem ment otthonról. A köztes időszakban engedték csökkenni a külső és a belső hőmérséklet közötti különbséget. Továbbá a fűtési görbéket a külső hőmérséklet változásához tudták igazítani.
3. Olyan szinergiákat figyeltek meg az intelligens eszközök kombinálásával, amely lehetővé teszi a felhasználó számára, hogy tovább növelje az energiamegtakarítás mértékét.

**Keresletoldali válasz opimalizálás okoseszközökkel**

*Keresletoldali válasz (Demand Response) és szerepe az intelligens otthonokban*

A keresletoldali válasz (Demand Response, DR) olyan szabályozási és technológiai megközelítések összességét jelenti, amelyek lehetővé teszik a fogyasztók számára, hogy energiafogyasztásukat tudatosan a piaci árak, hálózati terhelések vagy egyéb ösztönzők függvényében alakítsák. A DR célja a villamosenergia-kereslet és -kínálat kiegyensúlyozása, különösen csúcsidőszakokban, ezzel növelve a hálózat megbízhatóságát és stabilitását.[23]

Az okosotthon rendszerek optimális terepet biztosítanak a keresletoldali válasz szabályozás alkalmazására, mivel számos érzékelővel és különböző aktuátorokkal vannak felszerelve, így valós időben képesek reagálni az aktuális energia árazásra.

*A DR programok típusai*

A DR programok csoportosítása a különböző szabályozási célok szerint az alábbi kategóriákba rendezhetők.:

1. Időalapú díjszabás: A szolgáltatók a sávos árazással ösztönzik a felhasználókat, hogy fogyasztásuk minél nagyobb arányban a kedvezőbb díjszabású időszakban jegyezzék. Ezt leginkább a háztartási készülékek automatizált ütemezésével képesek elérni.
2. Kapacitáspiac-alapú jutalmazás: Amennyiben egy adott időszakban a fogyasztás egy bizonyos szint alá csökken, akkor a fogyasztók kedvezményeket kapnak. Ezzel az intézkedéssel a hálózati csúcsfogyasztás csökkentése a cél.
3. Vészhelyzeti keresletoldali válasz: A rendszerbiztonság szempontjából kiemelten fontos, hogy az előre nem látható hálózati vészhelyzetek estén a felhasználók válaszként csökkentik a fogyasztásukat. [24]

*Optimalizáció változó árazás esetén*

Yantai Huang és munkatársai[5] egy olyan koncepciót dolgoztak ki, amivel az egyes okosotthon készülékek vezérlését nem külön-külön kezeli, hanem összhangban így

működésük egy közös optimalizált terv szerint zajlik. Ezáltal valós időben az árazás függvényében módosítja a vezérlési sémát. A kutatócsoport a feladat megoldására egy összetett vegyes diszkrét-folytonos nemlineáris modellt alkotott, majd erre építve egy új algoritmust terveztek. A szimulációk eredményei meggyőzőek voltak, az algoritmus képes volt a pillanatnyi árakhoz igazítani a modellt és ezáltal jelentős 15,1%-os energia megtakarítást értek el vele. A komfort megőrzésének érdekében olyan változókat vezettek be, mint a felhasználó számára komfortos működési intervallumokat, amivel kijelölhető az az időszak amikor az adott berendezést használni kívánja, valamint felhasználói célárat.

Izviye Fatıma Tepe és Erdal Irmak [2] tanulmánya egy valós idejű kereslet válasz stratégiát alkalmaz, a háztartási készülékek energia fogyasztásának napon belüli optimálisabb eloszlásának érdekénben. Ezzel fenntartva az egyensúlyt a villamos energiatermelés és fogyasztás között. Törökországban ez a folyamat úgy néz ki, hogy a végfelhasználók önként csökkentik az energia fogyasztásukat, és ezzel jelentős anyagi megtakarításhoz jutnak.

A tanulmányban alkalmazott stratégia az aktuális áramárakat beépíti a modellbe és a korábban megfigyelt tevékenységek, fogyasztási minták és a háztartási gépek üzem idejének ismeretében úgy időzíti a különböző háztartási eszközök működését, hogy a lehető legköltséghatékonyabb időszakba essen. A vezérlési stratégia továbbá figyelembe veszi a felhasználó által meghatározott kezdést és befejezést, hogy a teljes üzemidő ezen preferált időszakon belül legyen. A fuzzy logikára épülő modell dinamikusan alkalmazkodik a fogyasztói szokások változásához a keresletoldali válasz hatékonyságának növelése és a gazdasági maximalizálásának érdekében. Ez az irányítási koncepció úgy képes optimális döntéseket hozni és ezek alapján beavatkozni, hogy figyelembe veszi a valós idejű árképzést a dinamikus díjszabást és az emelkedő blokkos tarifákat.

A szimulációs eredmények azt mutatják, hogy a megtakarítás mértéke a komfortérzet csökkenésével nő. A megtakarítás maximalizálásának érdekében az első mérésnél a felhasználói komfort csökkentésével 38%-os megtakarítás érhető el. Ez a hozzáállás nem életszerű, hiszen a komfort megtartása nem opció, hanem alapkövetelmény, ennek ellenére ez a mérés kiváló referenciaként szolgál a második méréshez, ahol a cél a komfort megtartása melletti hatékony költségcsökkentés volt, így is jelentős a megtakarítási volumen akár elérheti a 29%-ot.

Amjad Anvari-Moghaddam és munkatársai tanulmányukban[1] egy Sydney-ben található alacsony energia igényű egyzónás házon végeztek méréseket. Két koncepciót dolgoztak ki külön a fűtésre és külön a hűtésre, az elv azonos volt, de a bemeneti paraméterek eltértek, mint például a valós idejű áramár, szoláris nyereség/vesztesség és a kültéri hőmérséklet.

Egy olyan nemlineáris programozási modellt fejlesztettek (MO-MINLP) aminél a felhasználói kényelem és az optimalizált energiafelhasználás egyszerre valósul meg.

Három különböző szcenáriót dolgoztak ki: alap, normál, és az intelligens. Az alap forgatókönyv esetén a háztartás nem rendelkezik okos eszközökkel, nem képes figyelni és reagálni a valós idejű energiaárak alakulására. A háztartási eszközöket a felhasználó indítja és a beltér hőmérsékletét egy klasszikus termosztáttal tartja a komfortzónán belül.

A normál szabályozó nem tekinti célnak a felhasználó preferenciáit. A szabályzás fókuszába a költségek csökkentése áll, a valós idejű energia árak ismeretében tervezi meg,

árváltozás estén módosítja a különböző eszközök működési idejének ütemezését. A szabályozó igyekszik a beltér hőmérsékletét a kívánt értéken tartani.

Az intelligens vezérlő egy teljes funkcionalitású okosotthonra épít és megoldja a komplex optimalizálási feladatot. A szabályzó az előre beállított hőmérsékletet kedvező költség vonzat mellett pontosan tartja, és elvégzi a feladatütemezést az egyéb eszközökkel kapcsolatban, amivel nem csak a komfortot növeli, hanem hozzájárul a még gazdaságosabb üzemeltetéshez.

A mérési eredmények alapján kijelenthető, hogy az intelligens vezérlő meggyőző eredményeket mutat a másik két megoldással szemben. A hűtési hatékonyság 55%-kal nőtt az alap szcenárióhoz képest és 25%-kal a normálhoz képest. A fűtési hatékonyság 63%-kal nőtt az alapesethez képest és 38%-kal a normálhoz képest. Megfigyelhető, hogy az intelligens és a normál szabályzó eredményei jóval közelebb állnak egymáshoz és jelentős megtakarítást érnek az alapeset eredményeivel szemben. A termikus komfort szempontjából a három szabályzó megközelítőleg azonos eredményt érnek el, azonban a normál szabályzó nem tud teljes mértékben megfelelni a felhasználó feladatütemezési preferenciáinak. A mérések eredményéből jól látható, hogy bár a vezérlési alapelv azonos, így is jelentős eltérés van a fűtési és a hűtési hatásfok között. A különbséget elsősorban a szoláris nyereség és veszteség hatásából ered. Nyáron a napenergia nem csak az üvegfelületeken keresztül jut be az épületbe, hanem a tetőn és a falakon keresztül is, ami rontja a hűtési hatékonyságot. Télen a napenergia az üvegfelületeken keresztül fűti a belteret, ami energetikai szempontból kedvező.

A passzív házak tervezéséhez használt szoftverek pont ezen okok miatt nagy jelentőséget tulajdonítanak az épületek megfelelő tájolására, és a nyílászárok méretének elhelyezkedésének és árnyékolásának megtervezésére. A gondosan megtervezett épület tető túlnyúlásai a nyári melegben amikor a nap magasan jár, árnyékol és nem engedi, hogy az üveg felületek közvetlen napsütésnek legyenek kitéve, viszont télen amikor a nap alacsonyban jár, akkor lehetővé teszi, hogy az üveg felületeket süsse a nap, ezzel a kialakítással aktív árnyékoló nélkül is hatékonyan maximalizálja a szoláris nyereséget és minimalizálja a veszteséget.

## KONKLÚZIÓ

A különböző vizsgálatok eredményei megerősítik, hogy az okosotthon vezérléssel milyen jelentős eredmények érhetők el az otthoni energiafelhasználás területén. Az optimalizálásra használt modellek rávilágítottak arra, hogy a felhasználói komfort és az energia megtakarítás nem egymást kizáró tényezők, hanem jól hangolt vezérléssel egyszerre is kompromisszum nélkül biztosíthatók.

A bemutatott tanulmányoknál mért megtakarítások mértéke a komfort megtartása mellett 15-38% között szór. Ez egy rendkívül széles tartomány, ami nem teszi lehetővé a különböző modellek eredményességének összehasonlíthatóságát. Az ilyen mértékű különbség egy részét valószínűsíthetően a kiindulási állapot és a hozzá tartozó komfortkülönbség okozza. A korábban bemutatott esettanulmányokban a helyi energia szolgáltató sávos vagy dinamikus árazást alkalmazott, így a gazdasági megtakarítás még jelentősebb. Amennyiben a szolgáltató egységárat állapít meg, akkor a megtakarítás mértéke szerényebb lesz. Egy ilyen okosotthon beruházás megtérülési ideje, még a kedvezőtlenebb esettel is számolva igen rövid.

Az intelligens szabályozók nem csupán technológiai innovációk, hanem eszközök egy fenntarthatóbb, kényelmesebb és hatékonyabb energiafelhasználás felé vezető úton. Ezek a technológiák várhatóan egyre nagyobb szerepet kapnak a modern épület üzemeltetésben.

## FELHASZNÁLT IRODALOM

[1] A. Anvari-Moghaddam, H. Monsef, A. Rahimi-Kian (2015). Optimal Smart Home Energy Management Considering Energy Saving and a Comfortable Lifestyle. IEEE Transactions on Smart Grid. 6. 324-332.
[2] Tepe, İ.F., Irmak, E. Optimizing real-time demand response in smart homes through fuzzy-based energy management and control system. Electr Eng 107, 2121–2145 (2025). https://doi.org/10.1007/s00202-024-02613-3
[3] P. Ukpene & T. Apaokueze.(2024). The Impact of Smart Home Technologies on Energy Efficiency, Cost Savings, and Environmental Benefits. Journal of Energy Engineering and Thermodynamics. 4. 21-32. 10.55529/jeet.44.21.32.
[4] A. A. Malysheva, B. Rawat, N. Singh, P. Chandra, Jena, Kapil (2024) Energy Efficiency Assessment in Smart Homes: A Comparative Study of Energy Efficiency Tests BIO Web of Conferences 86, 01083 (2024) https://doi.org/10.1051/bioconf/20248601083
[5] Huang Y,Wang L, Kang Q,Wu Q (2016) Model predictive control based demand response for optimization of residential energy consumption. Electr Power Compon Syst 44(10):1177–1187. https://doi.org/10.1080/15325008.2016.1156787
[6] M. Ringel, R. Laidi, D. Djenouri, Multiple benefits through smart home energy management solutions, Energies 12 (8) (2019) 1537.
[7] C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin, Smart homes and their users, Pers. Ubiquit. Comput. 19 (2) (2015) 463–476.
[8] C. Vlachokostas, Smart buildings need smart consumers, Int. J. Sustain. Energy 39 (2020) 648–658.
[9] C. Chen, X. Xu, J. Adams, J. Brannon, F. Li, A. Walzem, When east meets west, Energy Res. Social Sci. 69 (2020), 101616.
[10] B. Sovacool, D. Furszyfer Del Rio, Smart home technologies in Europe, Renew. Sustain. Energy Rev. 120 (2020), 109663.
[11] A. Zaidan, B. Zaidan, A review on intelligent process for smart home applications based on IoT, Artif. Intell. Rev. 53 (1) (2020) 141–165.
[12] X. Fan, B. Qiu, Y. Liu, H. Zhu, Bochong Han, Energy visualization for smart home, Energy Procedia 105 (2017) 2545–2548.
[13] D. Choi, H. Choi, D. Shon, Future changes to smart home based on AAL healthcare service, J. Asian Architecture Build. Eng. 18 (3) (2019) 190–199.
[14] T. Kadylak, S. R. Cotten, United States older adults' willingness to use emerging technologies, Inf., Commun. Society 23 (5) (2020) 736–750..
[15] S. Arthanat, H. Chang, J. Wilcox, Determinants of information communication and smart home automation technology adoption for aging-in-place, J. Enabling Technol. 14 (2) (2020) 73–86.
[16] A. Sanchez-Comas, K. Synnes, J. Hallberg, Hardware for recognition of human activities, Sensors 20 (15) (2020) 4227.

[17] R. Basatneh, B. Najafi, D. Armstrong, Health sensors, smart home devices, and the internet of medical things, J. Diabetes Sci. Technol. 12 (3) (2018) 577–586.
[18] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, M.L.M. Kiah, A review of smart home applications based on Internet of Things, J. Network Comput. Appl. 97 (2017) 48–65
[19] S. Cockbill, V. Mitchell, A. May, Householders as designers? Energy Res. Social Sci. 69 (2020), 101615.
[20] E. Lutolli, S.L. Vrhovec, Adoption of smarthome devices: Blinded by benefits, ignoring the dangers? Elektrotehniski Vestnik 86 (5) (2019) 267–273
[21] Y. Strengers, L. Nicholls, Convenience and energy consumption in the smart home of the future, Energy Res. Social Sci. 32 (2017) 86–93
[22] A.Gupta: Smart Home Device Market Research Report: By Product Type (Smart Lighting, Smart Security Systems, Smart Thermostats, Smart Appliances, Smart Home Hubs), By Technology (Wi-Fi, Bluetooth, Zigbee, Z-Wave, Thread), By Application (Security, Energy Management, Home Automation, Healthcare, Entertainment), By End Use (Residential, Commercial, Industrial) and By Regional (North America, Europe, South America, Asia Pacific, Middle East and Africa) - Forecast to 2035 Source: https://www.marketresearchfuture.com/reports/smart-home-device-market-8043 - Letöltve: 2025.08.01.
[23] https://www.iea.org/energy-system/energy-efficiency-and-demand/demand-response Letöltve: 2025.08.01.
[24] https://www.energy.gov/oe/demand-response Letöltve: 2025.08.01.
[25] C. Kollár, C. Kollár, T. I. Kakusziné, J. Bencsik, B. M. Rákóczi, R. Sánta, E. Szűcs, and G. Szűcs, Domotika 1. Kolozsvár: Koinónia Kiadó, 2023.

DOI: https://doi.org/10.12700/btsz.2025.7.3.39

# ORGANIZATION OF LIVE-FORCE PROTECTION OF A MILITARY RADAR OBJECT

# EGY KATONAI RADAROBJEKTUM ÉLŐERŐS VÉDELMÉNEK MEGSZERVEZÉSE

BRAUN András[1] – PETŐ Richárd[2]

**Abstract**

Hungary military facility equipped with radars located in five settlements in different parts of the country. Each object is equipped with different types of radar, where radars can detect air targets at different angles, altitudes and distances. What all facilities have in common is that the protection of the object is essential for its smooth operation. In the course of our research, we would like to describe the organization of the live-force protection of a military radar object. In our study, we aimed to establish an armed security guard, describe its main tasks, order of use of coercive means and discuss the rules for the use of firearms.

**Keywords**

Armed Security Guard, Radar, Military Technology

**Absztrakt**

Magyarország öt településén, az ország különböző pontjain található radarokkal ellátott katonai létesítmény. Az egyes objektumok különböző típusú radarokkal vannak felszerelve, ahol a radarok más-más oldalszögeken, eltérő magasságokon és távolságokon képesek a légi célokat felderíteni. Mindegyik létesítmény esetében közös az, hogy az objektum védelme elengedhetetlen a zavartalan működés érdekében. Kutatásunk során egy katonai radarobjektum élőerős védelmének megszervezését kívánjuk ismertetni. Tanulmányunkban a fegyveres biztonsági őrség felállítását, főbb feladatainak ismertetését, a kényszerítő eszközök használatának rendjét, illetve a lőfegyverhasználatának szabályainak taglalását tűztük ki célul.

**Kulcsszavak**

Fegyveres biztonsági őrség, Radar, Haditechnika

1 braun.andras92@stud.uni-obuda.hu | ORCID: 0009-0008-3958-5751 | PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | Doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

2 peto.richard@bgk.uni-obuda.hu | ORCID: 0000-0002-6757-0863 | Adjunct professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, Egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

## BEVEZETÉS

Napjainkban a légtérvédelem, többek közt a légtér felderítése, kiemelten fontos szerepet tölt be Magyarországon, mely a radarok működése nélkül elképzelhetetlen lenne. Tanulmányunk elsődleges célja a fegyveres biztonsági őrség megszervezése, ahol ismertetjük az olvasót az őrzött létesítmény fegyveres biztonsági őrség szolgálatváltási rendjéről, valamint az őrségparancsnok, az őrparancsnok, az őrök, kapu ügyeletesek, járőrök általános és különleges kötelességeiről, illetve kötelmeiről egyaránt. Külön hangsúlyt fektetünk a kényszerítő eszközök alkalmazásának, de leginkább a lőfegyverhasználatának rendjére, módjára, a lőfegyverek alkalmazására. Lőfegyverek használatánál kiemelkedően a fegyverek és lőszerek tárolására, amelyekkel az aktuális létesítmény fegyveres biztonsági őrsége fel van szerelve, el van látva. Az őrségnek támadás esetén vagy akár elemi csapás esetén is mindig a szituációnak megfelelően a lehető legprecízebben kell eljárnia. Amennyiben fegyverhasználathoz kell folyamodniuk, annak megvannak a maga szabályai és különböző lépései, illetve, hogy mi előzi meg a fegyverhasználatot. Maga a magatartás, a hideg vér megőrzése kimondottan fontos, ugyanis, ha fokozódik a helyzet, élesben kell bizonyítaniuk tudásukról, s a megfelelő kiképzettségükről. Szükséges tehát ismertetni a személyi állományt, hogy mennyire elengedhetetlen a felkészítésük, megfelelő oktatásuk különböző esetekre. Egyénileg és párokban, nagyobb létszámban is meg kell állják a helyüket az őrzött területen szolgálatot teljesítő őrparancsnoknak, járőröknek, kapu ügyeleteseknek, s ehhez elengedhetetlen az elméleti, mentális, szellemi, fizikai és gyakorlati kiképzettség. [1] [2] [3]

## A FEGYVERES BIZTONSÁGI ŐRSÉG ÉS AZ ELHELYEZÉSÉRE SZOLGÁLÓ OBJEKTUM JELLEMZÉSE

Az objektumot drótkerítéssel kell körbevenni ügyelve a nyomsáv kialakítására. A drótkerítés szerepe, hogy meggátolja, illetve lelassítsa az objektumba való illetéktelen behatolást. A nyomsáv folyamatos felügyeletét, az élőerőt támogató, CCTV rendszerrel kell ellátni. A nyomsáv karbantartásáról folyamatosan gondoskodni kell. Elsősorban a periméter védelmi eszközök épségének, illetve illettéktelen személy behatolásának érzékelése miatt. A nyomsáv növényzete évszaktól függően változik, így a nyári időszakban a megnövekedett növényzet kitakaró hatással bír. A területre való belépés csak a szolgálat engedélyével lehetséges. A főbejárati kapu nyitását-zárását pedig a fegyveres biztonsági szolgálat hajtja végre. A személyi védelmet a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX Törvény I. fejezetére, valamint a fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról szóló 27/1998. (VI: 10.) BM rendeletre hivatkozva a fegyveres biztonsági őrség biztosítja. [4] [5]

A fegyveres biztonsági őrség állandó, harmadfokú őrség, mely áll:

- őrségparancsnokból,
- őrparancsnokból,
- őrökből, akik járőrként, illetve reagáló csoportként tevékenykednek.

Az objektum őrzésvédelmét érintő szolgálati ügyekben, az őrségparancsnok egyidejű tájékoztatása mellett, az őrség felé utasításra jogosult személyek:

- az objektum parancsnok,
- az objektum parancsnok helyettes,

- a mindenkori ügyeletes parancsnok,
- az objektumügyeletes.

Az őrök az év minden egyes napján 24 órás váltásos munkaidőrendszerben látják el feladataikat. Az aktuális őrségutasításban meghatározott munkaidőrendszertől a munkáltató sajátosságainak megfelelően, illetve különleges jogrend időszakában, ideiglenesen el lehet térni. „Az őrség állományának szolgálatba vezénylését előre meg kell tervezni. Ki kell alakítani váltásokat és be kell ütemezni a tárgyhónapra a szabadnapok, illetőleg az évi szabadságok kiadását." [4, 56.§ (1)] Az őrségbe vezényelt váltás állománya köteles pihenten, szolgálatra alkalmas állapotban, a szolgálatváltás előtt, az őrség eligazítási helyén megjelenni és az előírt formaruhába átöltözni. A szolgálatot átadni készülő őrparancsnok a váltás előtt előkészíti azokat a konkrét feladatköröket, amelyeket az újonnan szolgálatba lépő őrparancsnoknak meg kell ismernie. Az új őrparancsnok a régi őrparancsnoktól átveszi a folyamatban lévő feladatokat, a szolgálat idejére vonatkozó konkrét utasításokat, a szolgálati helyiségek berendezéseit okmányait, a fegyverszobát. Kiadja az új őrségnek a fegyvereket és a lőszert, valamint levezényli az új őrség fegyvereinek töltését, végrehajtja a szolgálatba lépő állomány eligazítását, felvezetését. A régi őrparancsnok vezényli a régi őrség leváltását, fegyvereinek és tárainak ürítését. Az új őrparancsnok irányítja és végzi a régi őrség fegyvereinek visszavételét. „A régi őrszolgálat csak az őrszolgálat szabályos átadása, a fegyver és lőszer leadása után távozhat. A szolgálatot átadó minden lényeges körülményről, eseményről a váltóőrt köteles tájékoztatni." [4, 59.§] „A szolgálati helyekre meghatározott létszámból a szolgálatot úgy kell megszervezni, hogy a váltótárs és a szolgálati váltásnak megfelelő készültség biztosított legyen." [4, 49.§] „Az őrök váltását az őrzés jellegétől függően kell végrehajtani. A leváltott őrök - a szolgálati rendszertől függően - az őrség helyiségében készültségi szolgálatot látnak el, vagy pihennek." [4, 50.§] Az évszaknak és az időjárási viszonyoknak megfelelően a váltás történhet az éppen aktuális őrutasításban meghatározottaktól eltérően is.

„Az eligazítás tartalma:

- az elöljáró utasításaiból adódó feladatok ismertetése,
- az általános szolgálati követelményekről és az előző szolgálat alatt történt eseményekről tájékoztatás,
- amennyiben szükséges az adott szolgálati időre szóló jelszám ismertetése,
- a felkészültség, a felszerelés ellenőrzése" [4, 58.§ (1)], szolgálatra képes állapot ellenőrzése
- fegyverhasználat szabályai, biztonsági rendszabályok.

„Az eligazítás folyamán az őrparancsnok meggyőződik arról, hogy a szolgálatba lépők nem állnak esetlegesen szeszes ital, kábítószer vagy egyéb bódító hatású készítmény hatása alatt, illetve, hogy megfelelő az egészségi állapotuk a szolgálat ellátásához. Ha a szolgálat ellátását akadályoztató okokat észlel, akkor intézkedik azok megszüntetése érdekében." [4, 58.§ (3)] „Tilos őrségbe vezényelni olyan őrt, aki nem ismeri az őrszolgálat ellátásának alapvető követelményeit, valamint aki ellen büntető vagy őrszolgálati vétség miatt fegyelmi eljárás van folyamatban, továbbá szolgálati beosztásából felfüggesztették." [4, 60.§] „Fegyveres biztonsági őrséggel kell védeni az állam működése, illetőleg a lakosság ellátása szempontjából kiemelkedően fontos tevékenységet, létesítményt, szállítmányt, ha a

védelmére a Magyar Honvédség, a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló törvény szerinti rendvédelmi szervek, valamint az Országgyűlés biztonságáról gondoskodó Országgyűlési Őrség, illetve Nemzeti Adó- és Vámhivatal jogszabállyal nem kötelezettek, de az őrzés a közbiztonság vagy a nemzeti vagyon védelme érdekében indokolt." [5, 1.§ (1)] „A fegyveres biztonsági őrzést úgy kell megszervezni, hogy az - figyelemmel az alkalmazott biztonságtechnikai eszközökre, szolgálati állatokra, az őrség szervezetére, létszámára, felszereltségére, szolgálati rendszerére - biztosítsa az adott létesítmény, illetve tevékenység őrutasításban meghatározott jogellenes cselekmények védelmét." [5, 3.§ (2)] A fegyveres biztonsági őrség alapfeladata a létesítmény őrzésvédelme, zavartalan működésének elősegítése, a jelzőberendezések riasztásaira történő reagálás, a riasztás okának felderítése. Az objektum általános őrzésvédelme során a fegyveres biztonsági őrség őrzi az objektum kerítése által határolt területet a rajta található épületekkel és berendezési tárgyakkal együtt. Ellenőrzi az objektum területére irányuló személy- és gépjárműforgalmat. Együttműködik az objektumban egyéb szolgálatot teljesítő, illetve munkát végző személyekkel.

Az őrség őrzésvédelmi feladatainak ellátása során:

- megakadályozza illetéktelenek behatolását a zárt területre,
- felszólítja a biztonságot sértő vagy veszélyeztető személyt tevékenysége abbahagyására és igazoltatja,
- visszatartja a tettlegesen ellenszegülő személyt a rendőrség megérkezéséig,
- kényszerítő eszközöket alkalmaz és fegyvert használ az arányosság követelményének betartásával a biztonságot veszélyeztető tevékenység megszakítása, felszámolása érdekében,
- felügyeli és kezeli a biztonságtechnikai eszközöket,
- rendkívüli események bekövetkezése esetén biztosítja az elsődleges intézkedések megtételéhez szükséges reagáló képességet,
- ellenőrzi az objektum bejáratait, a belépés jogszerűségét,
- felfedi a biztonságra veszélyt jelentő cselekményeket, továbbá a biztonsági szabályzat előírásainak megsértését,
- intézkedik a rendellenességek megszüntetésére,
- betartatja és betartatja az objektum területén érvényben lévő tűzvédelmi rendszabályokat.

Az őrség tagjai kötelesek az irányítási rendszer vonatkozó és a környezetvédelmi, munkavédelmi és tűzvédelmi szabályok előírását betartani. Bizalmas információkat és üzleti titkokat a vonatkozó külső és belső szabályozásban foglaltak szerint kell kezelni. A rábízott eszközöket és anyagokat védeni, előírás szerint kell kezelni.

„Az őr:

- szolgálatban fegyelmezett, fegyveres biztonsági őrhöz méltó magatartást tanúsít,
- felelősséget érez őrtársai iránt, segíti, egyben visszatartja őket a jogsértő cselekedetektől,
- éber, minden körülmények között megőrzi az államtitkot, a szolgálati, az üzleti és a magántitkot, betartja a személyes adatok kezelésére vonatkozó jogszabályi előírásokat,

- szakmai ismereteit állandóan fejleszti,
- szolgálati tevékenysége során érvényt szerez a törvényes rendelkezéseknek, az aktuális őrségutasításban előírtaknak,
- a szolgálati feladatát fegyelmezetten végzi, mindenkor betartja a szolgálati utasításokat,
- engedelmeskedik elöljáróinak, vezetőinek, segíti őket a feladatok végrehajtásában, a fegyelem fenntartásában,
- szeszes italtól befolyásolt, illetve bármilyen okból bódult állapotban lévő személy szolgálatot nem láthat el. Aki szolgálatát önhibájából nem tudja ellátni, felelősségre kell vonni." [4, 19.§ (1)]

Az őrség tagjai szolgálati idejük alatt senkit sem fogadhatnak, csomagot, levelet, telefonüzenetet nem vehetnek át, szolgálati idejük alatt mobiltelefont nem vihetnek magukkal. „Az őr a szolgálatban, ha az a szolgálati feladatai maradéktalan végrehajtását nem veszélyezteti, az aktuális őrutasításban meghatározott területen segítséget nyújt:

- a rendőri intézkedés végrehajtásához,
- balesetnél a helyszín biztosításához, a rendőrség, a mentők, a tűzoltók értesítéséhez,
- a bűncselekmény tettesének elfogásához,
- elfogott személyek őrzéséhez vagy előállításához,
- a sérültek részére elsősegélynyújtáshoz." [4, 19.§ (2)]

„Az őrség tagja amennyiben bűncselekmény elkövetéséről vagy gyanújáról tudomást szerez, jelenti parancsnokának." [4, 19.§ (3)] „A járőröknek járőrútvonalat kell kijelölni. Ha több járőr működik egy időben, az elöljáró, illetve az őrség irányítására jogosult személy ismertetőjelet, illetve számozást állapít meg részükre." [4, 30.§ (2)] A járőr megfigyelőhelyét rejteni kell, a járőr menetvonalhoz kapcsolódó feladatait, idejét, módját az úgynevezett járőrútvonal táblázatban kell előírni. „Az előírt feladat végrehajtása után a járőr bevonul az őrség elhelyezési körletébe és jelenti a parancsnoknak a feladat végrehajtását." [4, 30.§ (4)]

A járőr feladatai:

- köteles az előre meghatározott időpontban, illetve az őrparancsnok útba indításának és eligazításának megfelelően a járőrtevékenységet megkezdeni,
- a járőrözés során különös figyelmet szentel az objektumot körülvevő kerítés sértetlenségére, ha rendellenességet észlel azonnal jelenti az őrparancsnoknak rádión,
- az objektumba behatoló, illetve onnan kilépő illetéktelen személyek feltartóztatása, igazoltatása, előállítása,
- az objektum belső területén történő munkaidőn túli mozgás felfedése, jogosságának ellenőrzése, folyamatos tűzfigyelés az objektum területén belül és körzetében,
- a meghatározott figyelési pontokon rejtett vagy nyílt figyelést végez,
- a járőrtevékenység során ellenőrzi a lezárt raktárterületek sértetlenségét,
- tűz esetén azonnal értesíti az őrparancsnokot, részt vesz a helyszínbiztosítási, mentési és tűzoltási feladatok végrehajtásában,
- a járőrtevékenység során a kijelölt járőrútvonalról letérni tilos,
- az esetlegesen elhelyezett ellenőrző pontokon a járőr regisztrálja ottlétét a nála lévő berendezés segítségével,

- akadályozza meg, hogy az objektum kerítése mentén robbanó, gyújtó, vagy pirotechnikai anyagot elhelyezzenek,
- a járőrözés során észlelt gyanús személyek csoportosulását, polgári gépjárművek forgalmát az objektum közvetlen közelében, az objektum fényképezését, filmezését, rajzolását haladéktalanul jelentse az őrparancsnoknak.

Az őrt vagy az objektumot ért támadás esetén az őrparancsnok köteles haladéktalanul értesíteni az őrség parancsnokát és az objektum vezető szolgálatot. Az őrségparancsnok, távollétében az őrparancsnok, ha a létesítményt támadás éri a rendelkezésre álló állománnyal megszervezi a védelmet. Támadás esetén azonnal értesíteni kell az objektum vezető szolgálatot, majd megérkezésük után az objektum parancsnoka vagy az általa kijelölt személy veszi át a további irányítást. A járőrözés közben ért támadás esetén az őrparancsnok riasztását követően a járőr, az őrparancsnok a Szolgálati szabályzatban előírtak alapján jár el. Az őrségparancsnok megszervezi a katonai szervezet tervében megszabott feladatok végrehajtását. Kisebb kaliberű támadás esetén a tetteseket el kell fogni, vissza kell tartani a rendőrhatóság kiérkezéséig. Abban az esetben, ha helyszínbiztosítás szükséges, akkor a vonatkozó előírások alapján végre kell hajtani. A támadást követően az esetleges sérültek részére történő segítségnyújtásról, illetve elszállításukról gondoskodni kell. [4] [5] [6] [7]

## A KÉNYSZERÍTŐ ESZKÖZÖK ALKALMAZÁSÁNAK RENDJE

„A fegyveres biztonsági őr a biztonságot veszélyeztető tevékenység megszakítása érdekében, az azt elkövető személlyel szemben az arányosság követelményének betartásával, az FBŐ. törvény 10.§ (2) bekezdés alapján:

- testi erővel cselekvésre vagy cselekvés abbahagyására kényszerítést,
- a visszatartott személy szökésének megakadályozására bilincset,
- a támadás megakadályozására vagy az ellenszegülés megtörésére vegyi vagy elektromos sokkoló eszközt, rendőrbotot,
- az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány ellen fegyveresen vagy felfegyverkezve intézett támadás elhárítására szájkosár és póráz nélküli szolgálati kutyát vagy lőfegyvert alkalmazhat, illetve használhat.” [5, 10.§ (2)]

„A kényszerítő eszköz alkalmazása esetén kerülni kell a sérülés okozását, az emberi élet kioltását. Az intézkedés során megsérült személy részére, amint az lehetséges, segítséget kell nyújtani. Szükség esetén a fegyveres biztonsági őr köteles gondoskodni arról, hogy a sérültet orvos elláthassa.” [5, 10.§ (3)] „A kényszerítő eszköz alkalmazására az érintettet, ha az eset körülményei lehetővé teszik, előzetesen figyelmeztetni kell.” [5, 10.§ (4)] „Ha az engedélyezett kényszerítő eszköz nem áll rendelkezésre vagy a használatára nincs lehetőség, a fegyveres biztonsági őr a bilincs, a rendőrbot helyett más eszközt is igénybe vehet, ha a helyettesített eszköz alkalmazásának törvényi feltételei fennállnak és az eszközzel elérni kívánt törvényes cél megvalósítására alkalmas.” [5, 10.§ (5)] Az őrszoba és az onnan eltávozó őrök között, valamint az együttműködési tervben meghatározott szervek között a hírösszeköttetés az alábbi rendelkezésre álló eszközök biztosítják, mint például a távbeszélőkészülék, szolgálati mobil és a hasábrádió. Itt felsorolandó a rendőrség (107), tűzoltóság (105) és mentők (104) elérhetősége is.

„A lőfegyver használatát a következő sorrendben meg kell előznie:

- felhívásnak, hogy a felhívott a biztonsági őr felszólításának engedelmeskedjen,
- más kényszerítő eszköz alkalmazásának,
- figyelmeztetésnek, hogy lőfegyverhasználat következik,
- figyelmeztető lövésnek.” [5, 10.§ (6)]

„A [5, 10.§ (6)] bekezdésben előírt megelőző intézkedések részben vagy teljesen mellőzhetők, ha az eset összes körülményei folytán a megelőző intézkedésekre már nincs idő, és a késedelem következtében a támadás a védett létesítményt, értéket vagy tevékenységet közvetlenül veszélyezteti.” [5, 10.§ (7)] „Lőfegyverhasználatnak csak a szándékosan személyre leadott lövés minősül. Nem minősül lőfegyverhasználatnak a vétlenlövés, az állatra, a tárgyra leadott lövés vagy a figyelmeztető és a jelzőlövés.” [5, 10.§ (8)] Lőfegyverhasználat a raktárépületek, lakóépületek, a repülőtereken légtér irányába szigorúan tilos! „A kényszerítő eszköz alkalmazását haladéktalanul jelenteni kell a felettesnek.” [5, 10/A.§ (1)] A fegyveres biztonsági őr lőfegyverhasználatának és az e törvényben meghatározott intézkedésének jogszerűségét az őrség működési helye szerinti illetékes rendőri szerv vizsgálja ki az államigazgatási eljárás általános szabályai szerint. „A fegyveres biztonsági őrt a fokozott büntetőjogi védelem, valamint az 1997. évi CLIX. törvény szerinti intézkedési és kényszerítőeszköz-használati jogosultság kizárólag az aktuális őrutasításban szereplő feladatok ellátása során illeti meg.” [7, p. 5.] „Az őr az FBŐ törvény 10.§-ában meghatározott intézkedési kötelezettséggel rendelkezik.” [4, 39.§ (1)] „Az őr az intézkedés megkezdésekor, amennyiben a körülmények megkívánják, a kényszerítő eszközt készenlétbe helyezi, felkészül a támadás elhárítására, az ellenszegülés megtörésére.” [4, 40.§ (1)] Törekedni kell arra, hogy „az ütés lehetőleg a támadó végtagot érje, kerülni kell, hogy az ütés a fejre, derékra, gyomorra, hasra irányuljon.” [4, 40.§ (2)] „A kényszerítő eszközöket - a testi kényszer és a bilincs kivételével - nem szabad a támadás, ellenszegülés megszűnése, megtörése után alkalmazni.” [4, 40.§ (3)] „Az őr intézkedéséről köteles jelentést írni, melynek egy példányát - a jogszerűség kivizsgálása céljából - meg kell küldeni az őrség működési helye szerinti illetékes rendőrkapitányságnak.” [4, 39.§ (2)] „Testi kényszert akkor kell alkalmazni, ha az őr erőfölényben van vagy az intézkedése alá vont személy állapota, magatartása folytán súlyosabb kényszerítőeszköz alkalmazása nem indokolt. Ilyenkor az őr alkalmazza az önvédelmi fogásokat.” [4, 41.§] „A bilincselést az erre a célra rendszeresített eszközzel kell végrehajtani. Ennek hiányában vagy ezek meghibásodása, megrongálódása esetén más ilyen célra megfelelő eszköz is alkalmazható, de tilos vékony fém- vagy műanyag huzalt, a jellegénél fogva sérülést okozó eszközt alkalmazni. Ugyancsak tilos a bilincs olyan módon való használata, amely indokolatlanul fájdalmat, sérülést okoz vagy jellegénél fogva megalázó.” [4, 42.§ (1)]

„A bilincselés módjai:

- két vagy több ember kezének egymáshoz bilincselése,
- kezek előre-, illetve hátrabilincselése,
- indokolt esetben lábak egymáshoz bilincselése,
- indokolt esetben tárgyhoz bilincselés.” [4, 44.§ (2)]

„A bilincselés módját az őr az adott körülmények között a legcélirányosabban választja meg azzal, hogy:

- a kezek hátrabilincselése akkor célszerű, ha a bilincs alkalmazására testi kényszer útján kerül sor vagy alapos okkal tartani lehet az őr elleni támadástól, illetőleg szökéstől,
- lábbilincselés, illetőleg kéz- és lábbilincselés együtt alkalmazása akkor indokolt, ha az elfogott személyről feltételezhető, hogy ellenkező esetben önmagában vagy másban kárt tenne,
- tárgyhoz bilincselésnek akkor és addig van helye, amíg más személy segítségül hívásával nem biztosítható az intézkedés eredményes befejezése, de tilos a tárgyhoz bilincselés alkalmazása járműben történő szállítás közben." [4, 44.§ (3)]

„Nem minősül embertelen, megalázó bánásmódnak a személy, fekvő helyzetben történő megbilincselése, ha arra támadása vagy erőszakos magatartása miatt került sor." [4, 44.§ (4)]

## LŐFEGYVERHASZNÁLAT

„A lőfegyverhasználat csak arra a személyre irányulhat, akivel szemben az FBŐ. törvény 10. §-a (2) bekezdésének *d)* pontjában írt feltételek fennállnak." [4, 44.§ (1)] A FBŐ „az állam működése vagy a lakosság ellátása szempontjából kiemelkedően fontos tevékenység, létesítmény, szállítmány ellen fegyveresen vagy felfegyverkezve intézett támadás elhárítására szájkosár és póráz nélküli szolgálati kutyát vagy lőfegyvert alkalmazhat, illetve használhat." [5, 10.§ (2 *d)*)] „Lőfegyverhasználatnak csak a szándékosan személyre leadott lövés minősül. Nem minősül lőfegyverhasználatnak a véletlenül bekövetkezett, állatra, tárgyra leadott lövés vagy figyelmeztetőlövés." [5, 10.§ (8)] „Személyre szándékosan leadott lövés akkor is lőfegyverhasználatnak minősül, ha az nem okozott sérülést." [4, 44.§ (4)] „A lőfegyverhasználat saját elhatározásból, vagy utasításra történhet." [4, 44.§ (2)] Akkor történhet utasításra, ha a lőfegyverhasználat feltételei fennállnak és az őrparancsnokkal folyamatos, személyes vagy rádiókapcsolat van. „A lövést lehetőleg lábra, ha pedig a támadó kezében a támadásra távolból is felhasználható eszköz van, kézre kell irányítani. A lőfegyverhasználat további alkalmazásának helye nincs, ha az célját elérte." [4, 44.§ (3)] „A figyelmeztető lövést általában függőleges irányban a légtérbe kell leadni. Ha ez nem biztonságos, a lövés irányát úgy kell megválasztani, számolva a becsapódást esetlegesen követő gurulattal is, hogy a lövedék életet, testi épséget ne veszélyeztessen és lehetőleg ne okozzon anyagi kárt." [4, 44.§ (5)] Lőfegyverhasználat esetén az őrparancsnok köteles a helyszín biztosításáról gondoskodni. „A lőfegyverhasználat vizsgálata során a lőfegyvert használó őr és az erre utasítást adó őrparancsnok jelentést ír." [4, 45.§ (1)]

„A lőfegyverhasználatról szóló jelentés tartalmazza:

- mikor, hol, kivel szemben, milyen fegyvert használt, hány lövést adott le, a fegyver típusát, gyári számát,
- a lőfegyverhasználat okát,
- a megelőző intézkedéseket,
- milyen sérülés történt, sor került-e elsősegélynyújtásra, orvosi ellátásra, hol tartózkodik a sérült,
- milyen kárt okozott a lövés, ki a károsult, az őr, illetve a károsult mit tett a kár enyhítésére,
- a helyszínre, a tanúkra, a bűnjelekre és az egyéb körülményekre vonatkozó adatokat

- a fegyverhasználatra feljogosító törvényhelyre történő hivatkozást." [4, 45.§ (2)]

„A lőfegyverhasználatnak nem minősülő lövést (az állatra, tárgyra leadott lövés, a figyelmeztető, a jelző és a vétlenlövés) az őr azonnal szóban jelenti elöljárójának, majd írásos jelentést készít, amely tartalmazza:

- mikor, hol, milyen célból, hány lövést adott le,
- a lövést kiváltó körülményeket, figyelmeztető lövésnél az alkalmazott megelőző intézkedéseket vagy azok mellőzésének okait,
- a lövés irányát és következményét,
- ha a lövés sérülést vagy kárt okozott, annak leírását,
- a lövést követően tett intézkedéseket,
- a helyszínre, a tanúkra, egyéb körülményekre vonatkozó adatokat." [4, 46.§ (1)]

A szolgálati fegyverek és lőszerkészletek tárolási rendjét az igazgató által kiadott utasítás alapján az adott őrségre vonatkoztatva kell meghatározni. Az aktuális utasításban meghatározottaktól eltérni nem lehet. Az őrség szolgálati pisztolyait kizárólag fegyverszobában, azon belül az erre a célra elhelyezett páncélszekrényben tárolhatja. A pisztolyok tárolásba helyezése előtt a tárakból a lőszert ki kell üríteni. A pisztolyokat fesztelenített és biztosított állapotban kell tárolni. A tárolás során az egyik pisztolytárat a pisztolyba, a másikat a pisztolytáska tartaléktár fészkébe kell elhelyezni. A pisztolyokhoz a norma szerint járó lőszereket furatos műanyagszámoló lapon kell a tároló helyen elhelyezni, a páncélszekrény ajtajának belső oldalán dokumentálni kell. [4] [7] [8]

## ÖSSZEFOGLALÁS

Az objektum védelme érdekében a járőrözés az egész területen folyamatos a különböző járőrútvonalakon. A 24 órás fegyveres biztonsági őrség biztosítja, hogy illetéktelenek ne juthassanak be az objektum területére, mindezt szigorú szabályok közt teszik, illetve az előírásokat betartva. Az élőerős védelem megszervezése során számításba kell venni, hogy a szolgálatot ellátó járőr megbetegedés esetén leváltásra kerülhet. Előre bejelentett betegség esetén a készenlétben lévő személyt ki kell értesíteni, szolgálatba kell vezényelni szolgálatteljesítési kötelezettség céljából. Szolgálatteljesítés során előfordulhat, hogy fegyverhasználatra kerül sor, aminek több kiváltó oka lehet, de erre a teljes fegyveres biztonsági őrségnek fel kell lennie készülve, s a lehető legjobban és leggyorsabban kell reagálnia minden esetlegesen kialakuló szituációban. Az objektum elhelyezkedésének tekintetében fontos tényező, ha egy erdős területről beszélünk, ahol vadászat folyhat a környéken, mely igencsak zavaró lehet az őrség számára, mivelhogy hallják a lövéseket a távolból. Az esetek túlnyomó többségében ez a tevékenység a vadásztársaságok által be van jelentve, s az őrségparancsnok ezt tudtára is adja a szolgálatban lévő állománynak, tehát ha a lejelentett időpontban lövéseket hallanak a távolból, akkor valószínűsíthető, hogy a vadásztársaság elkezdte a vadászatot. Ilyen esetben, ha a járőrök nem észlelnek, ezek tudatában persze, rendellenességet, akkor azt jelentik az őrparancsnoknak, hogy nem őket ért támadásból hallatszódnak a lövések, így nincs szükség készenlét fokozására, vagy bárminemű egyéb beavatkozásra. A fegyveres biztonsági őrségnek bárminemű riasztásra, legyen az tűzvédelmi vagy behatolás jelzés, kész kell lennie megkezdeni a kialakult helyzet szakszerű és a biztonsági előírásoknak megfelelő intézkedéseket, tevékenységeket.

## FELHASZNÁLT IRODALOM

[1] BEREK L. – BEREK L. – RAJNAI Z., *A tudományos kutatás folyamata és módszerei*. Óbudai Egyetem, 2022. [Online] https://oda.uni-obuda.hu/handle/20.500.14044/25308

[2] BEREK L. – BEREK T. – BEREK L., *Személy- és vagyonbiztonság*. Óbudai Egyetem, 2016. [Online] http://nbn.urn.hu/N2L?urn:nbn:hu-6315

[3] TÓTH A. – TÓTH L., *Biztonságtechnika*, Nemzeti Közszolgálati Egyetem, 2014. [Online] https://www.scribd.com/document/391792597/Biztonsagtechnika-2014-222p-pdf

[4] 27/1998. (VI. 10.) BM rendelet a fegyveres biztonsági őrség Működési és Szolgálati Szabályzatának kiadásáról, [Online] https://net.jogtar.hu/jogszabaly?docid=99800027.bm

[5] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról, [Online] https://net.jogtar.hu/jogszabaly?docid=99700159.tv

[6] 2012. évi I. törvény a munka törvénykönyvéről, [Online] https://net.jogtar.hu/jogszabaly?docid=a1200001.tv

[7] GYÖNGYÖSI E., *Szakmai ismeretek Fegyveres Biztonsági Őr*, 2022, [Online] https://www.bv.gov.hu/sites/default/files/fegyveres_biztonsagi_or-szakmai_ismeretek_signed_9344449_2_20221003114030.pdf

[8] 253/2004. (VIII.31.) Kormányrendelet a fegyverekről és lőszerekről, [Online] https://net.jogtar.hu/jogszabaly?docid=a0400253.kor

DOI: https://doi.org/10.12700/btsz.2025.7.3.49

# CASE STUDIES OF POTENTIALLY HAZARDOUS NEAR-EARTH OBJECTS WITH PRE-IMPACT DETECTIONS THREATENING CRITICAL INFRASTRUCTURES

# ESETTANULMÁNYOK AZ ELŐRE JELZETT BECSAPÓDÁSÚ POTENCIÁLISAN VESZÉLYES FÖLDKÖZELI OBJEKTUMOK KRITIKUS INFRASTRUKTÚRÁKAT VESZÉLYEZTETŐ EDDIGI ESETEIBŐL

REZSABEK Nándor[1]

**Abstract**

In recent years, the detection, discovery and investigation of so-called Pre-Impact Detection or Past Impactor Potentially Hazardous Objects (PHO) Near-Earth Objects (NEO) have been a prominent area in the research of small celestial bodies in the Solar System. As a result, their monitoring has become a separate sub-area in terms of managing the cosmic risk posed by extraterrestrial objects. The aim of this study is to present the planetary background, the history of the detection of these celestial bodies, their monitoring systems, their number and their characteristic physical properties. From the investigations aimed at this, it is also to present in detail, as a case study, a case of high importance from a civil, military and scientific perspective, which fundamentally affects the issue of security and has potentially endangered a civil and national defense critical infrastructure.

**Keywords**

extraterrestrial objects, pre-impact detections, asteroids, meteoroids, meteorites, critical infrastructures

**Absztrakt**

A Naprendszer apró égitestjeinek kutatásában az elmúlt években kiemelt területet jelentett az ún. előre jelzett becsapódású (Pre-Impact Detection vagy Past Impactor) potenciálisan veszélyes (Potentially Hazardous Object, PHO) földközeli objektumok (Near-Earth Objects, NEO) felismerése, felfedezéseik és vizsgálatuk. Mindezek eredményeképp az extraterresztrikus objektumok jelentette kozmikus kockázat kezelése szempontjából már külön részterületet jelent ezek monitorozása. Jelen tanulmány célja, hogy egyrészt bemutassa ennek bolygótani (planetológiai) hátterét, ezen égitestek detektálásának történetét, monitoring rendszereiket, számosságukat, jellemző fizikai tulajdonságaikat. Erre irányuló vizsgálataiból pedig esettanulmányként részletesen ismertessen civil, katonai és tudományos szempontból is kiemelt fontosságú, a biztonság kérdéskörét alapvetően érintő egy-egy polgári és honvédelmi kritikus infrastruktúrát potenciálisan veszélyeztető eddigi esetet.

**Kulcsszavak**

extraterresztrikus objektumok, előre jelzett becsapódású égitestek, kisbolygók, meteoridok, meteoritok, kritikus infrastruktúrák

[1] rezsabek.nandor@stud.uni-nke.hu | ORCID: 0009-0002-4885-4438 | PhD student, Ludovika University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering | PhD hallgató, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola

## BEVEZETÉS

Ha nem is a precedenst jelentő legelső, 2008-as Szudánban földet ért esettől (1. Ábra), de a második, 2014-ben az Atlanti-óceánba hulló kisbolygótól kezdődően az ún. előre jelzett becsapódású objektumok kutatási eredményei és népszerűen megfogalmazott információi messze túlmutattak a szakmai publikációkon, valamint ismeretterjesztő orgánumok beszámolóin, így esetről esetre a napi sajtóban is megjelentek. Mindennek a társadalmi érdeklődésnek, valamint a biztonság iránti lakossági elvárásnak fontos szerepe lehetett abban, hogy megfigyelésük, esetleges megtalálásuk és vizsgálatuk, továbbá monitoringjuk a Földet veszélyeztető potenciálisan veszélyes földközeli objektumok között idővel külön kategóriát képzett. Ezen túlmenően a kozmikus kockázatokkal mind alap- és alkalmazott kutatási, sőt űrszondás megoldásokkal (DART, Hera) a kísérleti fejlesztési szinten is foglalkozó két nagy űrhivatal, az amerikai NASA és az európai ESA dedikált tudományos központjai külön monitoringrendszert alakítottak primer adataik gyűjtésére és nyilvántartásukra.

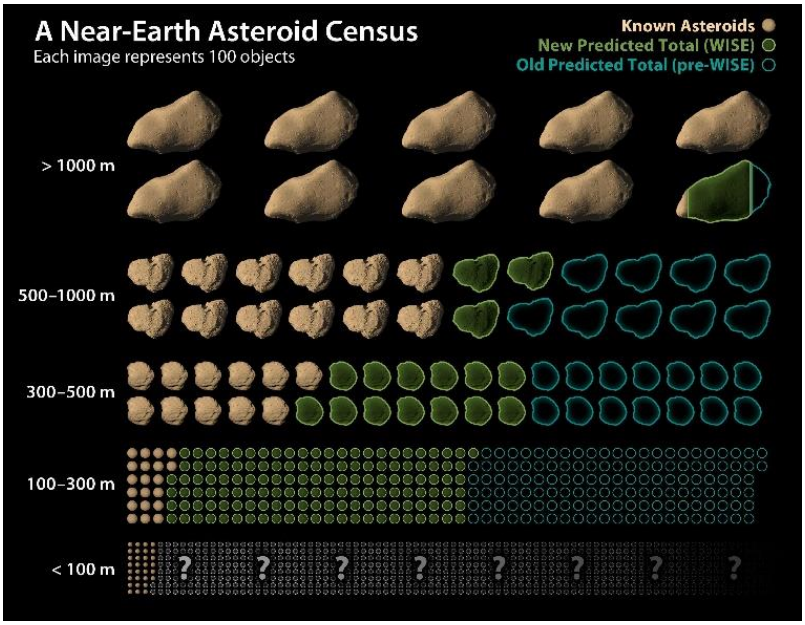

*1. Ábra:A 2008 TC3 aszteroida földet ért darabjainak keresése Szudánban, valamint a megtalált, és Almahata Sitta néven meteoritként klasszifikált fragmentjei a szerző magángyűjteményében, https://upload.wikimedia.org/wikipedia/commons/8/86/323176main_line3rdday_946-710.jpg – Rezsabek L. fotó*

Jelen publikáció szerzője a Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola *Katonai környezetbiztonság* kutatási területén, a *Környezet és a biztonság kapcsolata* kutatási témában kidolgozás alatt álló, *Extraterresztrikus objektumok becsapódása és következményeinek kezelése a kritikus infrastruktúrák vonatkozásában* munkacímű értekezése részkutatásaként vizsgálta az előre jelzett becsapódású potenciálisan veszélyes földközeli objektumokat. Általánosságban bolygótani (planetológiai) hátterüket, detektálásuk mikéntjét, monitoring rendszereiket, számosságukat, jellemző fizikai tulajdonságaikat. Másrészt dedikáltan egy-egy esettanulmányban összegezte a polgári és honvédelmi kritikus infrastruktúrákat (KI) veszélyeztető egyes eseteit. A *Biztonságtudományi Szemle* mostani számában ennek eredményeit foglalja össze.

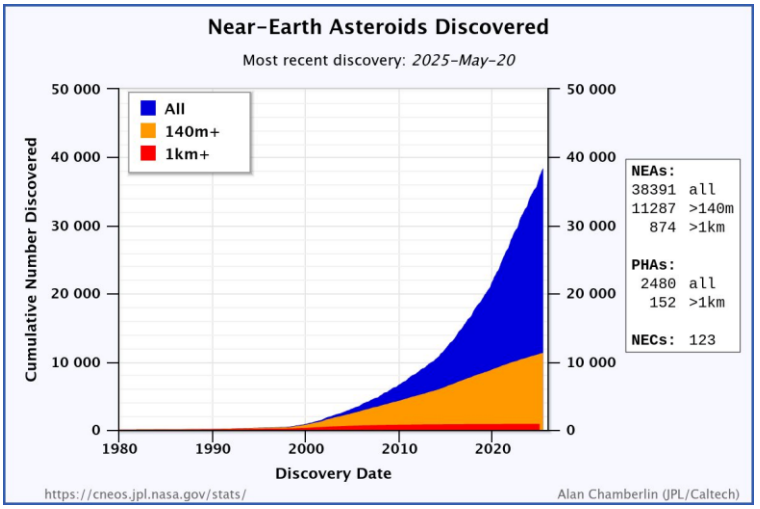
## A TUDOMÁNYOS PROBLÉMA ÉS KUTATÁSI MÓDSZERTANA

A World Economic Forum világméretű kockázatokat elemző aktuális riportja 2024–2025-ös felmérésére alapozva 33 globális veszélyeztetettséget listáz. Ezek között a környezeti problémák csoportján belül nevesíti a nem időjárási jellegű természeti katasztrófákat. Leírásában tételesen említi az extraterresztrikus kockázatokat is, egyik példaként pedig a kisbolygóbecsapódásokat. Olyan eseményként, amely emberéletben és az ökoszisztémában is kárt tehet, infrastrukturális vagy gazdasági károkat okozhat [9 pp. 74–77.].

A 2010-es évektől már jól ismert, hogy az ilyen jellegű planetáris kockázat elsősorban a Földet veszélyeztető kisebb objektumok esetében áll fenn, mivel ezeket korábban nem, vagy csak jóval kisebb arányban detektálták, így nem is készülhettek fel esetleges károkozásukra. Az erre vonatkozó, két esztendővel korábbi adatokokon nyugvó 2013-as eredmények [10] például azt mutatták, hogy főleg a 100 m alatti égitestek esetében (2. Ábra) rendkívül alacsony a felfedezett égitestek aránya. A legfrissebb, 2025-ös adatok [12] szerint ugyan exponenciális növekedés jellemzi (3. Ábra) a (földközeli objektumokon belül) a földközeli kisbolygók (NEA) számát, sőt potenciálisan veszélyes objektumok (PHO) között a 140 m alatti kisbolygók (PHA) száma is lineárisan nőtt, ugyanakkor az előre jelzett égitestek megismerésével valós fenyegetéssé váltak az korábban „hiányzó” objektumok.




*2. Ábra: A katalogizált NEA-k nagyságrendje egyes mérettartományokban (2011.09.29-ig) https://planetary.s3.amazonaws.com/web/assets/pictures/20130314_PIA14734.jpg*




*3. Ábra: A felfedezett NEA-k száma az idő függvényében (2025.05.21-ig), https://cneos.jpl.nasa.gov/stats/totals.html*

Ennek megfelelően az előre jelzett becsapódású objektumok első detektálása, majd tudományos alapú vizsgálatának kezdete jelentette azt a kiemelkedően fontos tudományos mérföldkövet ezen kisebb mérettartományba eső, a becsapódás esélyével fenyegető aszteroidák/meteoroidok kutatásában, továbbá az impakt eseményekeikre való felkészülésben.

Vizsgálatukat azonban érdemes kiterjeszteni a civil es katonai létfontosságú rendszerek esetleges fenyegetettségére is. Mindez egyelőre nem kapott kellő figyelmet a téma természettudományos kutatói, valamint a szabályzók megszületését előmozdító döntéshozók körében. A cikkben ismertetett részkutatás relevanciáját főképp ez jelenti.

Kutatási módszertanában a vonatkozó szakirodalom feltárását, szakmai adatbázisok primer információinak szekunder adatta történő feldolgozását, térképi alkalmazások használatát, illetve hazai jogszabályi szemlézést alkalmazva.

## A TÉMA BEMUTATÁSA ÉS KUTATÁSI EREDMÉNYEI

### A téma alapfogalmai

*Kisbolygó (aszteroida):* 1 m feletti, kő/fém/kő–fém összetételű égitest vagy égitesttöredék. A Mars és a Jupiter közötti belső, valamint a Neptunuszon túli külső kisbolygóövben (Kuiper-öv) találhatók; a bolygónkat megközelítők a földközeli objektumok közé tartoznak.

*Meteoroid:* Légkörön kívüli kozmikus pályán tartózkodó, nanométerestől 1 m-ig terjedő porszemcse, vagy apró kő/fém/kő–fém összetételű égitest vagy égitesttöredék.

*Üstökös (kométa):* Jégbeágyazott kőzetmaggal bíró égitest, mely a Naprendszer külső régiójában található gömbszimmetrikus Oort-felhőből származik. A Napot megközelítve alakul ki légköre, a kóma, valamint ion- és porcsóvája.

*Meteor (hullócsillag):* A légkörbe belépő kisbolygó/meteoroid felizzása–ionizációja okozta légköri–csillagászati jelenség. Adott fényességhatár felett tűzgömbnek, légköri robbanása esetén bolidának hívjuk.

*Meteorit:* A meteorjelenség során a kisbolygó/meteoroid légköri áthaladást túlélő darabja(i); részben vagy egészben földet is érthet.

*Impakt esemény (meteorit- vagy kisbolygó becsapódás):* A felszínt elérő, azzal ütköző kozmikus test okozta kataklizmikus jelenség.

*Impakt kráter (becsapódási kráter, meteoritkráter, asztroblém, asztrobléma):* Kisbolygó- / meteoritbecsapódás során létrejövő felszíni alakzat.

*Földközeli objektum (földsúroló, Near-Earth Object, NEO):* Olyan kisbolygó/meteoroid (Near-Earth Asteroid, NEA) vagy üstökös (Near-Earth Comet, NEC), amelynek pályája meghatározottan közeli bolygónk pályájához képest.

*Potenciálisan veszélyes objektum (Potentially Hazardous Object, PHO):* Olyan kisbolygó/meteoroid (Potentially Hazardous Asteroid, PHA) vagy üstökös (Potentially Hazardous Comet, PHC), melynek pályamozgása feltételezi egy esetleges kozmikus ütközés lehetőségét.

*Előre jelzett becsapódású objektum (Pre-Impact Detection vagy Past Impactor):* A becsapódás/hullás előtt, még kozmikus pályáján, felfedezett potenciálisan veszélyes földközeli objektum.

**Az előre jelzett becsapódások**

Naprendszerünk kisbolygóinak és üstököseinek három fő rezervoárját különíthetjük el: az aszterodiákat vagy a Mars és Jupiter közötti fő kisbolygóövben, vagy a Neptunuszon túl, Kuiper-övben találjuk; a kométákat a külső Naprendszer gömbszimmetrikus halójában, az Oort-felhőben. A bolygórendszerünk dinamikájából következő hatások révén pályájuk módosulthat, és ezek az égitestek válhatnak földközeli objektumokká (NEO), illetve részhalmazuk potenciálisan veszélyes objektumokká (PHO).

Az előre jelzett becsapódású (Pre-impact Detection, Past Impactors) objektumok alapvető ismérve, hogy még kozmikus pályájukon, a földi légkörön kívül detektálják őket. Földi a becsapódásuk vagy hullásuk ezt követően röviddel, néhány nappal, sőt akár pár órán belül következhet be. Egyben vagy aprózódva szárazföldi területre, vagy víztestbe érkezhetnek.

Az első ilyen típusú felefedezésre 2008-ban került sor; ez az égitest a 2008 TC3 jelölést kapta [8]. Utóbb a szudáni sivatagi környezetben megtalált meteoritdarabjait [6] Almahata Sitta néven klasszifikálták. Környezetbiztonsági jelentőségük felismerésére a második bekövetkezési esettől (2014 AA) került sor. Kampányszerű megfigyelésük és monitorozásuk ezután indult el. A 2008-tól 2025-ig terjedő időintervallumban 11 felfedezés történt.

Ebből 3 magyarországi megfigyelés eredménye (2022 EB5, 2023 CX1, 2024 BX1) [18]. A HUN-REN kutatói hálózat Csillagászati és Földtudományi Kutatóközpont Konkoly Thege Miklós Csillagászati Intézetben Sárneczky K. észlelte elsőként ezeket. A magyar felfedezések tudományos és financiális hátterét a GINOP-2.3.2-15-2016-00003 jelzetű „Kozmikus hatások és kockázatok” projekt biztosította [2 pp. 1–2.].

**Az előre jelzett becsapódások monitoringja**

Az előre jelzett becsapódások adatait mind az amerikai (NASA), mind az európai (ESA) űrhivatal monitoring rendszerei listázzák. Így a legmegbízhatóbb, a jelen kutatások szempontjából primer adatforrásának a Center for Near Earth Object Studies (CNEOS) [18] és az Near-Earth Object Coordination Centre (NEOCC) [17] információit lehet tekinteni.

| CNEOS (NASA) | NEOCC (ESA) |
|---|---|
| 2008 TC3 | 2008TC3 |
| 2014 AA | 2014AA |
| 2018 LA | 2018LA |
| 2019 MO | 2019MO |
| 2022 EB5 | 2022EB5 |
| 2022 WJ1 | 2022WJ1 |
| 2023 CX1 | 2023CX1 |
| 2024 BX1 | 2024BX1 |
| 2024 RW1 | 2024RW1 |
| 2024 UQ | 2024UQ |
| 2024 XA1 | 2024XA1 |

*1. Táblázat: Az előre jelzett becsapódású égitestek lajstromozása a CNEOS és NEOCC monitoringrendszereiben (2025. május 21-ig), saját szerkesztés*

A két adatbázis által előre jelzett becsapódásúként klasszifikált objektumokat összehasonlítva (1. Táblázat) teljes egyezést találunk. Mind a CNEOS, mind a NEOCC ugyanazt a 11 égitesteket listázza. Kismértékű eltérés mindösszesen írásmódjuk szintaktikájában van. Ebből a szempontból a Naprendszer égitestjeinek nevezéktanában határozó Nemzetközi Csillagászati Unió (International Astronomical Union, IAU), azonban belül is az apró égitestek tekintetében illetékes Kisbolygókutató Központ (Minor Planet Center, MPC) írásmódja a perdöntő [16]. Ennek megfelelően mindegyik esetben a névben található évszám után szóköz szükséges (azaz a CNEOS által használt forma).

| CNEOS (NASA) | NEOCC (ESA) |
|---|---|
| megnevezése | sorszáma |
| felfedezés időpontja (UTC) | objektum megnevezése |
| becsapódás időpontja (UTC) | átmérő (m) |
| észlelés és becsapódás közti idő (hh:mm) | becsapódás dátuma / időpontja (UTC) |
| mérettartomány (m) | becsapódás sebessége (km/s) |
| földrajzi szélesség (fok) | becsapódás pályaszöge (fok) |
| földrajzi hosszúság (fok) | becsapódás irányszöge (fok) |
| magasság (km) | becsült energia (kt) |
| pálya megtekintése | becsült energiája más forrásokban (kt) |
| felfedező obszervatórium | történet |
| felfedezésről tudósító körlevél | |
| hivatkozások | |

*2. Táblázat: Az előre jelzett becsapódású égitestek monitoringrendszerei által használt adatstruktúra összehasonlítása (2025. május 21-ig), saját szerkesztés*

Az egyes objektumokról nyilvántartott adatok struktúráját (2. Táblázat) összevetve az állapítható meg, hogy a CNEOS 12, a NEOCC 10 paramétert rögzít. Kissé eltérő megfogalmazásokkal ebből 4 kategória azonos (elnevezés, becsapódás ideje, méret, referencia). Megállapítható, hogy a 2 adatbázis együttes használata adja az ebből következő szekunder

adatok képzéséhez a legteljesebb eredményt. Ezen túl további paraméterek, információk és kutatási eredmények háttéranyagként a megadott referenciaoldalakon úgyszintén elérhetők.

**Az előre jelzett becsapódású objektumok sorsa**

Az előre jelzett becsapódás során a légköri zuhanást túlélő, ugyanakkor a földi óceánokba/tengerekbe zuhanó égitestek/égitestdarabok megtalálására nincs mód. Azok a planetáris eredetű objektumok azonban, amelyek szárazföldön landolnak, esetlegesen fellelhetők.

Meteoritként történt földet érésük esetén paramétereik az egyesült államokbeli Meteoritikai Társaság (Meteoritical Society) által fenntartott, az érintett nemzetközi szakmai közösség által referenciának tekintett Meteoritical Bulletin Database (Metbull) adatbázisból [15] nyerhetők ki.

| Előre jelzett becsapódású objektum | Darabszám |
|---|---|
| óceánba/tengerbe zuhant | 6 |
| földfelszínt ért és megtalálták | 4 |
| földfelszínt ért, de nem gyűjtötték be | 1 |

*3. Táblázat: Előre jelzett becsapódású objektumok sorsa (2025. május 13-ig), saját szerkesztés*

A CNEOS, a NEOCC és a Metbull adatait vizsgálva megállapítható, hogy az előrejelzett aszteroidák/meteoroidok közül 6 az óceánba/tengerbe zuhant; 4 földfelszínt ért, és meteoritként megtalálták; 1 földet ért ugyan, de ezidáig nem gyűjtötték be (3. Táblázat).

| Meteoroid / aszteroida | Meteorit | Év | Hely | Meteorit-típus | Tömeg |
|---|---|---|---|---|---|
| 2008 TC3 | Almahata Sitta | 2008 | Nahr an Nil, Szudán | ureilite-an | 3950 g |
| 2018 LA | Motopi Pan | 2018 | Ghanzi, Botswana | howardite | 215 g |
| 2023 CX1 | Saint-Pierre-le-Viger | 2023 | Seine-Maritime, Normandia, Franciarország | L5-6 | 1200 g |
| 2024 BX1 | Ribbeck | 2024 | Brandenburg, Németország | aubrite | 1800 g |

*4. Táblázat: Előre jelzett becsapódás során földet ért meteoritok (2025. május 13-ig), saját szerkesztés*

Mind a 4 meteorittípus a kőmeteoritok közé tartozik; legnagyobb össztömegben (3950 g) a 2008 TC3-ból származó Almahata Sitta darabjait találták meg (4. Táblázat). A Motopi Pan howardit csoportjának – így értelemszerűen az 2018 LA-nak is – a feltételezett szülőégitestje a legnagyobb méretű kisbolygó, a (4) Vesta; míg a Ribbeck – és a 2024 BX1 – esetében az 1982-ben Lovas M. által meglelt (3103) Eger aszteroida.

A 2023 CX1 és a 2024 BX1 aszteroida/meteoroid is hazai, a Csillagászati Intézeti találat [18]. A 2023 CX1-ből származó Saint-Pierre-le-Viger franciaországi [4], valamint a 2024 BX1-ből eredő Ribbeck (4. Ábra) meteorit németországi [5] szórásmezőin is sikerrel gyűjtött be példányokat (mindkét esetben) a Magyar Meteoritikai Társaság Kereszty Zs. vezette keresőexpedíciója, továbbá (a német hullásnál) a Német Űrkutató és Űrtudományi

Központ (Deutsches Zentrum für Luft- und Raumfahrt, DLR) egyik magyar munkatársa, továbbá egy privát hazai keresőcsoport.


*4. Ábra: A 2024 BX1 földfelszínt ért, majd utóbb Ribbeck néven klasszifikált meteorit darabjai, saját fotó*

## Az impakt eseményekhez kapcsolható hazai jogszabályok feltárásának tapasztalatai

A hazai jogrendben a Naprendszer planetáris kockázatot jelentő apró égitestjeivel összefüggő vonatkozás mindössze néhány, a kutatási témától független vonatkozásban szerepel. Ilyen az oktatás, a muzeális gyűjteményi előírások, a frekvenciasávok elosztása, a rádióamatőr tevékenység.

A 2024 végén kivezetett 2012. évi CLXVI. törvény [20] és végrehajtási rendeletei (65/2013. (III. 8.) Korm. Rendelet [21]; 359/2015. (XII.2.) Korm. rendelet [22]) ugyanakkor nem tettek említést a polgári és honvédelmi létfontosságú rendszerek tekintetében extraterresztrikus veszélyeztetettségről.

A 2025 elejétől hatályos 2024. évi LXXXIV. törvény [23] és végrehajtási rendeletei (474/2024. (XII. 31.) Korm. rendelet [24]; 475/2024. (XII. 31.) Korm. rendelet [25]) esetében a polgári kritikus infrastruktúráknál már megjelenik a világűr fogalma, de leszűkítve annak űralapú szolgáltatásaira, honvédelmi tekintetben továbbra nincs erre vonatkozó utalás.

Megállapítható tehát, hogy sem a nemzetközi eredménynek számító hazai felfedezések, sem a jelentős finanszírozással megvalósult „Kozmikus hatások és kockázatok” projekt nem hozott áttörést abban, hogy mindez a kritikus civil, valamint a katonai infrastruktúrák tekintetében jogszabályi vonatkozásban is megfogalmazásra, vagy egyáltalán említésre kerüljön.

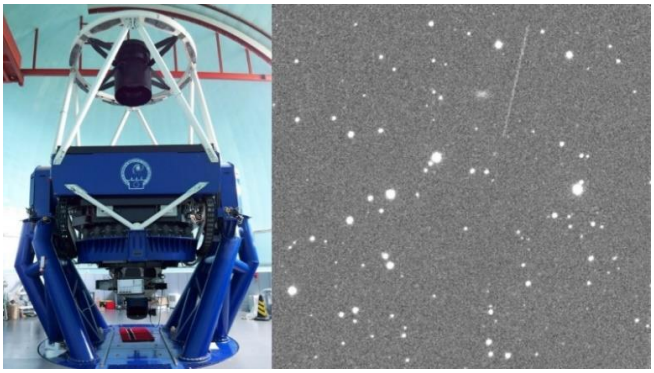
## ESETTANULMÁNY I – POLGÁRI KRITIKUS INFRASTRUKTÚRÁK VESZÉLYEZTETETTSÉGE

| Becsapódó objektum: 2024 XA1 | Ország | Földrajzi egység | KI távolság a becsapódástól | KI ágazat | KI alágazat | KI alapvető szolgáltatás | Felszíni geológia |
|---|---|---|---|---|---|---|---|
| Földet érés | Oroszország | Jakutföld | | | | | mészkő |
| Veszélyeztetett KI | Oroszország | Jakutföld | 89 km | Közlekedés | Légi közlekedés | Oljokminszk repülőtere | mészkő |

*5. Táblázat: A 2024 XA1 földet érésének polgári KI elemeket veszélyeztetető paraméterei, saját szerkesztés*

2024. december 3-án a 0,7 m átmérőjű C0WEPC5 (ideiglenes) jelzetű (előre jelzett becsapódású) meteoroid (5. Ábra) 7 órával felfedezése után Szibéria felett a légkörbe lépett [1]. A tizenegyedikként (ezidáig utolsóként) felfedezett előrejelzett objektum utóbb a 2024 XA1 megnevezést kapta. A modellszámítások azt mutatták, hogy meteoritként a tajgában földet is érhetett, valamint becslést adtak arra, hogy a szórásmezőn vélhetően hol és mekkora tömegű darabjai találhatók meg egy esetleges később in situ keresőexpedíció során [17].

A szórásmező alig 11 km-re húzódik az oroszországi Jakutföld (Szaha Köztársaság) Kilier községétől, valamint igen közel Oljokminszk városától. A 8455 lakosú, Léna parti településen többek között a közlekedési KI, ezen belül a vízi és a légi közlekedési alágazatba tartozó létfontosságú létesítmények települtek [11]. Ezek közül az oljokminszki repülőtértől az égitest becsapódás távolsága mindössze 89 km-re [13] következett be (5. Táblázat).



*5. Ábra: A 2024 XA1 elhaladása az égbolton, valamint a pályaszámítását segítő egyik megfigyelésének eszköze, a Kínai Tudományos Akadémia, Yunnan Obszervatórium 2,4 m-es Lijiang távcsöve, https://news.cgtn.com/news/2024-12-07/China-s-observatories-capture-images-of-falling-near-Earth-asteroid-1z8aadMNTQQ/p.html*

## ESETTANULMÁNY II – KATONAI KRITIKUS INFRASTRUKTÚRÁK VESZÉLYEZTETETTSÉGE

| Becsapódó objektum: 2022 EB5 | Ország | Földrajzi egység | KI távolság a becsapódástól | KI ágazat | KI alágazat | KI alapvető szolgáltatás | Felszíni geológia |
|---|---|---|---|---|---|---|---|
| Földet érés | Norvégia | Norvég-tenger | | | | | vízfelület |
| Veszélyeztetett KI | Norvégia | Jan Mayen-sziget | 101 km | Honvédelem | Honvédelmi szempontból fontos rendszerek és létesítmények | NATO LORAN C rádiónavigációs hálózat állomása (2015-ig) | bazalt |

*6. Táblázat: A 2022 EB5 víztestbe érkezésének honvédelmi KI elemeket veszélyeztetető paraméterei, saját szerkesztés*

2022. március 11-én az összességében ötödik (a magyarországi felfedezések közül az első) előrejelzett becsapódású, 2022 EB5 jelzetű kisbolygó Grönlandtól keletre, Izlandtól északra az Atlanti-óceánba peremtengerét jelentő Norvég-tengerbe zuhant. Mindez a norvég felségterületet is jelentő Jan Mayen-szigettől (6. Ábra) délre következett be [17]. A kisbolygó vélhetően szilikátos összetételű, a szenes kondrit meteoritokkal rokon, C-típusú; átmérője 5–6 m-es. Még a légkörben feldarabolódott, majd úgy zuhant a tengerbe [3].

Ennél az esetnél már konkrétan honvédelmi rendszerelemek sérülékenysége is napirendre került: a szigeten ugyanis 1959 és 2015 között a NATO LORAN C rádiónavigációs hálózatának egyik állomása üzemelt [7]. A tengerbe zuhanó test az ottani távolságokat figyelembe véve igen közel, 101 km-re [13] landolt a honvédelmi szempontból fontos rendszerek és létesítmények közé sorolt KI elemtől (6. Táblázat).

A külső erők jelentette kockázat mellett érdemes a sziget kapcsán szót ejteni a belső erők által kiváltott kockázatokról is. A Jan Mayen térségében igen jelentős a földrengés veszélyeztetettség. A LastQuake adatbázis csak ebben ez évben (2025. május 18-ig) 29, a Richter-skála a szerinti 2,0 magnitúdónál erősebb földrengést listáz. A legjelentősebb, 6,5 erősségű fészekmélysége 10 km, epicentrumának koordinátái é. sz. 71,1895 ny. h. 8,0133 voltak [14]. Az itteni tűzhányó tevékenység kiváltó oka a forrópontos vulkanizmus. A Volcanoes of the World adatai szerint tűzhányója, a Beerenberg rétegvulkán utolsó kitörése 1985-ben zajlott [19].

*6. Ábra: A 2022 EB5 által veszélyeztetett Jan Mayen-sziget ábrázolása egy 1967-es szovjet katonai térképen, https://upload.wikimedia.org/wikipedia/commons/a/ab/R-29-IX-X-XI_200-K_1967_Jan_Mayen.jpg*

## ÖSSZEGZETT KÖVETKEZTETÉSEK

Megállapítható, hogy az előre jelzett becsapódású (Pre-Impact Detection vagy Past Impactor) potenciálisan veszélyes (Potentially Hazardous Object, PHO) földközeli objektumok (Near-Earth Objects, NEO) felismerése, felfedezéseik és vizsgálatuk tekintetében a korábban nem lajstromozott, kisebb mérettartományba eső égitestek megtalálására van mód és lehetőség. Detektálásuk, légkörbe lépésük, valamint esetleges földet/vízfelületet érésük azonban összességében alig néhány órányi időtartamú. A polgári és honvédelmi célú kritikus infrastruktúrákat becsapódásuk/hullásuk direkt módon is sújthat. A civil és katonai létfontosságú rendszerekre közelében landolva a földrajzi és földtani környezetet módosítva is képződhet kárterület. A KI elemek vonatkozásában ilyen típusú káreseményekre hazánkban – a felfedezésük tekintetében elért nemzetközi eredmények ellenére – nincs megfelelő törvényi szabályozás.

## FELHASZNÁLT IRODALOM

[1] Antier, K., *Small asteroid to enter Earth atmosphere above Eastern Siberia in a few hours!*, IMO International Meteor Organization, 2024. [Online]. Elérhető: https://www.imo.net/small-asteroid-to-enter-earth-atmosphere-above-eastern-siberia-in-a-few-hours/ [Hozzáférés: 2024.12.03.]

[2] Barta V. et al., *Kozmikus hatások és kockázatok*, Budapest, Magyarország: Csillagászati és Földtudományi Kutatóközpont, 2020, 47 p.

[3] Geng, S. et al., Near-Earth object 2022 EB5: From atmospheric entry to physical properties and orbit, *Astronomy & Astrophysics*, 670, A27, 2023, 11 p.

[4] Kereszty Zs., A magyar meteoritkereső expedíció által talált francia meteorit, *Planetology.hu*, 2023. [Online]. Elérhető: https://planetology.hu/a-magyar-meteoritkereso-expedicio-altal-talalt-francia-meteorit/ [Letöltés: 2025.05.22.]

[5] Kereszty Zs., Ribbeck – új németországi, aubrit meteoritot találtunk!, *Planetology.hu*, 2024. [Online]. Elérhető: https://planetology.hu/ribbeck-uj-nemetorszagi-aubrit-meteoritot-talaltunk/ [Letöltés: 2025.05.22.]
[6] Kiss L. és Sárneczky K., Egy sikeres meteorit-expedíció, *Meteor*, 40, 4, 2010, pp. 9–10.
[7] *Loran Station Jan Mayen*, loran-history.info, 2024. [Online]. Elérhető: https://www.loran-history.info/jan_mayen/jan_mayen.htm [Hozzáférés: 2025.05.23.]
[8] Putsay, M. et al., Meteorbecsapódás a meteorológiai műhold szemével, *Légkör*, 53, 4, 2008, pp. 9–11.
[9] *The Global Risks Report 2025, 20th Edition, Insight Report*, Cologny/Geneva, Switzerland: World Economic Forum, 2025., 104 p.
[10] *WISE's near-Earth asteroid survey*, The Planetary Society, 2013. [Online]. Elérhető: https://www.planetary.org/space-images/wise-near-earth-asteroid [Letöltés: 2025.05.18.]
[11] Солдатов, С., *Олёкминск. Республика Саха (Якутия)*, Народная энциклопедия городов и регионов России „Мой Город”, 2025. [Online]. Elérhető: https://www.mojgorod.ru/r_saha/oljokminsk/index.html [Letöltés: 2025.04.06.]
[12] *Discovery Statistics*, NASA JPL CNEOS Center for Near Earth Object Studies, 2025. [Online]. Elérhető: https://cneos.jpl.nasa.gov/stats/totals.html [Letöltés: 2025.05.21.]
[13] *Google Earth Pro*, Google, 2025. [Letöltés: 2025.05.23.]
[14] *LastQuake*, CSEM / EMSC Centre Sismologique Euro-Méditerranéen / Euro-Mediterranean Seismological Centre, 2025. [Online]. Elérhető: https://m.emsc.eu/ [Letöltés: 2025.05.18.]
[15] *Meteoritical Bulletin Database*, The Meteoritical Society, 2025. [Online]. Elérhető: https://www.lpi.usra.edu/meteor/ [Letöltés: 2025.04.21.]
[16] *MPC Database Search*, IAU MPC Minor Planet Center, 2025. [Online]. Elérhető: https://minorplanetcenter.net/db_search [Letöltés: 2025.05.22.]
[17] *Past Impactors*, ESA NEOCC Near-Earth Object Coordination Centre, 2025. [Online]. Elérhető: https://neo.ssa.esa.int/past-impactors [Letöltés: 2025.05.21.]
[18] *Pre-impact detections*, NASA JPL CNEOS Center for Near Earth Object Studies, 2025. [Online]. Elérhető: https://cneos.jpl.nasa.gov/pi/ [Letöltés: 2025.05.21.]
[19] *Volcanoes of the World*, SI NMNH Global Volcanism Program, 2025. [Online]. Elérhető: https://volcano.si.edu/ [Letöltés: 2025.05.23.]
[20] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv [Letöltés: 2024.11.27.]
[21] *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR [Letöltés: 2024.11.27.]
[22] *359/2015. (XII.2.) Korm. rendelet a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1500359.KOR [Letöltés: 2024.11.27.]
[23] *2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A2400084.TV [Letöltés: 2025.02.22.]

[24] *474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A2400474.KOR [Letöltés: 2025.02.22.]

[25] *475/2024. (XII. 31.) Korm. rendeletaz ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről.* [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A2400475.KOR [Letöltés: 2025.02.23.]

DOI: https://doi.org/10.12700/btsz.2025.7.3.63

# THE FINANCIAL SECTOR IN CYBERSPACE: RISKS, TRENDS, AND STRATEGIC RESPONSES FOR PROTECTING CRITICAL INFRASTRUCTURE

# PÉNZÜGYI SZEKTOR A KIBERTÉRBEN: KOCKÁZATOK, TRENDEK ÉS VÁLASZLEHETŐSÉGEK A KRITIKUS INFRASTRUKTÚRA VÉDELMÉBEN

GULYÁS Olivér[1] – KISS Gábor[2]


## Abstract

This study examines cyberattacks targeting the financial sector, aiming to explore why financial institutions have become primary targets of attacks. The analysis provides an overview of the main types of cyberattacks, their technological, economic, and social impacts, as well as the relevant regulatory frameworks at both and international and EU levels. The research draws on the most recent reports from the European Union Agency for Cybersecurity, the European Parliament, and other professional organizations. Special attention is given to sector-specific vulnerabilities, targeted attack patterns—such as phishing, ransomware, DDoS attacks, and social engineering techniques—and their long-term consequences. An important finding is that cybersecurity vulnerabilities in the financial sector not only result in direct financial losses but may also undermine social stability and political trust. The study concludes with policy recommendations aimed at strengthening regulatory frameworks, enhancing technological defenses, and improving cybersecurity awareness and education for both financial institutions and users.



## Keywords

cyber attack, financial institution, cyber resilience, critical infrastructure, cyber security



## Absztrakt

A tanulmány a pénzügyi szektort érintő kibertámadásokat vizsgálja. Megpróbálja megválaszolni miért váltak a támadások elsődleges célpontjaivá. Az elemzés áttekinti a kibertámadások típusait, azok technológiai, gazdasági és társadalmi hatásait, valamint a nemzetközi és uniós szintű szabályozási kereteket. A kutatás az Európai Unió Kiberbiztonsági Ügynökség, az Európai Parlament és más szakmai szervezetek legfrissebb riportjaira támaszkodik. A tanulmány külön figyelmet fordít a pénzügyi szektor specifikus kockázataira, az azokat célzó célzott támadási mintázatokra – adathalászat, zsarolóvírusok, DDoS támadások és *social engineering* technikák – valamint azok hosszú távú következményeire. Fontos megállapítás, hogy a pénzügyi szektor kiberbiztonsági sérülékenységei nem csupán anyagi károkat okoznak, hanem közvetve a társadalmi stabilitásra és a politikai bizalomra is hatást gyakorolhatnak. A tanulmány zárásként javaslatokat fogalmaz meg a szabályozási környezet erősítésére, a technológiai védekezés fejlesztésére, valamint a pénzintézeti és felhasználói edukáció fokozására.



## Kulcsszavak

kibertámadás, pénzintézet, kiberreziliencia, kritikus infrastruktúra, kiberbiztonság


[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbudai University | doktorandusz, Óbudai Egyetem

[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-9376 | associated professor, Óbudai University | egyetemi docens Óbudai Egyetem

## BEVEZETÉS

A digitalizáció térnyerésével a gazdaság és a társadalom mind nagyobb részét befolyásolja a számítástechnikai rendszerek megbízhatósága és biztonsága. A kibertámadások már nemcsak technológiai kihívást jelentenek, hanem komoly gazdasági, társadalmi és politikai következményekkel is járhatnak. Különösen igaz ezutóbbi a pénzügyi szektorra. A pénzintézetek a gazdaság gerincét képező mechanizmusokat szolgálják ki, és mint ilyenek, fokozottan kitettek a rosszindulatú támadásoknak.

Jelen tanulmány célja, hogy átfogó képet nyújtson a kibertámadások fogalmáról, típusairól és a pénzügyi ágazatra gyakorolt hatásaikról. Különös tekintettel arra, hogy ezen ágazat miként vált napjainkra egyik elsődleges célpontjává a modern kiberfenyegetéseknek. Az Európai Unió, az Egyesült Államok és különböző nemzetközi szervezetek jelentései alapján bemutatásra kerülnek a legfrissebb trendek, támadási módszerek és szabályozási kihívások, amelyek meghatározzák a pénzintézetek kiberrezilienciáját a 21. században.

## A KIBERTÁMADÁSOK FOGALMA ÉS JELENTŐSÉGE

A kibertámadás megnevezés alatt kell érteni minden számítógépek, számítógépes rendszerek ellen indított műveletet. Egy-egy ilyen művelet az adatlopást, az adatok megsemmisítését, de akár a teljes informatikai rendszer elérhetetlenségét, végső esetben teljes tönkre tételét is célozhatja.

Az Európai Parlament egyik elemzésében a kibertámadások demokráciára gyakorolt hatását vizsgálja. Véleményük szerint a „kibertámadások által okozott károk túlmutatnak a gazdaságon és a pénzügyeken, mivel veszélyeztetik a társadalom alapvető működését” [1].

A pénzügyi szektor évszázados működése során már megismerte, felkészült a tradicionális veszélyforrásokra – rossz hitelek, csalások stb. A 21. századtól viszont új veszélyforrásokkal kell szembenézniük. A 2020-as évektől már majdnem minden, a pénzügyi szektort vizsgáló jelentés a kibertámadások veszélyét emeli ki. Jerome Powell, az Amerikai Egyesült Államok központi bankjának szerepét betöltő Federal Reserve elnöke, egy beszédében arra hívta fel a figyelmet, hogy a kiberfenyegetések már nagyobb veszélyt jelentenek az Egyesült Államok gazdaságára, mint a 2008-as, egész világot érintő gazdasági válság [2].

Az épített környezetünket, infrastruktúránkat, az alapvető szolgáltatásokat fenyegető emberi tényezők közé bekerült a magán és állami infrastruktúrát egyaránt veszélyeztető terrorizmus mellé a kiberbűnözés, mint hangsúlyos tényező [3]. 2020-ban az Egyesült Államok kongresszusa a 2001. szeptember 11-i eseményekkel emelte azonos szintre a kiberfenyegetések által jelentett veszélyt. Ugyanez a jelentés azonban arra is figyelmeztetett, hogy az ország nem készült fel ezekre a támadásokra [4].

A számítógépes rendszerekbe való erőszakos behatolás már majdnem minden országban bűncselekmény. Mára már közhelynek számít, de az informatika és az Internet fejlődésével megszűntek a földrajzi korlátok. Ez természetesen igaz a hackertámadásokra is, azok sem maradnak országhatáron belül. Az ilyen támadások felderítésében komoly nehézség a hatóságok tevékenységének összehangolása, hiszen a támadó az egyik ország joghatósága alá tartozik, míg a megtámadott esetében más állam az illetékes. A támadások felderítése akkor válik (szinte) lehetetlenné, ha a támadó mögött az adott ország kormánya áll. A

kormányzati inspirációra elkövetett cselekmények tetteseit így, ha megtalálják, akkor sem vonják felelősségre [5]. A pénzintézetek gazdaságban betöltött szerepüknél fogva emiatt sokszor kormányzatilag szervezett behatolások célpontjaivá válnak [6].

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) évről évre elemzi a kiberfenyegetéseket. A vizsgálatuk mind az európai, mind pedig a globális folyamatokra is kiterjed. Az ENISA legutolsó, 2024-es riportja kiemelte, hogy 2023. július – 2024. június között a kibertámadások száma jelentősen megnőtt. Mind az incidensek sokfélesége, azok száma mind pedig azok következménye „rekordszintre" emelkedett. A folyamatban lévő regionális szintű konfliktusok továbbra is meghatározóak maradtak. A „hacktivizmus" jelensége folyamatosan terjed, számos új csoport jelent meg ezen a területen. A riport kiemeli, hogy a nemzeti vagy európai szinten zajló jelentős események adtak motivációt a megnövekedett „hacktivista" tevékenységhez a vizsgált időszakban (pl. európai választások) [7]. Az ENISA jelentés kiemelte, hogy a kiberincidensek egyre inkább a létfontosságú ágazatokat érintik.

Az ENISA riport hét fő fenyegetést azonosított, ezek közül a három legfontosabb a rendelkezésre állás elleni fenyegetés, ezt követte a zsarolóvírusok és az adatok elleni fenyegetés.

2023. július és 2024. júniusi időszakban a támadások által leginkább érintett ágazatok:

1. Közigazgatás (19%)
2. Közlekedés (11%)
3. Banki/pénzügyi ágazat (9%)
4. Üzleti szolgáltatások (8%)
5. Digitális infrastruktúra (8%)
6. Lakosság (8%)
7. Gyártás (6%)
8. Média (5%)
9. Egészségügy (4%)

*Forrás: Európai Parlament [8]*

## PÉNZÜGYI SZEKTOR, MINT KRITIKUS INFRATRUKTÚRA

A kibertámadások fő motivációi a pénzügyi haszonszerzés, a kémkedés, a rombolás és az ideológiai okok voltak [9]. A pénzügyi szektor pont a korábbiakban említettek gazdaságban betöltött szerepe miatt kerül sokszor a támadások kereszttüzébe.

A pénzügyi rendszerek a gazdaságban betöltött szerepük miatt nemcsak a szó átvitt, de tisztán jogi értelmében is kritikus infrastruktúrák. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény egyértelműen nevesíti azokat az úgynevezett létfontosságú rendszerelemeket, amely ágazatokba tartozó szolgáltatások elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához. A törvény alapján az „1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához." A listán belül kiemelt az egészségügy, a lakosság személy- és vagyonbiztonsági

sága, a gazdasági és szociális közszolgáltatások biztosítása, az ország honvédelme. A jogszabály szövege szerint „ezek kiesése a feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna".

2012. évi CLXVI. törvény 1. sz melléklete kifejezetten nevesíti: „20. Pénzügy pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei 21. bank- és hitelintézeti biztonság 22. készpénzellátás".

Az előzőek alapján a pénzintézetek kritikus infrastruktúrának számítanak. A pénzintézetek átfogó szabályozása emiatt elengedhetetlen. Néha azonban nehéz megtalálni a szabályozás megfelelő mértékét. Szubjektív tapasztalat, hogy amit a pénzintézetektől elvár a szabályozó, például tájékoztatás vagy adatvédelem tekintetében, ugyanazt már nem követeli meg minden szolgáltatótól, például távközlési cégektől.

Bármely pénzintézetet, annak rendszereit érintő kibertámadásnak lehet:

- gazdasági hatása: mert a banki és pénzügyi termékek és szolgáltatások működését érintheti.
- társadalmi hatása: áttételesen a köznyugalmat is megzavarhatja egy bankot érintő kibertámadás – Postabank-pánikhoz hasonló hatása is lehet annak, ha az ügyfelek azt gondolják, hogy nem tudnak hozzáférni a bankban „tárolt" pénzükhöz, mert egy bank rendszere „megsérült" vagy a bank rendszerét „feltörték".
- politikai hatása: áttételesen az állam és intézményei iránti közbizalmat is érintheti, amennyiben egy bankot érintő kibertámadás az adott bank teljes működését is veszélyeztetheti vagy a közvélekedés azt feltételezi, hogy a teljes működést veszélyeztetheti. Az ezáltal kiváltott pánik már a közbizalmat is érintheti.

A pénzintézetek által biztosított pénzügyi műveletek lényegében a reálgazdaság véráramát jelentik. A pénzintézeteket érő kibertámadások így nemcsak a pénz absztrakt áramlását, hanem a mögöttük meghúzódó valós gazdasági tevékenységeket is veszélyeztetik. Az egyébként adatcserére használt kommunikációs hálózaton, fertőzési csatornákon tovaterjedő támadások rendszerszintű problémákat eredményezhetnek. A problémák pedig az ügyfelek bizalmát ingathatják meg. Mivel a pénzügyi szakma alapja a bizalom, a bizalom megingása az adott szolgáltatókon túl mások számára is károkat okozhat. Egy, a bankszektor, vagy más pénzügyi intézmények elleni, összehangolt módon elvégzett kibertámadással akár globális likviditási krízis is okozható [10].

Van azonban egy (al)szektor, ahol sérülnek a pénzügyi rendszerekkel kapcsolatos szigorú szabályozói elvárások. A szabályozás kettős mércéjét mutatja az új típusú digitális, vagy neobankok helyzete. A szereplők sokszor ugyanazokon a piacokon működnek, ugyanazokat a szolgáltatásokat nyújtják, mint a hagyományos vagy divatos szóval „kőbankok". A neobankokra vagy fintech cégekre vonatkozó szabályozás azonban sokkal megengedőbb, mint a „klasszikus" pénzintézetekre vonatkozó. Nincsenek olyan szigorú szabályok, a működésük kevésbé átvilágított, nincsen masszív tőkekövetelmény vagy céltartalékolási elvárás, nem történik meg a rendszerek folyamatos auditja stb. Ez az, ami miatt sokszor rugalmas(abb) szolgálatást tudnak nyújtani. Egy fintech cég csődje esetén azonban hiábavaló lenne a helyi jegybanktól vagy betétbiztosítótól ugyanazt a helytállást elvárni. Ezen cégek esetében nincs szigorú szabályozás, ugyanakkor csőd esetén állami szerepvállalás sem.

Bár egy nagyon fontos iparágról beszélünk, de tekintettel a téma mélységére, jelen vizsgálatnak nem képezi tárgyát a fintech cégek speciális szabályozása.

## KIBERTÁMADÁSOK A PÉNZÜGYI SZEKTORBAN

A kibertámadások fejlődéstörténetét egy korábbi cikkben bemutattuk [11]. A pénzügyi intézmények tekintetében általánosságban elmondhatjuk, hogy a „nagyüzemi", nem igazán válogatós vírus- (féreg) támadások mellett, a célzott, egyedi felhasználókra irányuló offenzívák is megjelentek. Közvetlen támadási célok lehetnek (i) az online vagy offline identitáslopás, (ii) személyes és üzleti adatok ellopása, (iii) bankkártyák és bankszámlák adatainak eltulajdonítása, (iv) illetéktelen behatolás az online felhasználói fiókokba. Bár a fentiek is komoly károkat okoznak, nem ritkák már azok a súlyosabb támadások sem, amelyek célja maga a pénzügyi rendszer megbénítása.

A sok millió dolláros/eurós anyagi veszteség mellett a kibertámadások egyéb károkat is okozhatnak. Legfontosabb talán az ügyfél bizalmának ideiglenes, vagy végleges elvesztése. A különböző technikákkal kivitelezett támadások mára már minden naposakká váltak, ezért a megfelelő színvonalú védelmi intézkedések mellett a vállalat minden dolgozójának éberségére szükség van. A professzionális szinten kivitelezett támadások szükségessé teszik az érintettek közötti együttműködés javítását. A várható haszon nagysága miatt megéri, hogy a pénzintézetek elleni támadásokhoz komoly, időigényes előkészületeket tegyenek [12]. A következőkben a kibertámadások átalakulását fogjuk vizsgálni.

## PÉNZINTÉZETEKET ÉRINTŐ TÁMADÁSOK JELLEMZŐI

Az elmúlt években a pénzügyi szektort érintő kibertámadások olyan mértéket öltöttek, hogy 2024-ben elkészült az első, kifejezetten a pénzügyi szektort vizsgáló ENISA riport is [13]. A riport egyik legfontosabb megállapítása egybecseng a mi korábbi, 2022-es vizsgálatunkkal. A pénzügyi ágazat továbbra is a kiberfenyegetések egyik legfontosabb célpontja marad mivel:

- az intézményekben tárolt (pénzügyi) adatok érzékenyek, nagy értékűek és
- azok ellopásával a támadók jelentős pénzügyi haszonra tehetnek szert.

ENISA 2023. július és 2024. júniusi időszakban 488 nyilvánosan bejelentett, az európai pénzügyi szektort érintő incidenst elemzett. Az ezekből készült riport fő megállapításai az alábbiak [13]:

- Az európai bankok voltak a támadások leggyakoribb célpontjai – 46 %-os arányban. Ezt követik a kormányzati ügynökségek és a pénzügyi szektorban működő közszférabeli szervezetek (13 %). A magánszemélyeket (10 %) pénzügyi jellegű *social engineering* kampányokkal csapták be.
- A pénzügyi szektorban a terheléses, DDoS-tevékenységek a geopolitikai eseményekhez, különösen Oroszország ukrajnai inváziójához kapcsolódtak. A hacktivisták gyakran európai hitelintézeteket (58%) és a kormányzati, pénzügyekkel kapcsolatos weboldalakat (21%) támadták. Céljuk, hogy működési zavart okozzanak és aggodalmat keltsenek a lakosság körében a kiberbiztonsággal, kiberrezilienciával kapcsolatban.

- Kiberincidensek – például csalás, zsarolóvírusok vagy adatvédelmi incidensek – következtében a pénzintézetek gyakran szenvedtek jelentős veszteségeket. Ezeket a veszteségeket tovább növelték a helyreállítással kapcsolatos költségek, a jogi költségek és a hatósági büntetések.
    - Az adatszivárgás továbbra is kritikus kérdés maradt. A támadók pénzügyi haszonszerzés céljából csalás, ellátási láncot érintő támadások (*supply chain attack*) vagy *social engineering* révén használták ki a kritikus sebezhetőségeket. A vizsgált esetek 39 százalékában az európai hitelintézetek voltak az elsődleges célpontjai azon támadásoknak amikor az incidensek effektív pénzügyi veszteségekhez, a szabályozó hatóságok által kiszabott büntetésekhez és „hírnévkárosodáshoz" (*reputational damage*) vezettek.
    - A kiberbűnözők a *social engineering* módszereket alkalmazták legsűrűbben. Az adathalászat (*phishing*), a sms-adathalászat (*smishing*) és a hanglapú adathalászat (*vishing*) voltak a legelterjedtebbek a vizsgált időszakban. Ezen incidensek célja érzékeny információk ellopása és ezeken keresztül pénzügyi csalások elkövetése volt. Az érintettek 38 százaléka magánszemély, 36 százaléka hitelintézet.
    - A csalások az összes incidens 6 százalékát tették ki, elsősorban magánszemélyeket (40 %) és hitelintézeteket (35 %) érintve. Bár a bejelentett esetek száma alacsonynak tűnik, a riport feltételezése, hogy nem került minden incidens lejelentésre. Az egyéb kibertámadásokból eredő másodlagos következmények szélesebb körű problémára utalnak. A kriptovalutákkal kapcsolatos incidensek esetében a lopások, csalások és a pénzmosás száma szintén jelentős mértékben nőtt.
    - A zsarolóvírus támadások elsősorban a kevésbé fejlett pénzügyi szervezeteket, például a szolgáltatókat (29 %) és a biztosítókat (17 %) célozták. A végeredmény: pénzügyi veszteség (38 %), adatszivárgás (35 %) és működési zavarok (20 %).
- A mobiltelefonokat érintő támadások darabszáma és komplexitása tovább emelkedett. A támadó programok egyre kifinomultabbak. A trójai banki programok és a kémprogramok növekvő fenyegetést jelentettek. Segítségükkel a hackerek át tudták venni az uralmat az eszközök felett, képessé váltak az ügyfél nevében tranzakciók végrehajtására. A hitelintézetek (36 %) és a magánszemélyek (24 %) voltak a leginkább érintettek ezekben a támadási típusokban.
- A beszállítói láncot érintő támadások, főként az adatlopás és a zsarolóvírusok, az érzékeny adatok eltulajdonítását és értékesítését (63 %), működési zavarokat (26 %) és pénzügyi veszteséget (11 %) eredményeztek.

## TÁMADÁSOK JÖVŐKÉPE, JAVASLATOK

Ahhoz, hogy a pénzintézetek hosszútávú védelmi stratégiát tudjanak kialakítani nem kell feltétlenül üveggömb. Igaz, hogy a gyorsan változó világ, még gyorsabban változó szegmenséről beszélünk, de nagyon sok támadási vektor már évek óta jelen van. Szeretnénk azt hinni, hogy „személyre szabott" támadás áldozatai vagyunk. De sajnos a legtöbbször

még mindig a régi „trükkök" működnek a legjobban, a régi hiányosságokat használják ki a támadók. Ez várhatóan a jövőben is így fog maradni.

**Jelszókezelés**

Továbbra is azt tapasztaljuk, hogy bár a felhasználók valódiságának ellenőrzésekor már sokszor többlépcsős azonosítást alkalmaznak a bankok, még mindig vannak hiányosságok. A jelszóhasználatban, a lehetséges jelszó erősségben még van hova fejlődni. Hiába szigorodnak a jelszóházirendek, az évről évre megjelenő „leggyakrabban használt jelszavak listája" továbbra is komoly hiányosságokat mutat. Továbbra is letaszíthatatlan a trónról az '123456' [14]. A nem megfelelő jelszóházirendeknek van pénzintézeti oldala – nem szabad engedni a túl gyenge jelszavak használatát –, de az egyének személyes felelőssége nem elvitatható.

Talán ez az egyik olyan információ biztonsági terület, ahol bár nagy a lemaradás, a leggyorsabban lehetne eredményeket elérni. Azonban, ami ritkán képezi a felhasználói edukáció részét, az a személyes és a munkahelyi rendszerekben használt jelszavak szétválasztása. Hiába talál ki egy erős céges jelszót a felhasználó, ha utána ugyanazt használja az otthoni infrastruktúrában is. Előfordul, hogy a jól megjegyzett bonyolult jelszót adja meg a felhasználó az összes felhasználási területen – így a véletlenül felkeresett adathalász oldalakon is.

**Hamis oldalak**

Az adathalászaton belül, a hamis banki oldalak elterjedtsége még mindig magas. Ezt a folyamatot támogatja a kártékony hirdetések és a keresőoptimalizálás-mérgezés (*malvertising* és a *SEO poisoning*). A bűnözők a keresőoptimalizálással, a keresési listák élére kerülő hamis oldalak segítségével lopják el a banki adatokat. A folyamatra egy aktuális példa az elmúlt időszakban végbement hazai bankegyesülés. Az egyesülés után új névvel, új entitás született. Az új bank weblapját, netbankját stb. a jogelőd pénzintézetek ügyfelei még nem ismerték. Az új netbanki oldalt sokan keresőalkalmazások segítségével próbálták megtalálni. A keresési listák élén azonban egy hamis weboldal szerepelt. Az igazira kísértetiesen hasonló oldalon az azonosító, majd a jelszó megadása után a bűnözőknek már könnyű dolga volt. A jelszavakkal végre tudták hajtani a szükséges változtatásokat és hozzáfértek az ügyfelek pénzéhez [15].

**Informatikai támogatás**

A hazai és a nemzetközi pénzintézetek robosztus informatikai rendszereken futnak, az alap-, számlavezető-rendszerek (*core* rendszerek) azonban általában régiek. Azok cseréje szinte lehetetlen a bonyolultság, az évek során végrehajtott sok apró változtatás – kivételkezelések például –, az üzletmenet folytonosság fenntartása miatt. A régi programnyelvek, összetett architektúra, bonyolult szabályrendszerek, redundáns folyamatok miatt a modernizálás, *upgrade*-elés szinte lehetetlen, de mindenesetre nagyon költséges.

**Új technológiák térnyerése**

A pénzügyi szervezetek számára elkerülhetetlen, hogy fejlett(ebb) fenyegetésérzékelő rendszereket építsenek ki. Az olyan új generációs eszközök, mint a behatolásérzékelő-, a behatolásmegelőző rendszerek és a biztonsági információ- és eseménykezelő megoldások képesek lehetnek észlelni az anomáliákat és valós időben reagálni azokra. A mestersé-

ges intelligencia és a gépi tanulás integrálása az előre jelző, elemző és az automatizált védekező rendszerekbe fokozza a kiberrezilienciát. Nem szabad viszont megfeledkezni arról, hogy már a támadók is a mesterséges intelligenciát hívják segítségül.

A következő jelentős kihívást a kvantumszámítógépek fogják jelenteni. A jelenleg működő titkosítási protokollokat teljes mértékben felboríthatják ezek a nagyteljesítményű számítógépek. A kvantumszámítógépek számítási kapacitás, sebessége milliárdszorosa a hagyományos számítógépeknek. Néhány évtizeden (?) belül a ma még „feltörhetetlen" titkosítási algoritmusok néhány perc alatt feltörhetővé válnak. Ráadásul ezek az eszközök nem csak a későbbi titkosításokat fogják ostromolni, hanem a már lemásolt, ma még védett rendszereket, adatokat fogják a jövőben feltörni. Hiába titkosítottunk ma egy adatot. Ez ma még lehet, hogy használhatatlan a tolvajoknak. De lehet, hogy a jövőben már fel fogják tudni törni az ellopott adatokat az új számítógépek segítségével.

**Szolgáltatásként nyújtott támadások**

A kiberbűnözés, ha egy több dimenziós döntési mátrixban figyelembe vesszük a költségeket – a megtérülést – a lebukás kockázatát, jó „alternatívát" jelent a bűnözőknek. Régen talán szempont volt, hogy a megfelelő tudás rendelkezésre álljon. Mostanra azonban már egy teljes specializált hálózat épült fel kiberbűnözési-szolgáltatások nyújtására. Ezen szolgáltatások a legális piacok üzleti modelljeit másolják. Szolgáltatásként nyújtott zsarolóvírusok és kártevők (*Ransomware-as-a Service* – RaaS, *Malware-as-a-Service* – MaaS) már viszonylag alacsony összegekért – havi 100-200 dollárért – már elérhetőek az internet sötét bugyraiban, a *Dark Weben* [16].

**Bűnözői ellátási lánc**

A kiberbűnözési szektorban is megtörtént a specializáció. A különböző lépéseket, már különböző aktorok hajtják végre. Nem ugyanaz a támadó szerzi meg az adatokat, mint aki a végén fel is fogja használni azokat. Lehet, hogy egy hacker célzott támadását megelőzően, egy másik hacker, aki csak figyeli, gyűjti és elemzi az adatokat már hónapok óta a feltört rendszerben „ül". Ezutóbbi alapján egy feltört vállalati jelszó, nem csupán egy fiók kompromittálódását jelenti. Lehet, hogy oldalirányú mozgással a teljes vállalati infrastruktúra, vagy akár több összekapcsolt vállalat megtörését is eredményezi. A támadók gyorsabban mozognak, mint valaha. A CrowdStrike jelentése szerint az átlagos „kitörési idő" – az időablak, mielőtt a támadók megkezdik az oldalirányú mozgást – 2024-ben az előző évi 62 percről mindössze 48 percre csökkent, a leggyorsabb megfigyelt idő pedig 51 másodperc volt. Ezutóbbi azt jelenti, hogy a „védőknek" kevesebb mint egy percük lehet a felderítésre és reagálásra, mielőtt a támadók még mélyebbre hatolnának a vállalati rendszerben. A generatív mesterséges intelligencia kulcsszerepet játszott a folyamat gyorsulásában [17].

A Verizon DBIR riportja szerint az adattolvaj naplók, feketepiacokon közzétett bejegyzések és a zsarolóvírus-áldozatok *domain* neveinek korrelációja azt mutatja, hogy az áldozatok 54 százalékánál már korábban megjelentek hitelesítő adatok a *Dark Weben*. Az áldozatok 40 százalékánál a vállalati e-mail címek voltak a kompromittált hitelesítő adatok [18].

Sajnos mind az *as-a-Service* szolgáltatások, mind pedig a bűnözői ellátási lánc kialakulása nagyon megnehezíti a védelmi szektor működését. Tény, hogy ezekre a folyamatokra is van már védelmi szolgáltatás. A kiszivárgott belépési adatokat, jelszavakat monitorozzák a *Dark Weben* – ha találnak céges adatokat, az előrejelez(het) egy jövőbeni támadást.

Amennyiben azonban mégis megtörténik a baj, elkezdődik a védekezés, majd azt követően a visszaállítás, akkor újabb problémával szembesülhetünk. Mivel a törés és a támadás időben, térben nagyon elválhat egymástól nagyon nagy odafigyelést igényel amikor egy támadás után megpróbáljuk visszaállítani a rendszereinket. Ne forduljon elő, hogy a még mindig fertőzött biztonsági mentésekre térünk vissza.

**Szabályozás**

Az olyan szabályozási keretek, mint a GDPR, a NIS-irányelv és a pénzügyi szereplőkre vonatkozó DORA betartása kulcsfontosságú a kiberbiztonsági ellenálló képesség fenntartásához. Ezek a jogszabályok szigorú elvárásokat támasztanak a pénzintézetek szabályzataival, eljárásaival kapcsolatban. A jogszabályoknak való megfelelés érdekében rendszeres megfelelési ellenőrzéseket, auditokat kell végezni(ük) [13]. A korábbi évek tapasztalata azt mutatja, hogy a szabályozás szigorodása szükséges rossz. Újabb fejlesztési költségek önkéntes vállalása, vagy akár a hamis banki oldalakkal kapcsolatos védekezésben az aktívabb pénzintézeti részvétel nem lenne kikényszeríthető szigorú törvényi előírások nélkül. Amit nem ír elő jogszabály, azt az ügyfelek nem fogják tudni kikényszeríteni.

Egy pénzintézet ritkán tud azzal ügyfelet nyerni, hogy ő a legbiztonságosabb. Az is igaz, hogy azzal már rengeteget tud veszíteni, ha kiderül, hogy nem-biztonságos. Ugyanakkor fontos kiemelni, hogy nehéz meghatározni hol húzódik az egyén felelőssége és hol kell a pénzintézetnek szerepet vállalnia – esetleg anyagilag is helytállnia. Például a korábban említett hamis banki oldal esetében az egyén felelőssége elvitathatatlan. Ugyanakkor vannak olyan vélemények is, amelyek szerint a pénzintézet nem tett meg mindent, hogy eltűnjön a hamis oldal, illetve nem tájékoztatta megfelelően az ügyfeleit.

**Képzés, oktatás**

Nem győzzük hangsúlyozni az egyének, pénzintézeti dolgozók, felhasználók stb. oktatásának fontosságát. „Az ember a leggyengébb láncszem”. Az alkalmazottak képzése, tudatosságnövelő programok alapvető fontosságúak, például a *social engineering* támadások kockázatának csökkentéséhez. A pénzintézetek (vagy általánosságban a vállalatok) folyamatos kiberbiztonsági képzésekkel, szimulált adathalász gyakorlatokkal tudják a kibertudatosságot növelni. Hogy egy előremutató példát is bemutassunk. Nagyon jó kezdeményezés például a KiberPajzs - https://kiberpajzs.hu/.

**BCP - DRP**

Az incidensekre való felkészülés egyik része annak kidolgozása, hogy mit tegyünk, ha már megtörtént a baj. Az incidensekre reagáló működés folytonossági vagy üzletmenet helyreállítási programok, reagálási tervek, jó esetben kommunikációs *roadmap* készítése nagyon fontos. A pénzintézeteknek jól meghatározott incidens tervekkel kell rendelkezniük. Ezek a tervek részletesen kell, hogy meghatározzák a kibertámadás során, majd azt követően a végrehajtandó lépéseket. Ezeket a terveket rendszeresen frissíteni és tesztelni kell. A hatékony tervek pontos intézkedéseket tartalmaznak a kiberincidensek észlelésére, megfékezésére, felszámolására, helyreállítására és a kommunikációjára vonatkozóan [13]. A tervek létrehozása nem önkéntes alapú, azokat a jogszabályok (NIS2, DORA) is előírják.

Fontos kiemelnünk, hogy az utolsó pontok esetében nem elégséges az adott pénzintézet keretein belül maradni. Az oktatásokat, jogszabályi előírásokat vagy akár a helyreállítási terveket ki kell terjeszteni a pénzügyi intézményekkel szimbiózisban, velük „összenőve" működő vállalatokra, harmadik felekre is – *supply-chain security*.

**Együttműködés és információmegosztás**

A pénzügyi intézmények közötti együttműködés és információmegosztás növeli az általános kiberellenálló-képességet. Például az iparági fórumokon való részvétel, a fenyegetésekkel kapcsolatos információk megosztása és a köz- és magánszféra közötti partnerségek (*Public Private Partnership*) segítenek az intézményeknek naprakésznek maradni a felmerülő fenyegetésekkel és a „legjobb gyakorlatokkal" kapcsolatban [13].

## ÖSSZEFOGLALÁS

Összefoglalóan elmondhatjuk, hogy a kibertámadások jelentős veszélyt jelentenek nemcsak gazdasági, hanem társadalmi és politikai szempontból is. A támadások célpontjai között kiemelt helyen szerepel a pénzügyi szektor, amely jogilag is kritikus infrastruktúrának minősül. A kibertámadások célja lehet az adatlopás, de súlyosabb rendszerleállás vagy akár rendszerszintű pusztítás is.

A legtöbb ország kiemelten kezeli ezeket a fenyegetéseket, mivel kihathatnak a társadalmi stabilitásra és a demokráciára is. Azonban a határokon átnyúló támadások felderítése továbbra is nehéz, különösen, ha állami szereplők állnak mögöttük.

A pénzintézetek továbbra is gyakori célpontok pénzügyi értékük, érzékeny adatállományuk miatt. A bizalomvesztés, a működési zavarok és a likviditási problémák rendszerszintű gazdasági válságokat is okozhatnak. A fő támadási formák továbbra is DDoS, adathalászat, *social engineering*, és zsarolóvírusok. Növekedik azonban a mobilos trójai, valamint ellátási lánc támadások száma. A politikai eseményekhez „kapcsolódóan" pedig a hacktivista támadások intenzitása emelkedett.

Régi IT-rendszerek és elavult programnyelvek lassítják a védekezés modernizálását. A jelszóhasználattal kapcsolatos hiányosságok, a hamis banki oldalak továbbra is nagy problémát jelentenek. Bemutattuk, hogy a kiberbűnözés már szolgáltatásként működik (RaaS, MaaS), valamint kialakultak bűnözői „ellátási láncok" is.

A támadók gyorsabbak és szervezettebbek, sokszor már mesterséges intelligenciát használnak. Várhatóan a jövő egyik legnagyobb fenyegetése a kvantumszámítógépek elterjedése lesz, mert ezek képesek lesznek a mai titkosítási módszerek feltörésére.

Szabályozási környezettel kapcsolatban megállapítottuk, hogy a GDPR, a NIS vagy a DORA-irányelvek betartása nagyon fontos a pénzügyi szektor ellenálló képességének biztosításához A szabályozás célja, hogy a pénzügyi rendszer szereplői megfelelő védelmet és reagálási képességet építsenek ki a kibertámadásokkal szemben.

## FELHASZNÁLT IRODALOM

[1] „Európai Parlament," 12 10 2021. [Online]. Available: https://www.europarl.europa.eu/topics/hu/article/20211008STO14521/miert-fontos-a-kiberbiztonsag-es-mibe-kerulhet-egy-kibertamadas-az-erintettnek. [Hozzáférés dátuma: 05 07 2025].

[2] J. Clay, „Trend Micro, Security News - April 16, 2021," 16 04 2021. [Online]. Available: https://www.trendmicro.com/en_hk/research/21/d/this-week-in-security-news-april-16-21.html. [Hozzáférés dátuma: 02 07 2025].
[3] N. R. Somogyi Tamás, „Kiberbiztonsági kihívások és megoldások a hazai pénzügyágazat járványhelyzet alatti szabályozási környezetének változása alapján," Biztonságtudományi Szemle, pp. 107-118, 2025. VII. évf. 1. szám.
[4] D. E. S. Julian E. Barnes, „Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul," 11 03 2020. [Online]. Available: https://www.nytimes.com/2020/03/11/us/politics/congress-cyber-solarium.html. [Hozzáférés dátuma: 02 07 2025].
[5] D. H. G. K. Oliver GULYAS, „Impact of cyber-attacks on the financial institutions," CENTERIS – International Conference on ENTERprise Information Systems, Procedia Computer Science Vol. , pp. 84-90, 2022.
[6] L. Evans, Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social En, New York: Bravex Publications, 2020.
[7] European Union Agency for Cybersecurity, „ENISA Threat Landscape 2024," July 2023 to June 2024, p. 4, 09 2024.
[8] „Európai Parlament," 27 01 2022. [Online]. Available: https://www.europarl.europa.eu/topics/hu/article/20220120STO21428/kiberbiztonsag-fo-es-ujonnan-felmerulo-fenyegetesek. [Hozzáférés dátuma: 02 07 2025].
[9] European Union Agency for Cybersecurity, „ENISA Threat Landscape 2024," July 2023 to June 2024, p. 4, 09 2024.
[10] Nemzeti Kibervédelmi Intézet, „A bankszektoron keresztül globális krízist okozhatnak a kibertámadások," Nemzeti Kibervédelmi Intézet, 11 02 2020. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/a-bankszektoron-keresztul-globalis-krizist-okozhatnak-a-kibertamadasok/. [Hozzáférés dátuma: 02 07 2025].
[11] G. Olivér, „A kiberbiztonság és a banki kibervédelem fejlődése," Biztonságtudományi Szemle, %1. kötet2022. IV. évf. 2. szám, pp. 1-13, 2022.
[12] BaFin - Bundesamt für Sicherheit in der Informationstechnik, BaFin Perspektiven, Berlin: Bundesamt für Sicherheit in der Informationstechnik, 2020.
[13] I. L. R. N. A. M. Marianthi Theocharidou, „ENISA Threat Landscape: Finance Sector," European Union Agency for Cybersecurity, 2024.
[14] NordPass, „Top 200 Most Common Paswwords," [Online]. Available: https://nordpass.com/most-common-passwords-list/. [Hozzáférés dátuma: 05 07 2025].
[15] T. S. Zsuzsanna, „24.hu," 23 05 2025. [Online]. Available: https://24.hu/fn/gazdasag/2025/05/23/dobbenetes-banki-csalasok-mbh-mobilapp-netbank-sms-kod-eszrevetlen-tranzakciok/. [Hozzáférés dátuma: 04 07 2025].
[16] F. Ferenc, „CyberThreat Report," 19 06 2025. [Online]. Available: https://www.cyberthreat.report/p/milliardnyi-kiszivargott-hitelesito. [Hozzáférés dátuma: 04 07 2025].
[17] CrowdStrike, „2025 Global Threat Report," 2025.
[18] Verizon DBIR Team: C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup, „2025 Data Breach Investigations Report," Verizon Business, 2025.

DOI: https://doi.org/10.12700/btsz.2025.7.3.75

# PRESENTATION OF A CONDITION MONITORING SYSTEM FOR A THREE-PHASE WOUND-ROTOR ASYNCHRONOUS MOTOR AND ANALYSIS OF STATOR-ROTOR CURRENT SPECTRUM WITH SIGNAL ANALYSIS SAFETY ASPECTS

# HÁROMFÁZISÚ CSÚSZÓGYŰRŰS ASZINKRON MOTOR ÁLLAPOTFIGYELŐ RENDSZERÉNEK BEMUTATÁSA ÉS ÁLLÓRÉSZ-FORGÓRÉSZ ÁRAMSPEKTRUMÁNAK ELEMZÉSE, JELANALÍZIS BIZTONSÁGI SZEMPONTJAI

BENDIÁK István[1]

**Abstract**

The condition monitoring of electrical machines holds outstanding importance in modern industry. Although the three-phase wound-rotor asynchronous motor is less frequently used nowadays, it remains advantageous in applications requiring high starting torque, such as crane drives. Due to its specific structure involving sliding contacts, it is particularly sensitive to various faults, making early detection essential. The system examined in this study is based on the spectral analysis of stator and rotor currents. Through spectral analysis, characteristic faults such as broken rotor bars or eccentricity can be identified. The application of Fourier analysis helps extract useful information from the measured signals. The aim of the research is to present an efficient condition monitoring system suitable for industrial applications. The purpose of this paper is to introduce the structure of the proposed monitoring system, the methodology of spectral analysis, and the importance of signal quality in safety-critical environments.

**Keywords**

Slip ring induction motor, Fourier analysis, spectrum

**Absztrakt**

A villamos gépek állapotfigyelése ki-emelkedő jelentőségű a korszerű iparban. A háromfázisú csúszógyűrűs aszinkron motor napjainkban ritkábban alkalmazott géptípus, de különösen nagy indítónyomatékot igénylő rendszerekben előnyös (daruhajtások). Sajátos (csúszó kontaktusok) szerkezete miatt érzékeny a különféle hibákra, ezért fontos ezek korai felismerése. A vizsgált rendszer az állórész- és forgórész-áram spektrumának elemzésén alapul. A spektrumanalízis segítségével olyan jellegzetes hibák azonosíthatók, mint például a törött rúd vagy excentricitás. Az Fourier-analízis alkalmazása segít a jelekből hasznos információkat megjeleníteni. A kutatás célja egy hatékony, iparban is alkalmazható állapotfigyelő rendszer bemutatása. A dolgozat célja a javasolt állapotfigyelő rendszer felépítésének, a spektrumanalízis módszertanának és a jelminőség fontosságának bemutatása biztonságkritikus környezetben.

**Kulcsszavak**

Csúszógyűrűs aszinkron motor, Fourier-analízis, spektrum

[1] bendiak.istvan@uni-obuda.hu | ORCID: 0009-0009-3320-4089 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

## CSÚSZÓGYŰRŰS ASZINKRON MOTOR MÉRÉSE, BEVEZETŐ

A villamos gépek állapotfigyelése kiemelkedő [1-13] jelentőségű a korszerű ipari rendszerekben, különösen a megbízhatóság, a hatékonyság és a biztonság szempontjából. Az ipari automatizálás térnyerésével és a prediktív karbantartás iránti igény növekedésével egyre fontosabbá válik a villamos forgógépek üzemi viselkedésének folyamatos megfigyelése. A háromfázisú csúszógyűrűs aszinkron motor napjainkban ritkábban alkalmazott géptípus, elsősorban a korszerűbb frekvenciaváltós hajtások térhódítása miatt. Ennek ellenére továbbra is előnyös bizonyos speciális alkalmazásokban, különösen nagy indítónyomatékot igénylő rendszerek esetén, például daruhajtásokban vagy nehézgép-mozgatásban.

A csúszógyűrűs aszinkron motor egyik fő előnye a szabályozható indítási jellemző, ugyanakkor sajátos szerkezete – különösen a csúszógyűrűk és a szénkefék jelenléte – miatt fokozottan érzékeny a különféle meghibásodásokra. Ezek a hibák lehetnek villamos eredetűek (pl. szigetelési problémák), mechanikai természetűek (pl. forgórész-törés, excentricitás), vagy a kontaktusokból adódó problémák (pl. ívképződés, érintkezési instabilitás). E hibák időbeni felismerése elengedhetetlen az üzembiztonság megőrzése és a nem tervezett leállások elkerülése érdekében.

A vizsgált állapotfigyelő rendszer az állórész- és forgórész-áram spektrumának elemzésére épül, amely nem invazív módon nyújt információt a gép belső állapotáról. Az áramjelek frekvenciaanalízise lehetővé teszi a tipikus hibajelenségek – mint például túlmelegedett forgórész rúd, rotor-excentricitás, kiegyensúlyozatlanság – azonosítását. A spektrumanalízis során alkalmazott Fourier-transzformáció lehetővé teszi a komplex időbeli jelek frekvenciakomponenseinek vizsgálatát, ami alapja lehet egy automatizált hibadetektáló algoritmusnak.

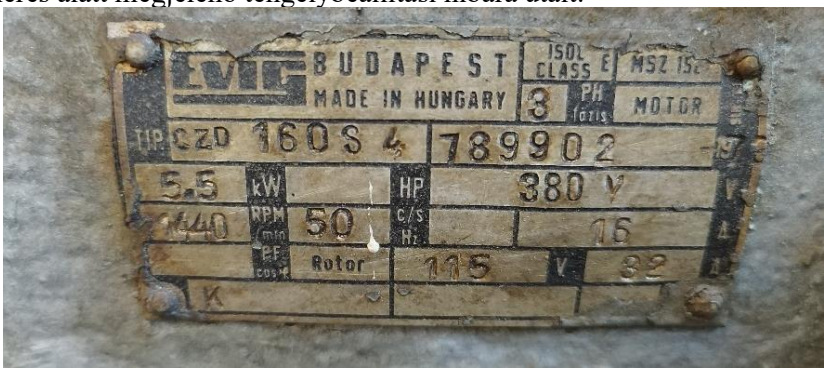
A jelen kutatás célja egy olyan hatékony és ipari környezetben is alkalmazható állapotfigyelő rendszer (kopási térkép) bemutatása, amely képes valós idejű diagnosztikai információkat szolgáltatni. A rendszer kiemelt figyelmet fordít a jelminőségre, valamint a zaj- és zavarvédelmi szempontokra, mivel ezek közvetlenül befolyásolják a diagnosztikai pontosságot. A biztonságkritikus ipari környezetben különösen fontos, hogy a mérési rendszer megbízható, ismételhető és megfelelő felbontású adatokat szolgáltasson.

A dolgozat részletesen bemutatja a javasolt állapotfigyelő rendszer felépítését, a spektrumanalízis alkalmazott módszertanát, valamint a jelanalízis során fellépő tipikus kihívásokat és azok kezelésének lehetőségeit. Kiemelten tárgyaljuk a statikus és dinamikus hibák spektrumban való megjelenését, valamint a hibafrekvenciák viselkedését különböző üzemállapotokban. A rendszer célja nem csupán a hibák detektálása, hanem azok osztályozása, előrejelzés becslése és a lehetséges következmények mérlegelése.

Végső soron a kutatás célja, hogy hozzájáruljon a háromfázisú csúszógyűrűs aszinkron motorok üzembiztonságának növeléséhez, a karbantartási stratégiák optimalizálásához és a karbantartási költségek csökkentéséhez. Az ipar 4.0 és a gépi tanulási technológiák térhódításával az ilyen típusú diagnosztikai rendszerek integrálhatók intelligens gyártási platformokba is. A fejlesztett rendszer hosszú távon lehetőséget kínál az üzemidő növelésére, a meghibásodási kockázatok csökkentésére, valamint a hibák ok-okozati összefüggéseinek pontosabb feltárására.

A gépről készített képsorozat (1-5. ábrák) bemutatja a motor adatait és a motor felépítését. Az 1. ábra a motor adattáblája a névleges feszültség, áram, frekvencia, fordulatszám, típussorozat megjelölése (CZD-csúszógyűrűs forgórészű darumotor). A 2. ábra motor

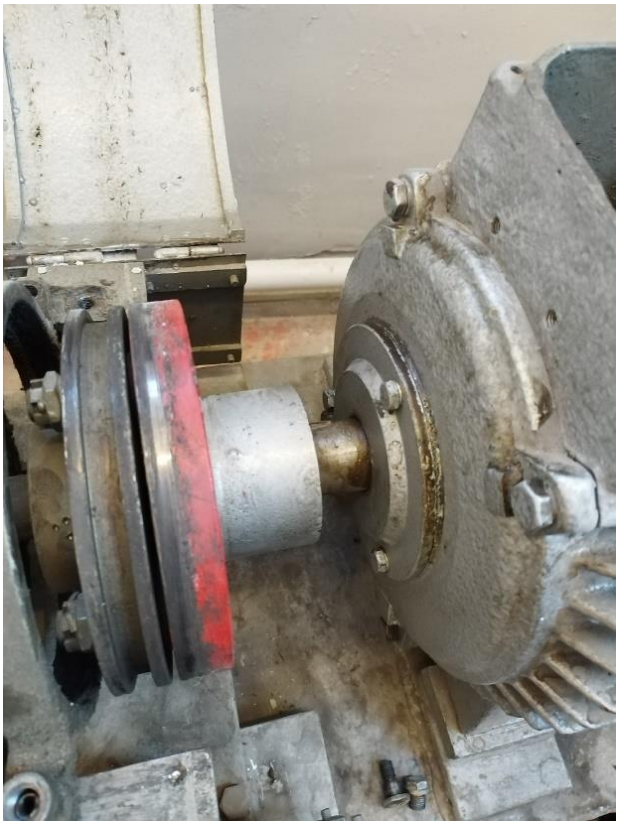
felső csúszógyűrű burkolat levétele után. A 3. ábra közeli felvétel a motor állórész és forgórész kötéséről, valamint a csúszógyűrűkről. A 4-5. ábrák a tengelykapcsolat ellenőrzése, amely a mérés alatt megjelenő tengelybeállítási hibára utalt.



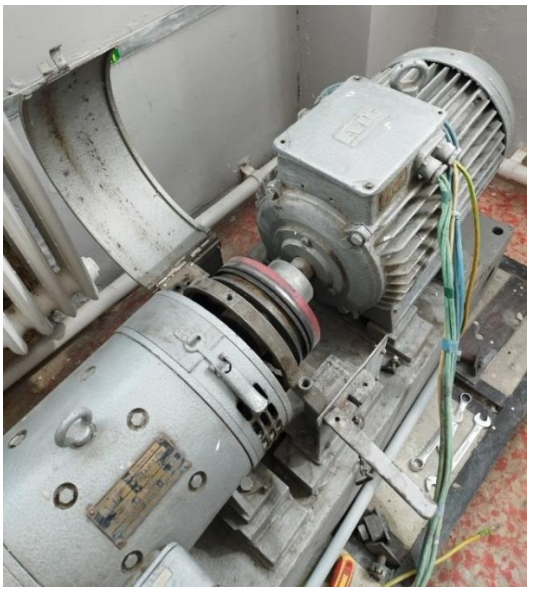

*1. ábra Csúszógyűrűs aszinkron motor adattáblája.*

*2. ábra Csúszógyűrűs aszinkron motor felső burkolat levétele után.*

*3. ábra Közeli felvétel a csúszógyűrűkről.*



*4. ábra Csúszógyűrűs aszinkron motor tengelykapcsolat burkolat eltávolítása.*

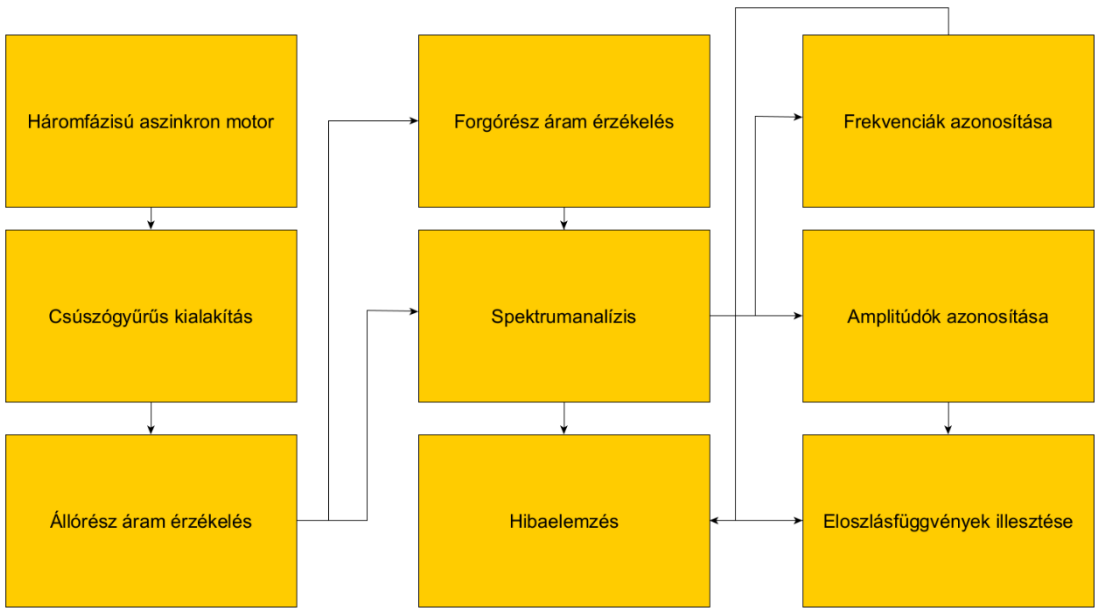


*5. ábra Csúszógyűrűs aszinkron motor tengelykapcsolatának ellenőrzése.*

## HÁROMFÁZISÚ CSÚSZÓGYŰRŰS ASZINKRON MOTOR ÁLLAPOTFIGYELŐ RENDSZERÉNEK HATÁSVÁZLATA

A mérési blokkvázlat (6. ábra) mutatja a háromfázisú csúszógyűrűs aszinkron motor állapotfigyelő rendszerének hatásláncát. A módszer célja a motor működése közbeni hibák korai felismerése és diagnosztizálása. A baloldalon (6. ábra) található a motor táplálása, amely háromfázisú váltakozó árammal történik. A hálózati feszültség és áram jelei mérésre kerülnek, ezek a bemeneti paraméterek. A motor csúszógyűrűs kivitele lehetővé teszi, hogy a forgórész áramait is közvetlenül mérni lehessen.

A mérőeszközök a motor állórész- és forgórészáramait [7] figyelik valós időben. A nyers áramjelek további feldolgozásra kerülnek egy előfeldolgozó egységben. Ez az egység zajszűrést, normalizálást és mintavételezést végez. Az így előkészített jelek frekvenciatartományba kerülnek átalakításra egy [8] gyors Fourier-transzformáció segítségével (előzetes feldolgozás). A spektrum alapján jellemző hibafrekvenciák kereshetők ki, amelyek például törött rúdra, excentricitásra vagy kiegyensúlyozatlanságra utalhatnak. A spektrum-adatokat egy kiértékelő algoritmus elemzi, amely gépi tanulással és [9] szabályalapú logikával történhet. A döntéshozó modul meghatározza, hogy van-e jelen hiba, és ha igen, milyen típusú. Az eredmények megjelennek egy vizualizációs felületen, ahol a karbantartó személyzet követni tudja az állapotváltozásokat. A rendszerriasztást is tud küldeni, ha súlyos meghibásodást észlel. A teljes diagnosztikai ciklus automatizált és ciklikusan ismétlődik [10].




*6. ábra Háromfázisú csúszógyűrűs aszinkron motor állapotfigyelő rendszerének blokkvázlata.*

A megoldás nagy számításai kapacitást igényel, de jól skálázható ipari környezetben. A rendszer célja, hogy csökkentse a nem tervezett leállásokat és javítsa az üzembiztonságot. Ez különösen fontos a nehéziparban, ahol a daruhajtások kritikus szerepet játszanak. A digitális adatfeldolgozás és a spektrumanalízis központi szerepet kap. A rendszer

bővíthető további érzékelőkkel is, például rezgés- vagy hőmérsékletmérőkkel. A kialakítás lehetővé teszi a valós idejű monitorozást és távoli hozzáférést is. Összességében a blokkvázlat egy modern, megbízható és ipar számára hasznos állapotfigyelő rendszer struktúráját mutatja be (6. ábra).

**A mérési elvek és módszerek (6. ábra alapján):**

- A bemutatott blokkvázlat egy csúszógyűrűs aszinkron motor működésének és vizsgálati elrendezésének főbb folyamati lépéseit mutatja be.
- A rendszer alapját a háromfázisú hálózati betáplálás biztosítja, amely ellátja a villamos gépet.
- A csúszógyűrűs motor különlegessége, hogy forgórésze csúszógyűrűkkel kapcsolódik a külső áramkörhöz, ezáltal szabályozhatóvá válik a nyomatékleadás.
- A forgórész csúszógyűrűire kapcsolt ellenálláslánc lehetőséget ad a nyomaték és az indítási áram karakterisztikájának optimalizálására.
- A vázlat kiemeli a mechanikai terhelés és a motor közötti kapcsolatot, amely meghatározza a működési viszonyokat.
- A forgórész és a terhelés közötti energiacsere vizsgálata fontos szempont a hatásfok és teljesítménytényező meghatározásában.
- A motor kimeneti tengelye mechanikai munkát végez, amelyet forgatónyomaték és fordulatszám jellemez.
- A hatásláncban a veszteségek különböző pontokon keletkeznek: tekercsveszteség (réz- és vasveszteség), valamint mechanikai (súrlódás, szellőzési) formában.
- A vázlat alapján az energiaátvitel vizsgálható teljesítményáramként is, amely villamos → mágneses → mechanikai formában jelenik meg.
- A diagram lehetővé teszi a gép különböző hatásfokainak (pl. részleges, belső, összhatásfok) elkülönített elemzését (különböző frekvenciákon).
- A tudományos kutatás szempontjából ez a hatáslánc ideális modell a veszteségek kvantitatív becslésére és optimalizálására (nagy frekvenciás veszteségek).
- A motor belső folyamatai, mint például a légrés aszimmetria, árameloszlás és nyomatékképzés, a modell mentén részletesen követhetők.
- A vázlatban szereplő komponensek alapján különböző szabályozási stratégiák – például indítási ellenállásváltoztatás – is szimulálhatók, valamint a két inverteres szabályozási módszerek tesztelése is megvalósítható (állórész és forgórész külön táplálása).
- A rendszer komplexitása lehetőséget ad különféle hibaforrások (pl. forgórész tekercssérülés,, rúdszakadás, vasmagtorzulás, hőterhelés) hatásainak modellezésére.
- Összefoglalva, ez a hatásvázlat egy többdimenziós vizsgálati és oktatási eszköz, amely valósághűn leképezi a csúszógyűrűs motor működési mechanizmusait kutatási célokra és oktatási célokra.

A forgórész áram mérése (közvetlenül ennél a géptípusnál megvalósítható) kulcsfontosságú a villamos gépek állapotának pontos értékeléséhez. A rotor áramspektrumnak kiemelt szerepe van a forgórész diagnosztikájában, mivel lehetővé teszi a frekvenciatartományban megjelenő jellemző hibajelek azonosítását szlip (csúszás) frekvenciát figyelembe

véve. A spektrumelemzése során a periodikus jelenségek – például a forgási frekvencia, harmonikusok vagy modulációs melléksávok – vizsgálatával pontosan meghatározhatók a hibák forrásai. Például excentricitás, repedések vagy laza rögzítések specifikus frekvencia-komponenseket eredményeznek és ennek közvetlenül a forgórészen történő azonosítása. Így a spektrumelemzése megbízható alapot nyújt a prediktív karbantartáshoz és az üzembiztonság növeléséhez a forgórész áram felhasználásával.

## KUTATÁSBAN HASZNÁLT MATEMATIKAI HÁTTÉR RÖVID BEMUTATÁSA

Következő fejezetrészben át kell [2] tekinteni azokat a matematikai készleteket (nem minden pontra kiterjedő matematikai készlet), amelyeket feltétlenül fel kell használni a forgógépek diagnosztikai elemzése során [2], [3].

A klasszikusan ismert Dirac-impulzus segítségével a formálisan kibővíthetjük a differenciálható függvények körét. Ha ugyanis a Dirac-impulzust függvényként kezeljük, akkor a véges ugrással rendelkező függvényeket is differenciálhatónak tekintjük. Valamely f(t) függvény f'(t) általánosított deriváltján olyan általánosított függvényt értünk, amelyre felírható [2]:

$$f(t) = \int_{-\infty}^{t} f(x)dx, \qquad \lim_{t\to\infty} f(t) = 0$$

Tipikus ilyen függvény az 1(t) egységugrás. Ennek ebben az értelemben vett differenciálhányadosa:

$$\dot{1}(t) = \begin{cases} \dot{0}, t < 0 \\ \text{nincs értelmezve}, t = 0 \\ 0, t > 0 \end{cases}$$

Nyilvánvaló, hogy $\dot{1}(t)$ ismeretében $1(t)$ nem állítható elő (1) alapján integrálással, mert a t=0 helyen 1(t) nincs értelmezve.

Be kell vezetni az $\dot{1}(t,\tau)$ függvény az alábbi definícióval [2]:

$$1(t,\tau) = \dot{\begin{cases} 0, t < 0 \\ t/\tau \quad , 0 < t < \tau \\ 1, \tau < t. \end{cases}}$$

Ennek határértéke $\tau \to 0$ esetén az 1(t) egységugrás. A $\delta(t,\tau)$ függvény definíciójából következik, hogy:

$$1(t,\tau) = \int_{-\infty}^{t} \delta(x,\tau)\,dx, \acute{1}(t) = \delta(t,\tau).$$

Képezzük a $\tau \to 0$ határértéket, akkor:

$$1(t) = \int_{-\infty}^{t} \delta(x)dx, \qquad 1(t) = \delta(t)$$

A Dirac-impulzus integrálja tehát az egységugrást adja és ennek megfelelően az egységugrás általánosított deriváltja a Dirac-impulzus [2].

Ennek alapján képezhetjük bármely szakadásos φ(t) függvény általánosított deriváltját.

Legyen:

$$\varphi(t) = [1 - 1(t - t_1)]\, f_1(t) + 1(t - t_1)\, f_2(t)$$

ahol $f_1(t)$ és $f_2(t)$ folytonosak és differenciálhatók.

Képezzük ennek általánosított deriváltját a szorzatra vonatkozó differenciális szabály formális alkalmazásával [2]:

$$\varphi''(t) = -\delta(t - t_1)f_1(t) + [1 - (t - t_1)]f_1''(t) + \delta(t - t_1)f_2(t) + 1(t - t_1)f_2''(t)$$

A folytonos f1(t) függvényekre $f_i''(t) = \dot{f}_1(t)$, míg pl.:

$$\delta(t - t_1)f_1(t) = \delta(t - t_1)f_1(t_1)$$

Hiszen $\delta(t - t_1)$ a $t_1$ hely kivételével mindenütt nulla.

Így tehát [2]:

$$q''(t) = [1 - 1(t - t_1)]\dot{f_1}(t) + [f_2(t_1) - f_1(t_1)]\delta(t - t_1) + 1(t - t_1)\dot{f_2}(t)$$

Mivel $1''(t) = \delta(t)$ vagyis a t=0 helyen fellépő egységnyi ugráshoz a $\delta(t)$ derivált tartozik, akkor a $t_1$ helyen fellépő $\Delta_1 = f_2(t_1) - f_1(t_1)$ ugráshoz nyilván a $\dot{\Delta}_1\delta(t - t_1)$ ugrás tartozik. A $q''(t)$ derivált integrálásával és

$$1(t) = \int_{-\infty}^{t} \delta(x)dx, \qquad 1(t) = \delta(t)$$

figyelembevételével visszakapjuk:

$$\varphi(t) = [1 - 1(t - t_1)]\, f_1(t) + 1(t - t_1)\, f_2(t)$$

függvényt.

Az itt formálisan bevezetett és később felhasznált általánosított derivált fogalma és néhány tétele matematikailag szigorúan is igazolható a disztribúcióelmélet vagy az operátorszámítás segítségével. Az „általánosított" derivált megegyezik a „disztribúció" értelemben vett deriválttal [2].

## LAPLACE-TRANSZFORMÁCIÓ ALKALMAZÁSA

A koncentrált paraméterű lineáris invariáns hálózatok átmeneti jelenségeinek törvényszerűségeit matematikailag közönséges, lineáris, állandó együtthatós differenciálegyenletek írják le, amelyek megoldásának kiindulási értékeit ismerjük [2].

Tudjuk, hogy a teljes megoldás meghatározását nagymértékben megkönnyíti a Laplace-transzformáció alkalmazása. Alábbiakban össze kell foglalni a legfontosabb szabályokat.

A Laplace-transzformáció egy f(t) valós változós (de esetleg komplex értékű) függvényhez egy F(s) komplex változós függvényt rendel [2]:

$$F(s) = \mathcal{L}f(t) = \int_{-\infty}^{\infty} I(t)\, f(t)e^{-st}dt$$

Megjegyzendő, hogy a gyakorlatban az F(s) függvényeket általában elemi úton számíthatjuk ki, vagy megfelelő táblázatból vesszük [2].

A Laplace-transzformáció néhány tétele:

A transzformáció lineáris, tagonként elvégezhető és az állandó szorzó kiemelhető:

$$\mathcal{L}\sum_{k=1}^{n} C_k\, f_k(t) = \sum_{k=1}^{n} C_k\, \mathcal{L}f_k(t) = \sum_{k=1}^{n} C_k F_k\,(s)$$

Az integrált függvény transzformáltja [2]:

$$\mathcal{L}\int_0^t f(\tau)d\tau = \frac{1}{s}F(s)$$

A derivált függvény transzformáltja [2]:

$$\mathcal{L}f''(t) = sF(s) - f(-0)$$

Az ún. hasonlósági tétel [2]:

$$\mathcal{L}f(kT) = \frac{1}{k}F\left(\frac{s}{k}\right), k > 0$$

Az ún. eltolási tétel:

$$\mathcal{L}[1(1-T)f(t-T)] = e^{-sT}F(s)$$

A tétel megfordítása:

$$\mathcal{L}^{-1}[e^{-sT}F(s)] = 1(t-T)f(t-T) = \begin{cases} 0, & t < T \\ f(t-T), & t > T \end{cases}$$

Az ún. csillapítási tétel:

$$\mathcal{L}[f(t)e^{-\gamma t}] = F(s+\gamma)$$

Itt a $\gamma$ lehet komplex is.

A konvolúció-tétel [2]:

$$f(t) = f_1(t)\cdot f_2(t) = \int_0^1 f_1(\tau)f_2(t-\tau)d\tau$$

$$F(s) = \mathcal{L}[f_1(t)\cdot f_2(t)] = F_1(s)F_2(s)$$

A határérték-tételek:

$$f(+0) = \lim_{t\to 0} f(t) = \lim sF(s)$$

$$\lim_{t\to\infty} f(t) = \lim_{s\to 0} sF(s)$$

Utóbbi akkor alkalmazható, ha F(s) minden szingularitásának valós része negatív, megengedve azonban az s=0 szingularitást.

A transzformáció megfordítását elvileg a Reimann-Mellin inverziós integrál szolgáltatja [2]:

$$I(t)f(t) = \mathcal{L}^{-1}F(s) = \frac{1}{2\pi j}\int_{\sigma-j\infty}^{\sigma+j\infty} F(s)e^{st}ds, \qquad \sigma > \sigma_0$$

Ahol $\sigma_0$ az F(s) konvergencia –abszcisszája. A gyakorlatban a fenti tételt ritkán alkalmazzák. Ha F(s) racionális tört, akkor az inverz transzformáció a kiejtési tétellel végezhető. Legyen M(s) és N(s) polinomok, N(s) minden zérusra egyszeres, akkor:

$$F(s) = \frac{M(s)}{N(s)}, f(t) = \sum_{k=1}^{n}\frac{M_{(s_k)}}{N''_{(s_k)}}e^{s_k t}, t > 0$$

$$N(s_k) = 0, N''(s) \neq 0, k = 1,2, \dots, n;$$
$$\lim_{s \to \infty} F(s) = 0$$

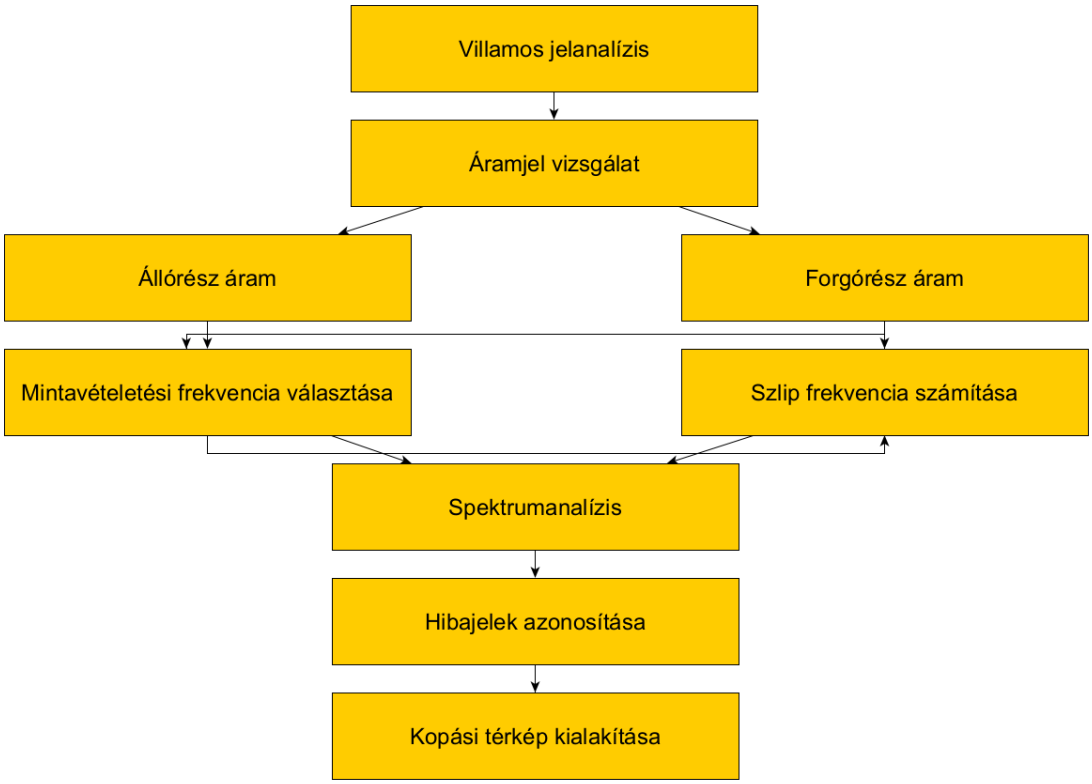
A kifejtési tétel egy másik alakja [24]:

$$F(s) = \frac{M(s)}{N(s)}, f(t) = \sum_{k=1}^{n} \frac{M_{(s_k)}}{N''_{k_{(s_k)}}} e^{s_k t}, t > 0$$
$$N_{(s_k)} = 0, N_k(s) = \frac{N(s)}{s - s_k}, N_k(s_k) \neq 0$$
$$\lim_{s \to \infty} F(s) = 0$$

Ha F(s) számlálója és nevezője megegyező fokszámú-vagyis F(s) nem tart a végtelenben nullához-, akkor az általtortet átalakítjuk egy állandó és egy valódi tört összegévé [2].

## HÁROMFÁZISÚ ASZINKRON MOTOR MECHANIKAI HIBÁINAK ELEMZÉSE ÁRAMJELALAK-ANALÍZISSEL

A következő fejezetben a csúszógyűrűs aszinkron motor mérési elve kerül bemutatásra és az adatfeldolgozás lépései vázlat alapján. A 7. ábra (blokkvázlat) leírása és jelentősége.



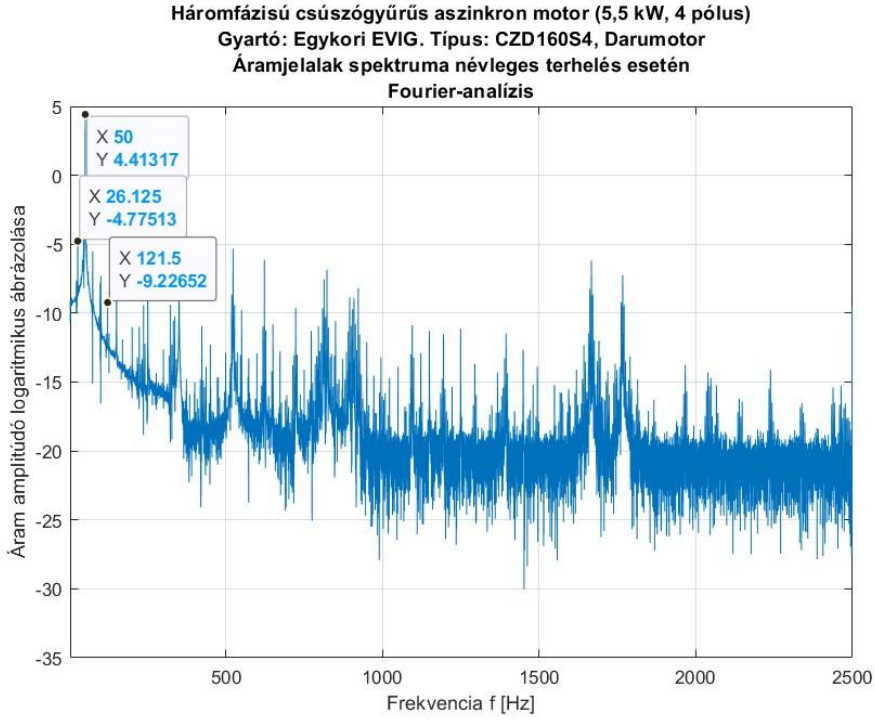

*7. ábra Villamos jelanalízis szerepe a villamos gépek vizsgálata során, mérési koncepció.*

**A blokkvázlat elemzése és folyamat bemutatása**

- A motor táplálása háromfázisú hálózatról történik, amely biztosítja a mérést.
- A mérés célja az állórész és a forgórész áramának elkülönített vizsgálata.
- A forgórész jeleit a csúszógyűrűkön keresztül lehet érzékelni, és külön jelfeldolgozás alá esnek.
- Az áramjelek A/D átalakításon történik, majd digitális adatgyűjtő egységbe kerülnek.
- A feldolgozás során Fourier-analízis történik a hibafrekvenciák meghatározására.
- A rendszer képes valós idejű mérésre és adatfeldolgozásra (napjainkra alapkövetelmény).
- Az eredmények alapján lehetséges a csapágyhibák, rotorhibák és egyéb rendellenességek detektálása, kielemzése.
- A rendszer alkalmas laboratóriumi és ipari alkalmazásra, továbbá bővíthető más szenzoros mérésekkel is.

## ÁLLÓRÉSZÁRAM SPEKTRUMÁNAK ELEMZÉSE

A következő fejezetben a motor állórészáram-spektrumának feldolgozása kerül bemutatásra. A felvett Fourier-analízis bemenetei értékei a gépről alkotott kopási térkép előkészítéséhez.

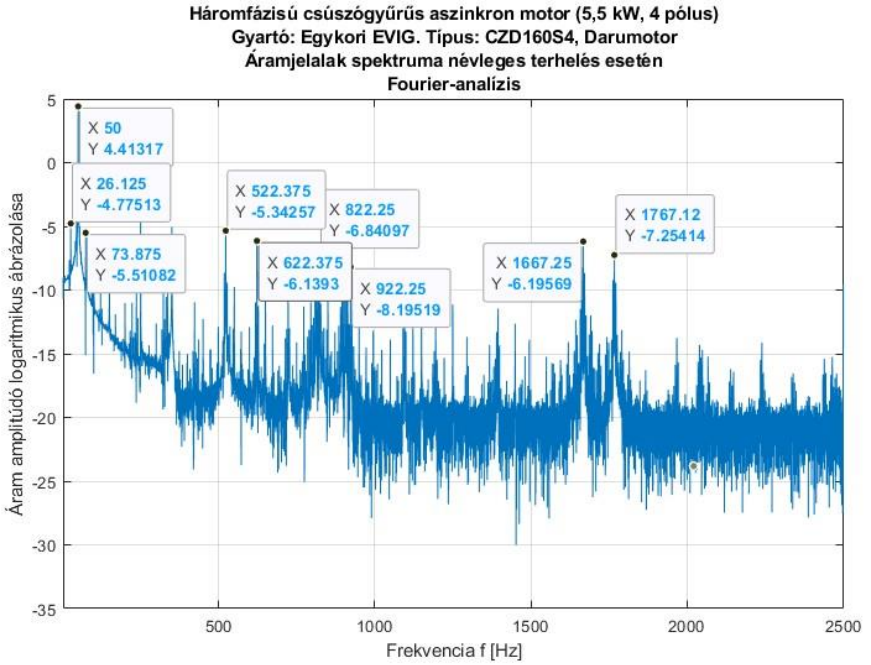



*8. ábra Háromfázisú csúszógyűrűs aszinkron motor állórész áram Fourier-analízise. Tartomány 0-2500 Hz-ig (FFT-Fast Fourier Transform).*

A 8. ábrán egy háromfázisú csúszógyűrűs aszinkron motor áramjelének spektruma látható. A motor teljesítménye 5,5 kW, 4 pólusú, és egykori EVIG (egykori Egyesült Villamosgépgyár, Budapest X., Gyömrői út 128.) gyártmányú, CZD160S4 típusú darumotor. Az ábrán az áram amplitúdó logaritmikus (dB) értéke szerepel a függőleges tengelyen. A vízszintes tengelyen a frekvencia [Hz] van feltüntetve, 0-tól 2500 Hz-ig.

A Fourier-analízis eredménye egy összetett spektrum, amely számos csúcsot és modulációs sávot tartalmaz. A legnagyobb amplitúdó az 50 Hz-es hálózati frekvenciánál látható, 4.41 dB értékkel. További kiemelt frekvenciák: 26.13 Hz (–4.78 dB) és 121.5 Hz (–9.23 dB).A spektrum jellemzője, hogy a névleges terhelés alatt végzett mérés dominánsan alacsony frekvenciatartományban mutat energia-koncentrációt.

A 26.1 Hz-es csúcs és más hasonló frekvenciák a forgórész ütésére, excentricitásra vagy egyensúlyhiányra utalhatnak. Ez különösen fontos egy csúszógyűrűs aszinkron motor esetében, ahol a mechanikai hibák könnyen jelentkezhetnek. A vizsgálatot folytatni kell az áramspektrum több megjelölt komponensét tartalmazó alkotórésszel.




*9. ábra Háromfázisú csúszógyűrűs aszinkron motor állórész áram Fourier-analízise. Tartomány 0-2500 Hz-ig (FFT-Fast Fourier Transform).*

A 9. ábrán folytatva háromfázisú csúszógyűrűs aszinkron motor áramspektrumának elemzését. Az ábra vízszintes tengelye ugyanúgy a frekvenciát [Hz], a függőleges tengelye az áram amplitúdóját ugyanúgy logaritmikus (dB) skálán ábrázolja.

A Fourier-analízis alapján jól elkülönülő frekvenciakomponensek láthatók, amelyek jellemzőek a motor villamos és mechanikai viselkedésére. A legnagyobb amplitúdójú csúcs 50 Hz-nél található, amely a hálózati frekvenciát természetesen a hálózati frekvencia alapharmonikusa. Számos további csúcs azonosítható, például 522,375 Hz-nél, 822,25 Hz-nél és 1767,12 Hz-nél. Ezek a csúcsok lehetnek mechanikai harmonikusok, oldalsávok vagy

valamilyen periodikus (tengelykapcsolati oszcilláció) hiba frekvenciakomponensei. Az áramspektrum 2500 Hz-ig terjed, és a zajszint közelítően –20 dB alatt marad.

## KÉT ÁRAMSPEKTRUM ÖSSZEHASONLÍTÁSA:

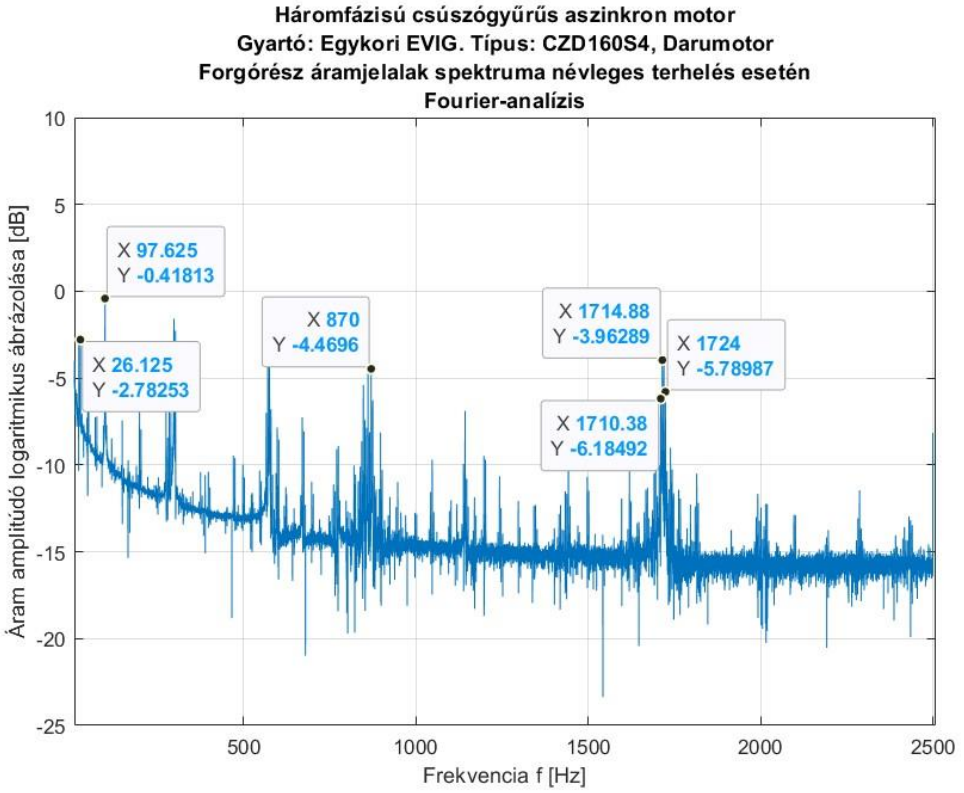
Mindkét ábrán jól látható a domináns 50 Hz-es frekvencia, amely a hálózati tápfeszültséget tükrözi, és ez a legnagyobb amplitúdójú csúcs. Az első spektrum kevesebb frekvenciakomponenst emel ki, így inkább az alacsony frekvenciatartományra koncentrál (26, 73 és 121 Hz körül). A második spektrum részletesebb, és több közép- és magas frekvenciás csúcsot jelöl meg, például 522, 822, 922, 1667 és 1767 Hz-nél. Ez utóbbi alapján feltételezhető, hogy a második mérés érzékenyebb volt a nagyobb frekvenciatartományokra vagy hosszabb adatfelvétel történt. Mindkét spektrum logaritmikus dB skálán mutatja az amplitúdót, és a csúcsok eloszlása utalhat rotor-, stator- vagy csapágyhibákra. A zajszint mindkét ábrán hasonló, –30 dB körül stabilizálódik, de a második spektrumban több szórt komponens figyelhető meg.

Összességében a második spektrum részletesebb és több diagnosztikai információt nyújt a motor állapotáról.

## FORGÓRÉSZ ÁRAMSPEKTRUMÁNAK ELEMZÉSE

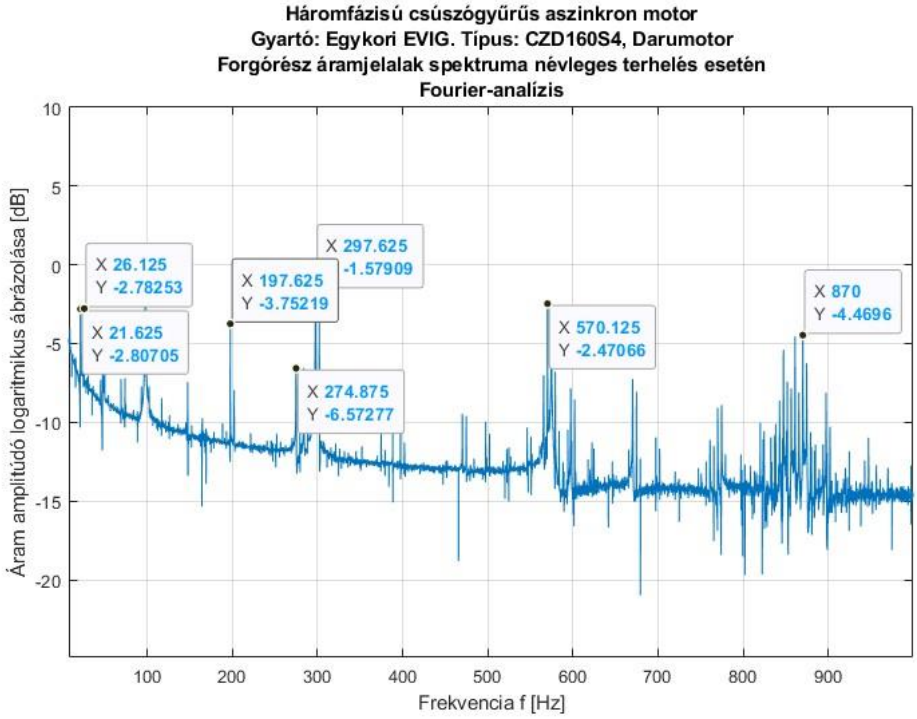
A 10. ábrán látható a csúszógyűrűs aszinkron motor forgórészének áramjeléből készült Fourier spektrum látható.

Az ábrán a vízszintes tengely a frekvenciát [Hz], a függőleges tengely az áram amplitúdóját mutatja logaritmikus skálán [dB]. A spektrumelemzés gyors Fourier-transzformációval készült, és névleges terhelés melletti mérési eredményeket tükröz. Az egyik legjelentősebb frekvenciacsúcs a 1714,88 Hz-nél jelenik meg, –3,96 dB amplitúdóval. Emellett további kiemelt komponensek találhatók 26,125 Hz, 97,625 Hz, 870 Hz és 1724 Hz körül. Ezek a frekvenciák alapvetően mechanikai jelenségekhez és villamos aszimmetriákhoz köthetők, például tengelykapcsolati és rotorhibákhoz. A spektrum alapzaja közelítően –15 dB alatt stabilizálódik, de számos kisebb frekvenciaösszetevő is kimutatható. A legnagyobb csúcsokat automatikusan megjelölték a képen koordináta-értékekkel együtt, ami segíti az elemzést. Ez az ábra jól használható a forgórész hibáinak diagnosztikájára, forgási frekvencia, excentricitás vagy tekercselési hibák felismerésére.




*10. ábra Háromfázisú csúszógyűrűs aszinkron motor forgórész áram Fourier-analízise. Tartomány 0-2500 Hz-ig (FFT-Fast Fourier Transform).*

A két forgórész áramspektrum 10-11. ábrák spektrális elemzése hasznos, de nem elegendő a hibatérkép felállítására. Az állórész és forgórész spektruma között eltérés a szlip (csúszás) frekvenciában van (valamint itt most nem részletezett villamos és forgási jellemzőn, a forgógépre érvényes frekvenciafeltétel) és motor pólusszámából adódó villamos és geometriai szögeltérések.




*11. ábra Háromfázisú csúszógyűrűs aszinkron motor forgórész áram Fourier-analízise. Tartomány 0-1000 Hz-ig (FFT-Fast Fourier Transform).*

A 11. ábra mutatja a következő forgórész áramspektrumát megváltoztatott frekvencia skála mellett (1000 Hz-ig). A vízszintes tengely a frekvenciát [Hz], a függőleges tengely az áram amplitúdóját mutatja logaritmikus skálán [dB].

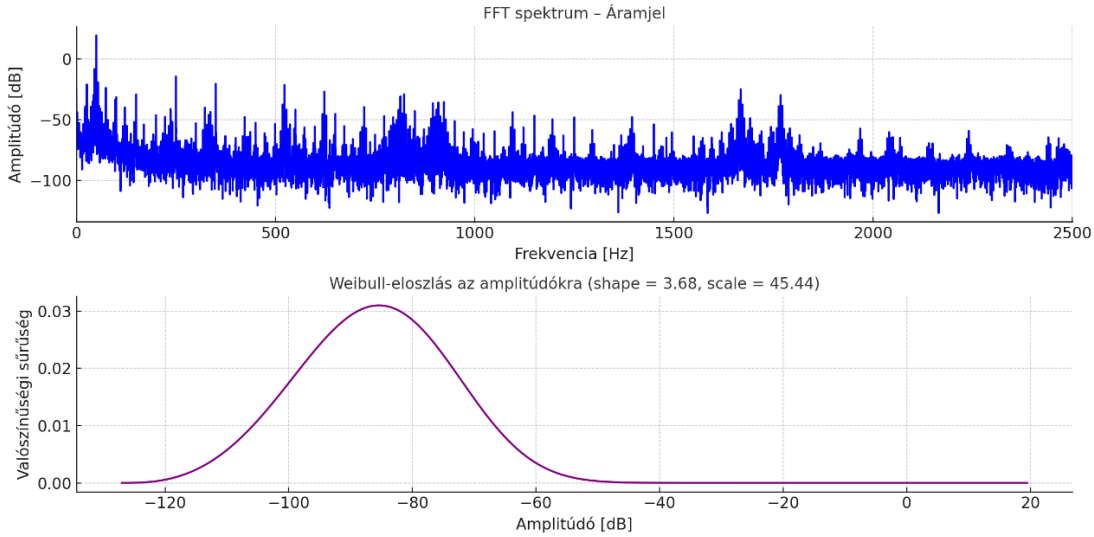
Az ábrán több jellegzetes csúcsot emel ki, például 21,625 Hz-nél, 197,625 Hz-nél, 297,625 Hz-nél és 870 Hz-nél. A legnagyobb amplitúdó –1,57909 dB, ami a 297,625 Hz frekvencián jelentkezik. A spektrum jól mutatja a jel frekvenciakomponenseinek eloszlását, amely alkalmas a forgórész hibadiagnosztikára. Az alapzaj szintje –15 dB körüli, viszonylag stabil, de a spektrumban több, kiemelkedő komponens is megtalálható. A 274,875 Hz-nél jelentkező –6,57 dB-es csúcs például mechanikai rezonanciára utalhat. A 870 Hz-es komponens ismét megjelenik, ahogy más spektrumokban is, ami megerősítheti annak fizikai jelentőségét.

Ez az ábra részletes képet ad a motor forgórészének állapotáról, és jól alkalmazható frekvenciaalapú hibakeresésre. Részletesebb elemzésre szükséges, mint a bemutatott néhány amplitúdó és frekvencia összehasonlítása, ezek a mérőszámok további számításra kerülnek.

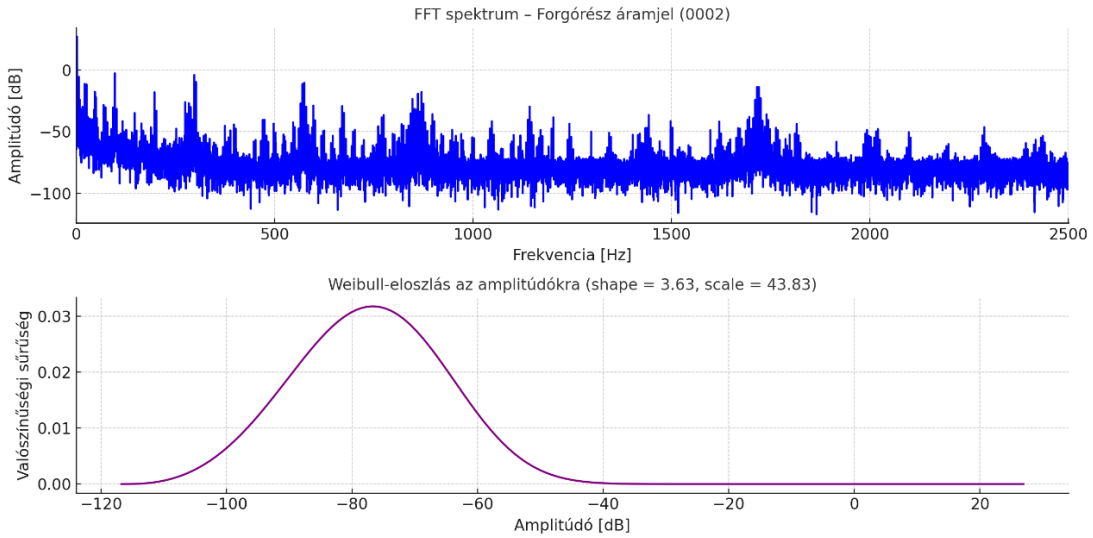
## KOPÁSI TÉRKÉP, HIBAJELEK RENDSZEREZÉSE, ÖSSZEFOGLALÁS

A kutatási elsődleges célja az [9] áramspektrumok mellett az eloszlás függvények szerepének felhasználása. Ebben az esetben a Weibull-és Gamma-eloszlás függvényekkel volt vizsgálva az amplitúdóspektrummal felhasználva. Ennek az a célja, hogy a gép egy

adott állapotában felvett áramspektrummal [10] összhangban megjelenítse a spektrum amplitúdó eloszlását. Ez az eloszlás még nem feltételen alkalmas hibametria felállítására, hanem arra szolgál, hogy támogassa a kopási térkép mezőeloszlásainak értékét amplitúdó nagyság szempontjából [12].

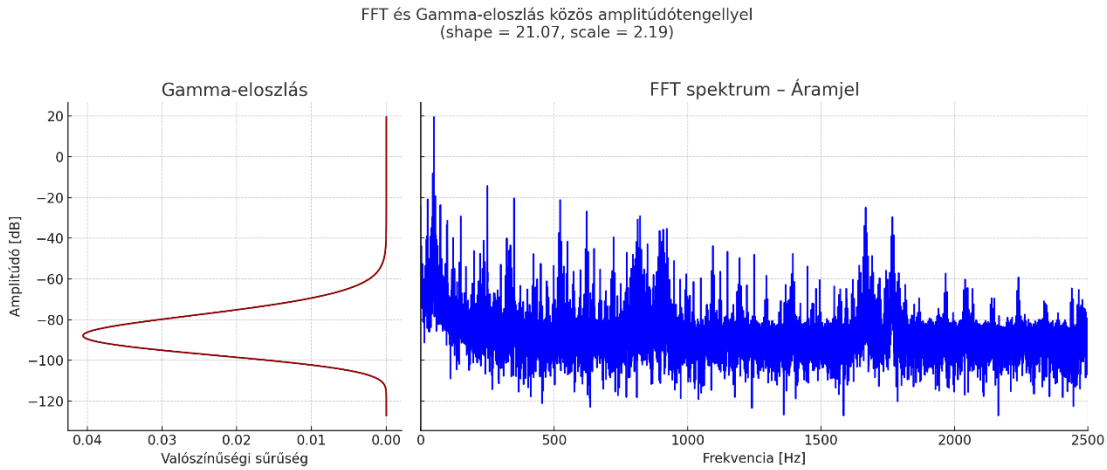



*12. ábra Háromfázisú csúszógyűrűs aszinkron motor állórész áram Fourier-analízise és amplitúdó komponensek Weibull-eloszlása.*

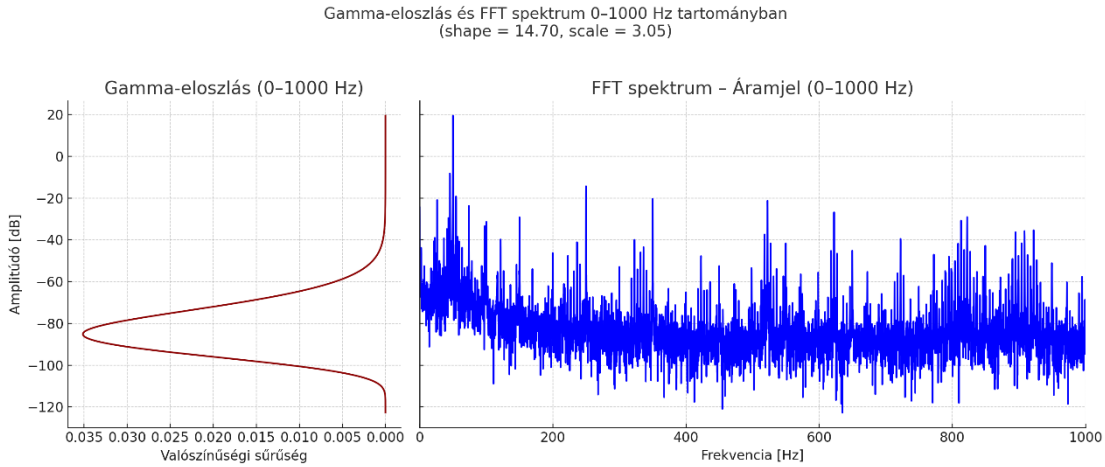



*13. ábra Háromfázisú csúszógyűrűs aszinkron motor forgórész áram Fourier-analízise és hozzátartozó amplitúdó komponensek Weibull-eloszlása (áramfelvétel 0002-számú mérése).*

A 14-15. ábrák esetén az eloszlás függvények az áramspektrum amplitúdó tengelyéhez vannak illesztve, amelynek a jelentősége abban van, hogy átláthatóbb frekvenciatartomány és az eloszlás függvény kapcsolata. Ebben az esetben Gamma-eloszlással függvénnyel szemléltetve [12].




*14. ábra Háromfázisú csúszógyűrűs aszinkron motor forgórész áram Fourier-analízise és amplitúdó komponensek Gamma-eloszlása.*



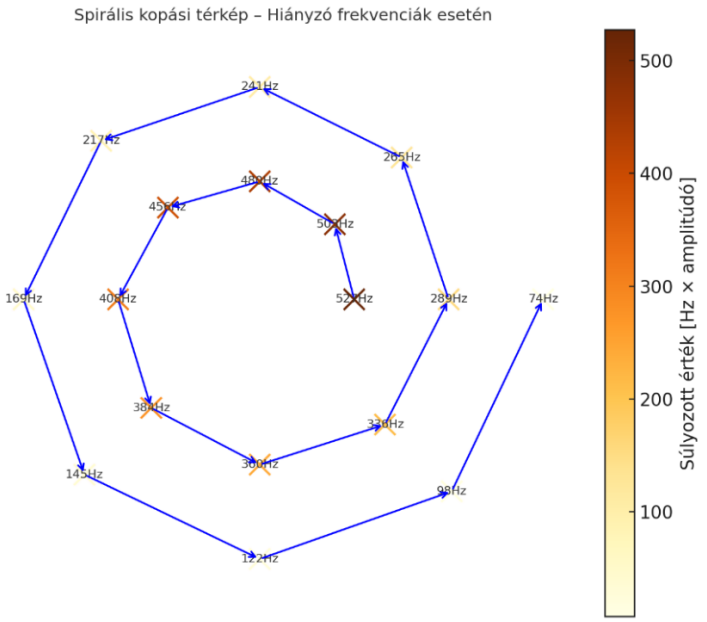

*15. ábra Háromfázisú csúszógyűrűs aszinkron motor forgórész áram Fourier-analízise és amplitúdó komponensek Gamma-eloszlása (0-1000 Hz-ig számolva).*

A [12] szakirodalom (Lukács Ottó: Matematikai statisztika című könyv) átfogóan tárgyalja a statisztikai módszerek alapjait, amelyek elengedhetetlenek a kutatások során. A könyv segítségével a kutatók képesek helyesen mintákat választani, eloszlásokat elemezni és hipotéziseket tesztelni. Bemutatja a lineáris regresszió, a korreláció és a többváltozós statisztika alkalmazását, amelyek nélkülözhetetlenek a komplex problémák megértéséhez (ebben az esetben az áramjel amplitúdó eloszlásait vizsgálva). A könyv rendszerezett elmé-

leti alapokat és gyakorlati példákat kínál, így kiváló eszköz a hazai kutatók számára. Összességében a könyv segít abban, hogy a kutatási eredmények megbízhatóak és tudományosan igazolhatók legyenek.

## KOPÁSI TÉRKÉPEK FEJLESZTÉSE MOTORÁRAM-JEL VIZSGÁLAT ALAPJÁN, HIBAJELEK RENDSZEREZÉSE, ÖSSZEFOGLALÁS

A 16-17. ábrák mutatják a kopási térkép két lehetséges változatát [9]. A első lépés a frekvenciaprioritás szerinti haladási sorrend kijelölése (16. ábra), a kopási térképe szemléletbe.




*16. ábra Spektrumból kiválogatott tengelyütési frekvenciák spirális elhelyezkedésük.*

A 16. ábrán egy spirális elrendezésű kopási térképet látunk, amely a „Hiányzó frekvenciák esetén” címkét viseli. A térkép célja az áramjelben megjelenő hibafrekvenciák spektrális jellemzőinek vizuális megjelenítése, különösen akkor, amikor egyes frekvenciák nem észlelhetők.

Az elrendezés spirálalakú, ami idő vagy kopási szint szerinti előrehaladást szimbolizálhat, így alkalmas a fokozatos változások bemutatására. A pontokon feltüntetett frekvenciaértékek (Hz-ben) mellett azok súlyozott amplitúdója (frekvencia × amplitúdó) is színkóddal jelenik meg. A színskála sötétbarnától a világossárgáig terjed, ahol a sötétebb színek magasabb súlyozott értékeket jeleznek.

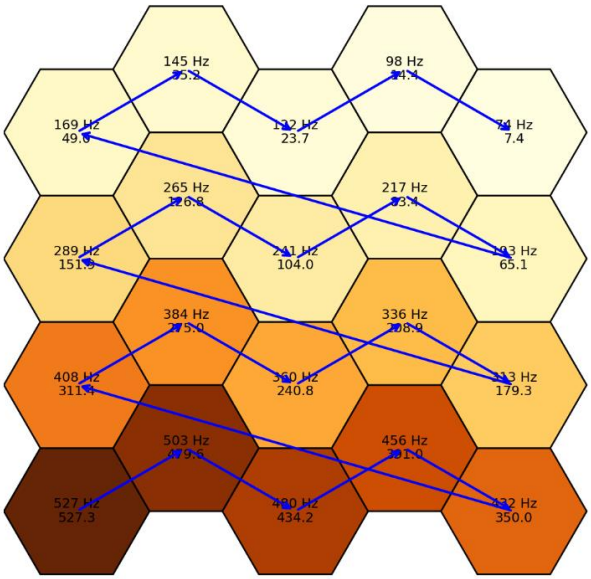
A 16. ábra kiemeli azokat a pontokat, ahol nagy intenzitású kopási jelek fordulnak elő, különösen 45 Hz, 52 Hz és 74 Hz környezetében. Ezeken a helyeken 'X' jelzés látható, ami a hiányzó vagy szokatlanul nagy frekvenciákra utal. A spirál mentén az egyes értékek közötti kapcsolatok kék vonalakkal vannak összekötve, jelezve a folytonosságot és az adatpontok közötti viszonyt. Az ilyen típusú megjelenítés hatékony eszköz lehet a forgógépek állapotfelügyeletében, különösen akkor, ha a hagyományos lineáris spektrumábrázolás nem

elég informatív. Az ábra különlegessége, hogy nemcsak az értékek nagyságát mutatja, hanem azok elhelyezkedését is egy vizuálisan jól értelmezhető struktúrában.

A 17. ábra egy kopási térkép haladási irány megjelöléssel méhsejt (Honeycomb) [9] típusú vizualizációt mutat, amely a frekvenciák és amplitúdók súlyozott értékeinek térbeli eloszlását szemlélteti hatszög (méhsejt) formában. A cellákban két adat szerepel: egy frekvencia érték (Hz-ben) és egy súlyozott érték (Hz × amplitúdó), melyeket színkódolás segítségével különböztetnek meg. A színek a világossárgától a sötétbarnáig terjednek, utóbbi a legnagyobb értékeket képviseli – például az alsó bal sarokban 527 Hz / 527.3. A színeloszlás jól láttatja a kopás intenzitásának mértékét, amely a térkép alsó részén sokkal hangsúlyosabb, mint a felső régióban.

A kék nyilak különlegessége, hogy explicit módon jelzik a haladás irányát, azaz azt az útvonalat, amely mentén a kopás (feltételezett haladási irány) jelensége terjed a térben. Ez a funkció a prediktív karbantartás szempontjából különösen értékes, mivel segít előre jelezni a károsodás terjedését. Az irányvonalak általában a nagyobb értékek felé mutatnak, tehát a rendszer logikusan halad a gyengébből az erőteljesebb hibatünetek felé. A középső sávban erős átmenetek figyelhetők meg, például 265 Hz / 126.8-tól 384 Hz / 275.0-ig, ami a kopási folyamat felerősödésére utal. A frekvenciaértékek is fokozatosan nőnek a spirálhoz képest rendezettebb, lineárisabb formában. Ezzel szemben a korábban vizsgált spirális kopási térkép inkább egy ciklikus vagy időben forgó elrendezést képviselt, amely a hibák fokozatos kialakulását vagy periodikus megjelenését sugallta. A spirál vizuálisan érdekes, de kevésbé rendszerezett, míg a jelenlegi méhsejtes térkép strukturált, jól szegmentált adatokat mutat. Míg a spirálban a frekvenciák időbeli ciklikussága dominált, a méhsejt (honeycomb) [9] térképen a térbeli viszonyok és útvonalak kaptak kiemelt szerepet.

A haladási irány megjelölésével az elemzés következtetései sokkal egyértelműbbé válnak, és a hibák forrása is jobban lokalizálható. A méhsejtek közötti szoros kapcsolatok, valamint a vizuálisan is követhető nyilak segítségével a rendszer viselkedése sokkal áttekinthetőbb. Az ilyen típusú ábrázolás különösen hatékony eszköz lehet forgógépek állapotfigyelésénél, hiszen egyaránt szolgál statikus és dinamikus diagnosztikára. Az irányított kopási térkép ezáltal nemcsak a jelenlegi állapotot mutatja be, hanem prediktív előrejelzést is biztosíthat a hiba tovább terjedéséről. Összességében elmondható, hogy ez az 17. ábra gazdagabb információval szolgál, és döntéstámogatás szempontjából is erősebb, mint a spirál alapú megjelenítés.




*17. ábra Háromfázisú csúszógyűrűs aszinkron motor tengelyütési frekvenciáinak méhsejt elrendezése és frekvenciaprioritás szerinti haladási iránya.*

A méhsejt kopási térkép egy speciális [10] vizualizációs módszer, amely a gépek rezgés- vagy kopáselemzésében alkalmazott frekvencia- és amplitúdóadatok térbeli eloszlását jeleníti meg hatszögletű cellákban. Minden cella egy adott elemzési pontot képvisel, és tartalmazza a jellemző frekvenciát (Hz) valamint a hozzá tartozó súlyozott értéket (frekvencia × amplitúdó).

A színskála segít gyorsan azonosítani a kritikus pontokat, ahol a kopás vagy rezgés mértéke magas. Az elrendezés előnye, hogy jól láthatók a lokális eltérések és az értékek közötti kapcsolatok. Amennyiben haladási irány is meg van jelölve, a térkép még hatékonyabban mutatja a hiba vagy kopás lehetséges terjedését. Ez a fajta megközelítés különösen hasznos a forgógépek prediktív karbantartásában, mivel lehetőséget ad a hibák forrásának pontosabb lokalizálására és a megelőző beavatkozásra.

## HONEYCOMB ALAPÚ KOPÁSI TÉRKÉP ALKALMAZÁSA FORGÓGÉPEK HIBADIAGNOSZTIKÁJÁBAN, ÖSSZEFOGLALÁS, KITEKINTÉS

### Bevezetés:

A korszerű állapotfelügyeleti rendszerek egyik kulcseleme a gépek működés közbeni rezgés- és frekvenciaelemzése. A hagyományos spektrumábrák mellett egyre nagyobb szerepet kapnak az olyan térbeli vizualizációs módszerek, amelyek lehetővé teszik a hibák lokalizációját és időbeli lefolyásának nyomon követését [9].

**Módszer:**

A mérési adatokat szenzorhálózat gyűjti különböző térbeli pozíciókban. Minden érzékelési ponton számítottunk egy frekvenciaértéket és annak súlyozott amplitúdóját (frekvencia × amplitúdó). Az eredményeket hatszög alakú cellákban ábrázoltuk, ahol a színskála a kopás intenzitását jelzi. A világos színek alacsonyabb, míg a sötét színek magasabb kopási szintet mutatnak [10].

**Eredmények:**

A honeycomb térképen jól láthatók azok a területek, ahol a gép alkatrészei intenzívebb hibát mutat. A méhsejt elrendezés előnye, hogy sűrűbb adatstruktúrák is jól megjeleníthetők, és a szomszédos cellák közötti összefüggések könnyen követhetők. A vizualizáció lehetővé tette a hibák térbeli terjedésének nyomon követését és a kritikus zónák korai azonosítását [11].

**Haladási irány megjelölése:**

A térképen alkalmazott kék irányvonalak a hiba lehetséges terjedését is szemléltetik. Ezek alapján nemcsak az aktuális állapot volt vizsgálható, hanem következtetések is levonhatók a jövőbeni fejlődésről.

**Következtetés:**

A méhsejt alapú kopási térkép hatékony eszköz a forgógépek hibáinak korai felismerésében és nyomon követésében. A módszer vizuálisan jól értelmezhető, részletgazdag, és alkalmas prediktív karbantartási stratégiák támogatására. További kutatások során javasolt a térképek automatizált elemzésének bevezetése neurális hálózatokkal vagy gépi tanulási algoritmusokkal.

## FELHASZNÁLT IRODALOM

[1] Jean-Claude Trigeassou, Electrical Machines Diagnosis, First published, 2011, Great Britian and the United States by ISTE Ltd and John & Sons, Inc. ISBN 978 1 84821 263 3

[2] Dr. Fodor György, Elméleti elektrotechnika II. Tankönyvkiadó, Budapest, 1989, ISBN 9631816095

[3] Bendiák István, Semperger Sándor, Aszinkron motorok mechanikai eredetű hibáinak elemzése áramjelalak-analízis módszerével: Temesvári, Zsolt; Wührl, Tibor; Molnár, György (szerk.) XXXVIII. Kandó Konferencia 2022 - Kiadvány kötet Budapest, Magyarország: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar (2022) 419 p. pp. 33-48. , 15 p.

[4] By Brian P. Graney and Ken Starry, Rolling Element Bearing Analysis, From Materials Evaluation, Vol. 70, No. 1, pp: 78-85, Copyright 2011 The American Society for Nondestructive Testing, Inc. Materials Evaluation- January 2012

[5] N. Bhole and S. Ghodke, "Motor Current Signature Analysis for Fault Detection of Induction Machine–A Review," 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), NaviMumbai, India, 2021, pp. 1-6, doi: 10.1109/ICNTE51185.2021.9487715.

[6] P. D. Yelpale, R. K. Jarial and A. J. Patil, "Fuzzy-based Induction Motor Fault Diagnosis Decision-Making System for Motor Current Signature Analysis," 2024 3rd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/INOCON60754.2024.10512034.
[7] M. S. Eddine, K. Djallel, G. Abdelhalim and M. R. Morakchi, "Comparative Study of Envelope and TKEO Demodulation Techniques for detecting Rotor bar breakage using Motor Current Signature Analysis (MCSA)," 2024 International Conference on Advances in Electrical and Communication Technologies (ICAECOT), Setif, Algeria, 2024, pp. 1-6, doi: 10.1109/ICAECOT62402.2024.10828764.
[8] K. Laxmi Sree and K. C. Deekshit Kompella, "High Resolution based Bearing Damage Identification in Poly Phase Asynchronous Motor using Gabor Transforms of Stator Current," 2021 IEEE Bombay Section Signature Conference (IBSSC), Gwalior, India, 2021, pp. 1-6, doi: 10.1109/IBSSC53889.2021.9673443.
[9] X. LI, B. -b. SUN and L. -w. SU, "Optimization of New Negative Poisson's Ratio Honeycomb Sandwich Reflector Structure," 2019 14th Symposium on Piezoelectrcity, Acoustic Waves and Device Applications (SPAWDA), Shijiazhuang, China, 2019, pp. 1-5, doi: 10.1109/SPAWDA48812.2019.9019311.
[10] X. -W. Yuan, Z. Yang, M. -J. Gou, M. -L. Yang and X. -Q. Sheng, "A Flexible and Efficient Method for the Analysis of Electromagnetic Scattering by Inhomogeneous Objects With Honeycomb Structures," in IEEE Antennas and Wireless Propagation Letters, vol. 21, no. 3, pp. 541-545, March 2022, doi: 10.1109/LAWP.2021.3138133.
[11] Xin Jin, Guoxi Li, Song Gao and Jingzhong Gong, "Optimal design and modeling of variable-density triangular honeycomb structures," 2017 8th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT), Cape Town, 2017, pp. 138-143, doi: 10.1109/ICMIMT.2017.7917452.
[12] O. Lukács, Matematikai statisztika, Budapest: Műszaki Könyvkiadó, 1999.
[13] H. Qiu, J. Lee, J. Lin, and G. Yu, "Wavelet filter-based weak signature detection method and its application on rolling element bearing prognostics," Journal of Sound and Vibration, vol. 289, no. 4–5, pp. 1066–1090, Feb. 2006. doi: 10.1016/j.jsv.2005.03.007.

DOI: https://doi.org/10.12700/btsz.2025.7.3.97

# HISTORICAL DEVELOPMENT OF LIGHTNING PROTECTION AND WITHIN LIGHTNING CURRENT DISTRIBUTION SIMULATION

# VILLÁMVÉDELEM ÉS AZON BELÜL A VILLÁMÁRAM-ELOSZLÁS SZIMULÁCIÓ TÖRTÉNETI FEJLŐDÉSE

SZIJÁRTÓ Gábor[1] – KOVÁCS Károly[2]

**Abstract**

Lightning protection in Hungary began to take a regulated form in the 1930s with the introduction of the first standard, MOSZ 274. Dr. Tibor Horváth played a significant role in advancing lightning protection research and education, resulting in the MSZ 274 standard series, which laid the foundation for national practices. During the 1960s, new perspectives emerged, such as the "rolling sphere" method, which gained worldwide recognition. From the 1990s, the modeling and simulation of lightning current distribution became increasingly important, supported by developments in electro-geometric models and computer simulations. Today, the design of lightning protection systems is governed by the MSZ EN 62305 standard series, which comprehensively addresses the protection of buildings and electrical systems against both physical and overvoltage effects. Simulation tools such as CDEGS and ATP-EMTP enable more accurate modeling of lightning currents, enhancing the safety and efficiency of protective measures. These advances ensure that lightning protection systems remain reliable and meet modern technological demands.

**Keywords**

lightning protection, lightning current distribution, EN 62305, model, simulation

**Absztrakt**

A villámvédelem Magyarországon az 1930-as években kezdett szabályozott keretek között működni, amikor meg-született az első szabvány, a MOSZ 274. Dr. Horváth Tibor professzor jelentős szerepet játszott a villámvédelmi kutatások és oktatás fejlesztésében, amelynek eredményeként az MSZ 274 szabványsorozat alapozta meg a hazai gyakorlatot. Az 1960-as években új szemléletet honosítottak meg, például a „gördülő gömb” módszert, amely világ-szerte elismertté vált. Az 1990-as évektől kezdődően a villámáram-eloszlás modellezésének és szimulációjának fontossága előtérbe került, különösen az elektro-geometriai modellek és a számítógépes szimulációk révén. A villámvédelmi rendszerek tervezése mára az MSZ EN 62305 szabványsorozaton alapul, amely részletesen foglalkozik az épületek és elektromos rendszerek fizikai és túlfeszültség elleni védelmével. A szimulációs eszközök, mint például a CDEGS és az ATP-EMTP, lehetővé teszik a villámáram pontosabb modellezését, támogatva a biztonságosabb és hatékonyabb védekezést.

**Kulcsszavak**

villámvédelem, villámáram-eloszlás, MSZ EN 62305, modell, szimuláció

[1] szijarto.gabor@phd.uni-obuda.hu | ORCID: azonosító 0009-0009-8856-871X | PhD student, Obuda University, Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

[2] kovacs.karoly@kvk.uni-obuda.hu | ORCID: azonosító 0009-0006-8180-1919 | university assistant professor, Obuda University, Kandó Kálmán Faculty of Electrical Engineering | egyetemi adjunktus, Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar

## BEVEZETÉS

A villámvédelem hazai történeti áttekintése során fontos kiemelni, hogy Magyarországon az első villámvédelmi szabályozás az 1930-es években alakult ki, később Dr. Horváth Tibor professzor munkásságának köszönhetően részletesebben ki lett dolgozva, aki a hazai villámvédelmi szakma megalapítója és vezető alakja volt. Az MSZ 274 szabványsorozatot ő fejlesztette ki, amely később az ország villámvédelmi rendszereinek alapját képezte, és jelenleg nem norma szerinti villámvédelem-ként ismert.

Horváth professzor jelentős szerepet játszott a Budapesti Műszaki Egyetem Villamosmérnöki Karán, ahol a Nagyfeszültségű Technika Tanszék vezetőjeként formálta a villámvédelem oktatását és kutatását. Tudományos munkájának egyik legfontosabb eredménye a villám becsapási helyét valószínűségi alapon tárgyaló elmélet volt, amely az 1960-as évek elején született meg. Ennek köszönhetően új szemléletet honosított meg, amely a villámvédelmi rendszerek vonzási terét és a villámcsapás fizikai folyamatait helyezte előtérbe, a korábbi, egyszerűbb védett tér megközelítés helyett. [1] Ez az innováció elősegítette a "gördülő gömb" módszer kidolgozását is, amelyet 1962 óta a magyar szabványokban alkalmaznak, és amely a villámvédelmi rendszerek szerkesztésében világszerte elfogadott eljárássá vált.

## A VILLÁMVÉDELEM TÖRTÉNETÉNEK ÁTTEKINTÉSE

### Kezdetek és korai rendszerek

A villámvédelem hazai szabályozása több évtizedes múltra tekint vissza, amelyet folyamatos átalakulások és fejlesztések jellemeztek, a biztonság növelését és az épületek, valamint az elektromos rendszerek védelmét szolgálva. A magyarországi villámvédelmi szabályozás fejlődése több szakaszra osztható, amely szakaszok a villámáram biztonságos földbe vezetésének kezdeti, egyszerű megoldásaitól a komplexebb védelmi rendszerek kialakításáig terjedtek.

Az első hazai szabvány, a 16 oldalas MOSZ 274, 1937-ben jelent meg, és a villámvédelmi megoldások még elsősorban a közvetlen védelemre összpontosítottak, vagyis a villámáram biztonságos földelésére. Az 1950-es évek szabványai még szintén ezen alapelvre épültek.

A '60-as években új fejlesztések következtek be a villámvédelem terén. A szabványok ekkor már a tetők, épületek és földelő rendszerek biztonságosabb kialakítására helyezték a hangsúlyt. Az MSZ 274 szabványsorozat elődje, amely évtizedeken át, 1937-től kezdve meghatározó alapját képezte a villámvédelmi szabályozásnak Magyarországon, több kiadást és módosítást is megélt, hogy lépést tartson a technológiai fejlődéssel és a villámvédelmi elvárásokkal.

Kezdeti időszakban megjelent szabványok:

- MOSZ 274, 1937. június (Biztonsági irányelvek villámcsapások romboló hatásának elhárítására);
- MNOSZ 274-52, 1953. február 15. (Biztonsági irányelvek villámcsapás káros hatásainak elhárítására)
- MNOSZ 274-52, Kiegészítés (1954)
- MSZ 274-62 1963. július 1. (Villámvédelem)
- MSZ 274-72 1973. július 1. (Villámvédelem)

**Kezdetek és korai rendszerek**

Az 1981-es módosítások és a gördülő gömbös módszer által bevezetett új védelmi szintek fontos előrelépést jelentettek, amelyek a villámcsapás becsapódásának pontosabb modellezését és hatékonyabb eloszlását tették lehetővé.

Az MSZ 274 szabványsorozat további megjelenései:

- MSZ 274/1-77 1977. október 1. - 2009. február 1. (Villámvédelem, Fogalommeghatározások)
- MSZ 274/2-81 1982. január 1. - 2009. február 1. (Villámvédelem, Épületek és egyéb építmények villámvédelmi csoportosítása)
- MSZ 274/3-81 1982. január 1. - 2009. február 1. (Villámvédelem, A villámhárító berendezés műszaki követelményei)
- MSZ 274/3-81, 1. módosítás (1985)
- MSZ 274/3-81, 2. módosítás (2001)
- MSZ 274/4-77 1978.április 1. - 2009. február 1. (Villámvédelem, Felülvizsgálat)
- MSZ/T 274-5:1994 (Villámvédelem, Az elektromágneses villámimpulzus elleni védelem)

Az idő előrhaladtával a villámcsapások másodlagos hatásai, így a túlfeszültségek elleni védelem is egyre fontosabbá vált. A modern elektronikai eszközök elterjedése ugyanis növelte annak szükségességét, hogy a szabályozás figyelembe vegye a villámcsapás közvetett hatásait is, melyek a berendezéseket károsíthatják.

Az MSZ 274 legutolsó kiadásai már részletesen meghatározták a villámvédelmi rendszer kialakítására és karbantartására vonatkozó követelményeket, beleértve a felfogók, levezetők, földelők és potenciálkiegyenlítési intézkedések részletes előírásait. A magyar szabványok kialakításában jelentős nemzetközi kapcsolatokat is kialakítottak. Horváth Tibor aktív szereplője volt az International Conference on Lightning Protection (ICLP) munkájának, ahol Magyarország több alkalommal is rendezőként vett részt, és amely konferencia-sorozat révén a magyar villámvédelem nemzetközi elismerésnek örvendett. A 2000-es évek elejére az európai uniós csatlakozással és nemzetközi szabványok bevezetésével egyidejűleg, hivatalosan is visszavonták a témával foglalkozó magyar szabványt, így a nemzetközi IEC/EN 62305 váltotta fel az MSZ 274 szabványsorozatot.

**Jelenlegi előírások**

Az MSZ EN 62305 villámvédelmi szabványsorozat első kiadása 2006-ban látott napvilágot, majd 2011-ben került bevezetésre Magyarországon, az európai szabványokhoz igazodva. E szabványsorozat célja, hogy átfogó védelmet biztosítson az épületek, az elektromos és elektronikus rendszerek számára mind a közvetlen villámcsapások, mind a másodlagos túlfeszültséghatások ellen.

Az MSZ EN 62305 szabványsorozat az európai szabványokkal harmonizálva biztosít átfogó védelmet az épületek, valamint az elektromos és elektronikus rendszerek számára.

Ez a szabványsorozat négy fő részből áll:

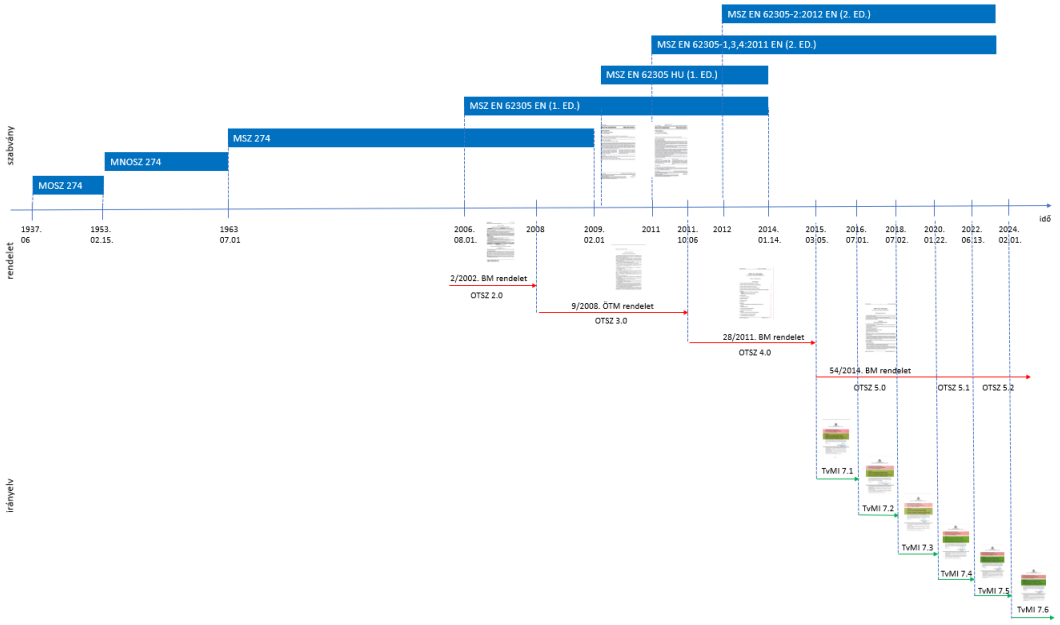
- MSZ EN 62305-1: Általános alapelvek: Ez a rész bemutatja a villámvédelem alapvető fogalmait, a villámcsapás fizikai jellemzőit és a védelem tervezésének általános irányelveit.

- MSZ EN 62305-2: Kockázatkezelés: Ebben a részben a villámcsapás okozta kockázatok felmérésének és értékelésének módszertanát ismertetik, segítve a megfelelő védelmi intézkedések kiválasztását.
- MSZ EN 62305-3: Építmények fizikai károsodása és életveszély: Ez a rész az épületek külső villámvédelmi rendszereinek tervezésére és kivitelezésére vonatkozó követelményeket tartalmazza, beleértve a felfogók, levezetők és földelők kialakítását.
- MSZ EN 62305-4: Villamos és elektronikus rendszerek építményekben: Ez a rész az épületek belső villámvédelmére fókuszál, különös tekintettel az elektromágneses impulzusok elleni védelemre és a túlfeszültség-védelmi intézkedésekre.

Az OTSZ változások időpontját és tartalmát nem mutatjuk be részletesen.

A szabványsorozat alkalmazása mellett a villámvédelemmel kapcsolatos követelményeket először a 2002. január 23-án hatályba lépett az első olyan tűzvédelemmel foglalkozó rendelet, ami a villámvédelmi követelményeket szabályozta. Később Országos Tűzvédelmi Szabályzatként (OTSZ) jelent meg a 9/2008 ÖTM rendelet, majd a 28/2011. BM rendelet, jelenleg pedig az 54/2014. BM rendelet határozza meg a követelményeket villámvédelem vonatkozásában. A hatályos OTSZ meghatározza a villámvédelmi rendszerek tervezésére, kivitelezésére és felülvizsgálatára vonatkozó előírásokat.

A jelenlegi villámvédelmi előírások Magyarországon nemcsak az MSZ EN 62305 szabványsorozaton alapulnak, hanem a Tűzvédelmi Műszaki Irányelvek (TvMI) és a Tűzvédelmi Törvény legutóbbi változásai is meghatározzák az alkalmazandó villámvédelmi követelményeket. A jogszabályi, szabványi, irányelvi változásokat az 1. ábra mutatja be.




*1. Ábra: Magyarországi jogszabályi, szabványi, irányelvi változások, saját szerkesztés*

Emellett a Tűzvédelmi Törvény [1] módosításai is hatással voltak a villámvédelmi előírásokra. A Tűzvédelmi Műszaki Irányelvek (TvMI) létrehozását az Országos Katasztrófavédelmi Főigazgatóság (OKF) irányította azzal a céllal, hogy konkrét, gyakorlati útmutatást adjon az OTSZ-ben meghatározott követelmények alkalmazására. A TvMI előírásai részletes leírásokat és példákat tartalmaznak a villámvédelmi rendszerek tervezéséhez, kivitelezéséhez és felülvizsgálatához. A TvMI a különböző létesítmények rendeltetéséhez, építési anyagaihoz és technológiai adottságaihoz igazítva nyújt specifikus útmutatást, így támogatva a villámvédelmi előírások pontos és szakszerű alkalmazását.

**DIN EN 62305-4 1. nemzeti melléklet: villámáram-eloszlás**

A DIN EN 62305-4 szabvány 1. nemzeti melléklete kifejezetten a villámáram-eloszlással kapcsolatos követelményeket és útmutatásokat tartalmazza Németországban. Ez a melléklet az általános európai előírásokat egészíti ki, hangsúlyt fektetve a németországi körülmények és sajátosságok figyelembevételére.

A melléklet bemutatja azokat a modelleket, amelyekkel a villámáram eloszlását számítani lehet az épületekben és az azokban található elektromos rendszerekben. Részletes iránymutatást ad arra vonatkozóan, hogyan kell figyelembe venni a villámcsapás különböző eloszlási áramutait. A melléklet olyan gyakorlati példákat és esettanulmányokat tartalmaz, amelyek bemutatják, hogyan kell a villámáram-eloszlási modelleket alkalmazni a különböző típusú épületekben és ipari létesítményekben.

**EN 62305 3. kiadás**

Az EN 62305 szabványsorozat harmadik kiadásában tovább finomították a villámáram-eloszlásra vonatkozó irányelveket, különös tekintettel a villámvédelmi rendszerek tervezésére és a túlfeszültség-védelmi eszközök kiválasztására. A cél a villámáram útjának pontosabb modellezése és a védelmi intézkedések hatékonyságának növelése.

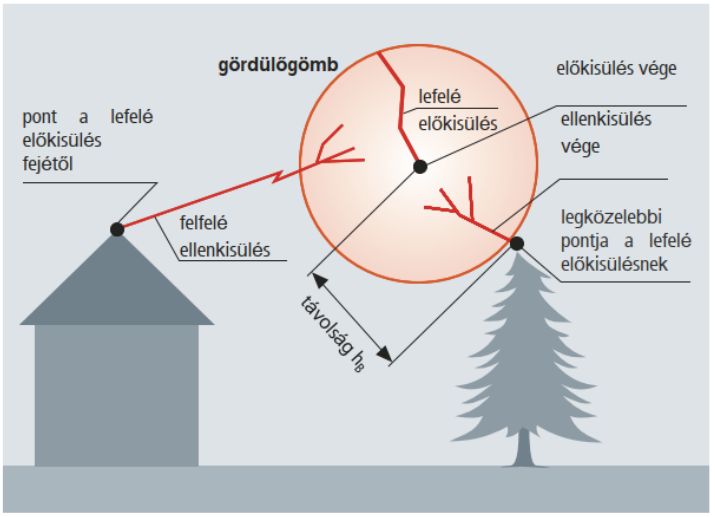
A villámáram-eloszlás pontosabb meghatározása lehetővé teszi a villámvédelmi rendszerek optimalizálását, csökkentve a villámcsapás okozta károk kockázatát. A szabvány frissítései várhatóan figyelembe veszik a legújabb kutatási eredményeket és a gyakorlati tapasztalatokat, biztosítva a villámvédelmi rendszerek megbízhatóságát és hatékonyságát.

## VILLÁMÁRAM-ELOSZLÁS SZIMULÁCIÓ NEMZETKÖZI FEJLŐDÉSE

A villámáram-eloszlás szimuláció nemzetközi fejlődése jelentős mérföldkő a villámvédelmi rendszerek kialakításában és fejlesztésében. Az elmúlt évtizedek során számos kutatás és technológiai újítás látott napvilágot világszerte, amelyek célja a villámcsapások által okozott károk minimalizálása és a védelem hatékonyságának növelése. A villámáram útjának pontos meghatározása, valamint annak biztonságos elvezetése az épületek és elektromos rendszerek védelmének alapvető elemeivé váltak. Ebben a fejezetben áttekintjük a villámáram-eloszlás fejlődésének nemzetközi trendjeit, bemutatjuk a különböző módszereket, amelyek az idők során kialakultak.

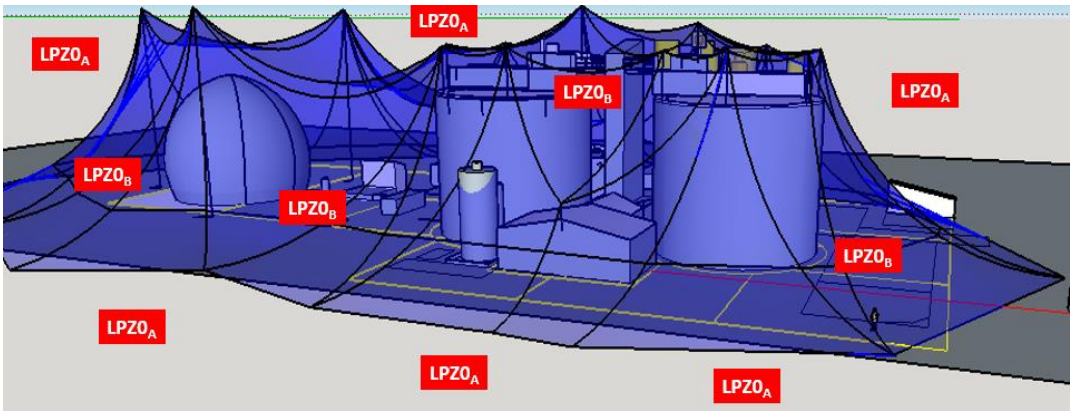
## Elektro-geometriai modell

Az elektro-geometriai modellek (Electro-Geometric Models, EGM) és a villám-áram-eloszlás közötti összefüggés alapvető fontosságú a villámvédelmi rendszerek tervezésében. Az EGM célja, hogy építmény esetében a villám lehetséges becsapási pontjait meghatározza.




*2. Ábra: Villámcsapás kialakulásának folyamata, [3]*

Figyelembe kell venni a gördülőgömb-módszerrel történő villámvédelmi szerkesztést. Ennek eredményeképpen csak azokba a pontokba injektálunk villámáramot, ahol ténylegesen lehetséges becsapási talppont a villámvédelmi szerkesztés alapján. A 3. ábrán gördülőgömb-módszerrel szerkesztett védett tér bemutatás látható, ahol a gömbfelület alatt elhelyezkedő terek védettnek minősülnek, mivel ezekbe a villám a modell alapján nem képes becsapni.



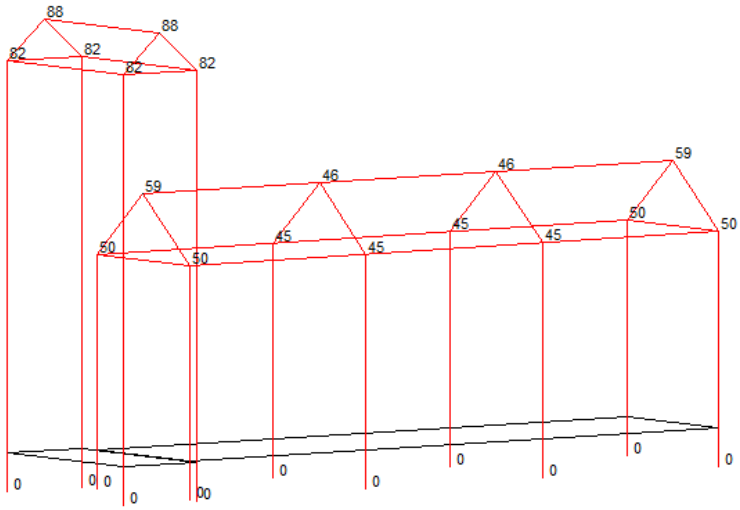

*3. Ábra: Villámcsapás kialakulásának folyamata, saját szerkesztés*

Az LPZ (Lightning Protection Zone – villámvédelmi zóna) jelölések az ábrán az MSZ EN 62305 szabvány szerint arra szolgál, hogy különböző területeket villámvédelmi

szempontból kategorizáljunk. Az LPZ $0_A$ és LPZ $0_B$ zónák a külső környezetre, a közvetlen villámcsapás veszélyének kitett területekre vonatkoznak. LPZ $0_A$ a közvetlen villámcsapásnak kitett tér, míg az LPZ $0_B$ közvetlen villámcsapástól védett tér. Mindkét esetben a villámcsapás elektromágneses tér hatása érvényesül.

Ezt követően a villámáramot minden lehetséges becsapási pontra beinjektáljuk, majd elemezzük annak eloszlását a külső villámvédelmi rendszer elemeiben, valamint – ha van kapcsolat – a belső rendszerekben is.

A 4. ábrán egy épület villámvédelmi rendszerének vázlata látható. Az épületen látható vezetők egy villámvédelmi rendszer részét képezik, amelyek felfogják a villámcsapásokat, és biztonságosan levezetik az áramot a földbe. A vörös vonalak jelölik a felfogó- és levezető rendszert, figyelembe véve az épület kritikus pontjait, például a tető és a sarkok. Az épület tetején és kiemelt pontjain elhelyezett vezetők, amelyek a villámcsapást hivatottak felfogni. Függőleges vezetők, amelyek a felfogott villámáramot biztonságosan levezetik az épület körüli földelőrendszerbe.




*4. Ábra: Épület villámvédelmi hálózatos rendszerének elektrogeometriai modellje, saját szerkesztés*

Az EGM konkrétan arra a kérdésre ad választ, hogy a villámáram hogyan oszlik el az épületek és egyéb szerkezetek különböző pontjai között.

**Kockázatelemzés és számítógépes szimulációk**

A valószínűségi modellek és digitális szimulációk alkalmazása lehetővé tette a villámáram eloszlásának pontosabb meghatározását.

A villámvédelmi kockázatelemzés egy olyan folyamat, amelynek célja, hogy felmérje a villámcsapásból eredő lehetséges kockázatokat egy adott épületben vagy létesítményben, és meghatározza a szükséges védelmi intézkedéseket. Ez az elemzés különösen fontos, mivel a villámcsapások súlyos károkat okozhatnak, beleértve az anyagi veszteséget, a személyi sérüléseket, valamint az elektromos és elektronikai rendszerek meghibásodását.

Magyarországon az MSZ EN 62305 szabványsorozat szabályozza a villámvédelmi rendszerek tervezésének és kivitelezésének részleteit, amely nemzetközi normákon alapul.

Ezen belül a MSZ EN 62305-2:2012 rész foglalkozik kifejezetten a villámvédelmi kockázatelemzéssel. Ez a szabvány előírja a kockázatelemzés végrehajtását, amely során az épület, a benne található eszközök és a környezet figyelembevételével kell megállapítani a szükséges védelem szintjét.

A villámvédelmi kockázatelemzésben fontos szerepet játszik a villámáram-eloszlás szimulációban, mivel a kockázatelemzés során határozzák meg, hogy milyen LPL (Lightning Protection Level: villámvédelmi szint) szintű potenciálkiegyenlítés szükséges.

Az EGM modellezés eredményét használva szimuláció segítségével vizsgálható a villámáram lehetséges utjai, és meghatározhatók azok a pontok, ahol a legnagyobb a villámrészáram értéke.

A villámáram-eloszlás szimulációval meghatározható, hogy miképpen érdemes kialakítani a külső villámvédelmi rendszert (pl. levezetők száma, földelőrendszer elrendezése, stb.), mekkora villámáram-levezetőképességgel rendelkezzenek a túlfeszültség-védelmi eszközök (surge protective device, röviden: SPD). A szimuláció eredményei alapján konkrét intézkedéseket lehet tervezni a villámvédelmi rendszer hatékonyságának növelésére és a kockázatok minimalizálására.

Számos szoftver létezik, amelyekkel villámáram-eloszlás szimulációt lehet készíteni. Ezek a programok általában olyan speciális funkciókkal rendelkeznek, amelyek lehetővé teszik a villámvédelmi rendszerek tervezését, az árameloszlás és a potenciálkülönbségek szimulációját.

### CDEGS (Current Distribution, Electromagnetic Fields, Grounding and Soil Structure Analysis)

A CDEGS egy átfogó szimulációs szoftver, amelyet földelési és villámvédelmi rendszerek tervezésére használnak. Képes modellezni a villámáram eloszlását és annak hatásait az épületek és a földelőrendszerek különböző pontjain. Használható többféle építmény esetén, mint például lakóépületek, ipari létesítmények és alállomások.

A szoftver különösen jól alkalmazható villámáram-eloszlási szimulációra, mivel képes figyelembe venni a fajlagos talajellenállásokat, a különböző anyagokat, valamint a villám által keltett elektromágneses mezőket. Nagyon pontos eredményeket nyújt komplex földelőrendszerek és villámvédelmi elrendezések esetén. Nagyobb ipari projektekhez ideális.

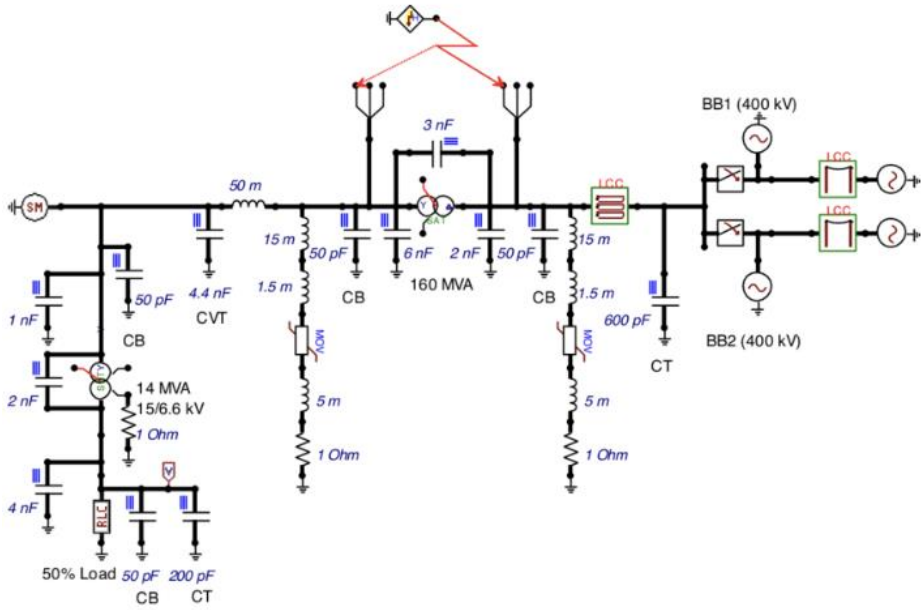
### ATP-EMTP (Alternative Transients Program - Electromagnetic Transients Program)

Az ATP-EMTP egy széles körben használt szoftver elektromágneses tranziens jelenségek szimulációjára, amely lehetővé teszi a villámáram által keltett túlfeszültségek és árameloszlás elemzését. Az energiaátviteli és elosztóhálózatok analízisére is használják, beleértve a villámcsapás okozta tranziens jelenségeket. Képes a villámáram-eloszlást modellezni különféle hálózati elemekben, így például kábelekben, transzformátorokban és alállomásokban.

Az 5. ábrán egy nagyfeszültségű alállomás szimulációs modellje látható. A modell részletesen bemutatja az alállomás különböző komponenseit, a villamos kapcsolódási pontokat, valamint a túlfeszültség-védelmeket. Főbb elemek:

- SH: villamos hálózatot szimbolizáló feszültségforrás
- BB: gyűjtősín csatlakozások, feszültségforrások

- CB (Circuit Breaker): Különböző helyeken található megszakítók, amelyek az áramkör megszakítására szolgálnak.
- CT (Current Transformer): Áramváltók, amelyek a mért áram nagyságának megfelelő arányos értéket biztosítanak a mérési rendszer számára.
- CVT (Capacitive Voltage Transformer): Kapacitív feszültségváltó, amely a nagyfeszültségű rendszerek feszültségmérésére szolgál.
- LCC: szűrő vagy kapcsolóeszköz (főként középfeszültségű rendszerekben használják), amely a villámáramokat kezeli.
- 50% Load: Az áramkör egyik pontján található 50%-os terhelés, amely szimulálja a rendszerben jelenlévő fogyasztói terhelést.
- 160 MVA és 14 MVA transzformátorok: Két különböző kapacitású transzformátor, amelyek a feszültségszintek átalakításáért felelősek.

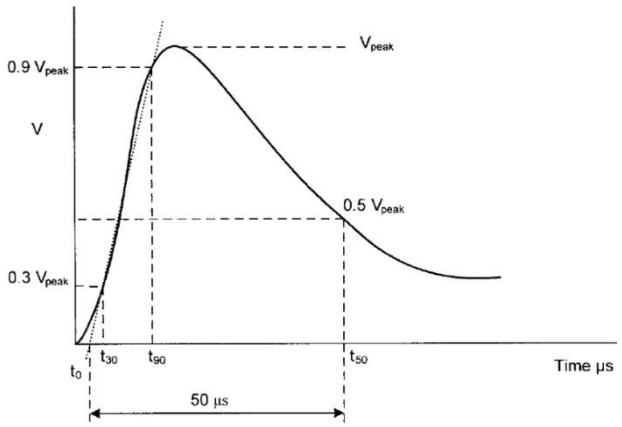



*5. Ábra: Nagyfeszültségű alállomás modellje villámáram és túlfeszültség-védelmi elemekkel [4]*

Az ábrán különböző kapacitív és induktív elemek is találhatók (pl. 50 pF, 1 Ω), amelyek a szimuláció során a valós hálózat viselkedésének modellezésére szolgálnak.

A 6. ábrán egy Heidler-féle villámáram hullámalak látható, amelyet az ATP-EMTP szoftverrel szimuláltak. Az ábra a villámáram időbeli változását mutatja be, amely a csúcspontján éri el a maximális értéket (V_peak). Az ábra jelölései a következők:

- t0: Az áram indulási pontja az időtengelyen.
- t30 és t90: A csúcspont elérésének jellemző időpontjai, ahol az áram a csúcspont 30%-át (t30) és 90%-át (t90) éri el.
- t50: Az az időpont, amikor az áram visszaesik a csúcsérték 50%-ára, ami a hullámlecsengési idő jellemzésére szolgál.
- 50 µs időtartam: A teljes áramimpulzus időtartama, amely az emelkedés és csökkenés fázisát is magába foglalja.



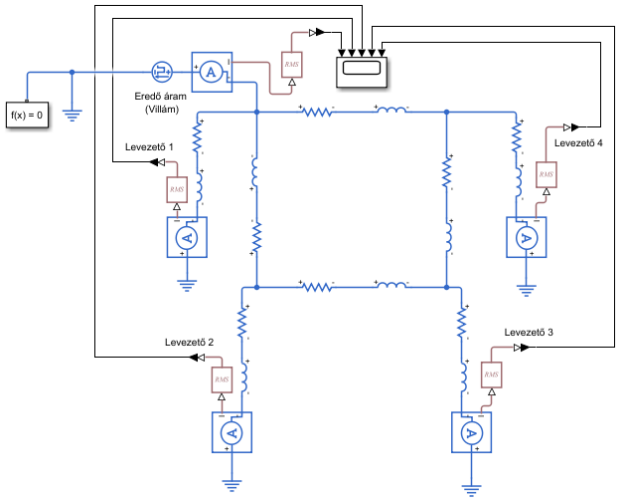

*6. Ábra: Heidler-féle villámáram hullámalak ATP-EMTP szimulációval [4]*

## XGSLab (eXGND and SLO Grounding System Laboratory)

Az XGSLab egy speciális szoftver, amelyet villámvédelmi rendszerek elemzésére is terveztek. A program különböző modulokból áll, amelyek lehetővé teszik az elektromágneses mezők, árameloszlások és potenciálkülönbségek szimulációját. Magas szintű pontossággal képes szimulálni a villámáram-eloszlást, figyelembe véve a talajrétegeket, a fajlagos talajellenállásokat és a hálózati elemeket. Könnyen kezelhető felhasználói felület, és képes különböző nemzetközi szabványoknak megfelelően modellezni.

## MATLAB és Simulink

A MATLAB és a Simulink alkalmazható villámvédelmi rendszerek (LPS: lightning protection system) modellezésére és elemzésére. A 7. ábrán bemutatott modell minden egyes vezetőszakaszát ellenállás, induktivitás (ha szükséges kapacitás) paraméterekkel lehet jellemezni, figyelembe véve a vezetők anyagát és méreteit. A modell egyik pontjára 10/350 µs hullámalakú, tetszőleges csúcsértékű villámáram-impulzust lehet injektálni egy oszcilloszkóp segítségével.



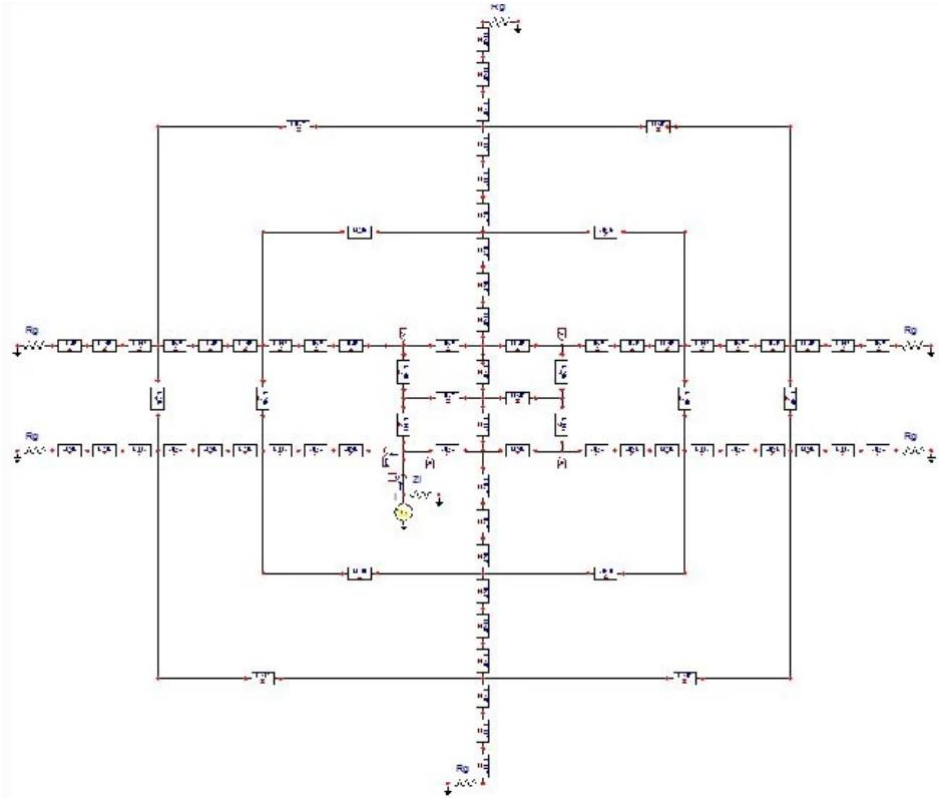

*7. Ábra: Modell villámáram-eloszlás szimulációhoz MATLAB Simulink programmal, saját szerkesztés*

Ezek a programok lehetővé teszik a villámáram-eloszlás pontos szimulációját különböző villámvédelmi rendszerekben, ezáltal segítve a tervezőket a hatékony és biztonságos villámvédelmi megoldások kialakításában.

**Nemzetközi példák villámáram-eloszlás szimulációra**

Három nemzetközi példa a villámvédelmi rendszerek szimulációjára, amelyek különböző megközelítéseket alkalmaznak – többek között a MATLAB/Simulink, az ATP/EMTP és egyéb numerikus modellezési eszközök segítségével

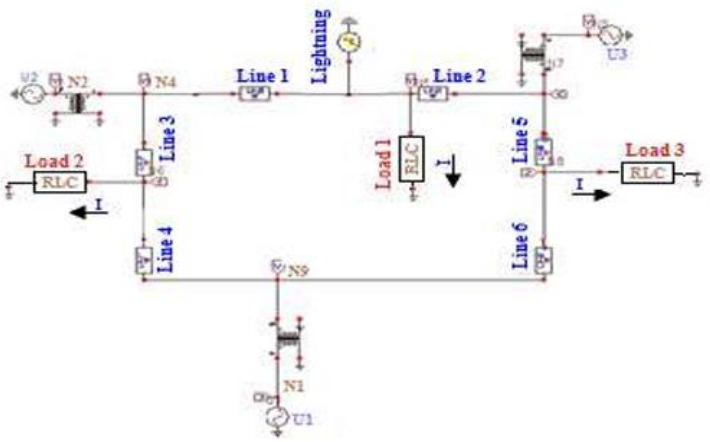
Az 1. esetben [5] egy többszintes épületre fejlesztettek ki a 8. ábrán látható villámvédelmi modellt ATP/EMTP környezetben.



*8. Ábra: Többszintes épület villámvédelmi rendszerének ATPDraw szimulációs modelljei A jelű becsapási pontra [5]*

A szimuláció célja az volt, hogy bemutassa a villámáram útját és eloszlását az épület különböző fémes részein és levezetőin keresztül. A modell figyelembe veszi a földelés és a levezetők paramétereit is. A szimulációk rámutattak arra, hogy a földelési rendszer geometriai kialakítása jelentős hatással vannak az árameloszlásra és a feszültségemelkedésre.

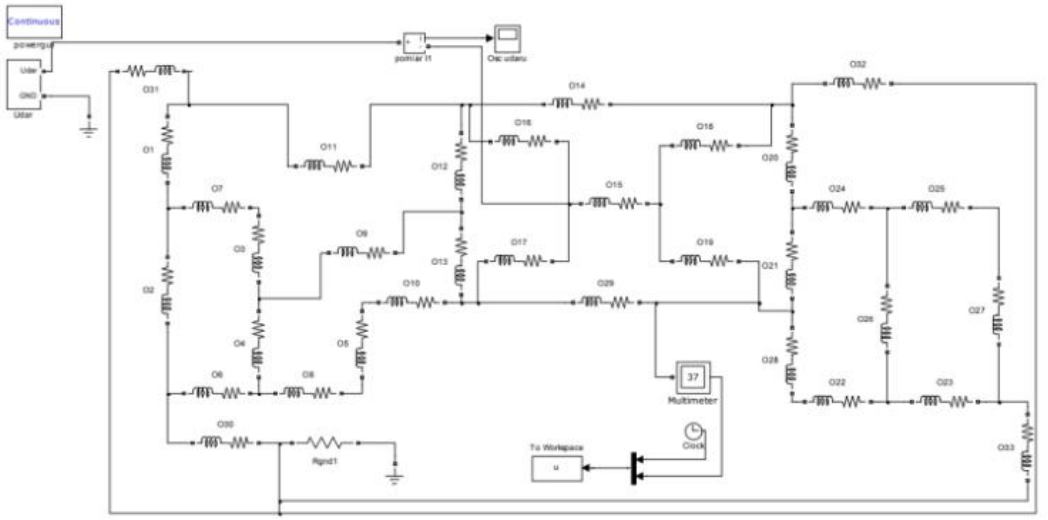
A 2. kutatás [6] két különböző platform – MATLAB/Simulink és ATP/EMTP – összehasonlítására fókuszál a villámcsapások hatásainak vizsgálata során. A 9. ábrán látható modell egy tipikus elektromos hálózatot szimulál, ahol különféle villámáram-hullámformák kerülnek beinjektálásra, és ezek hatását analizálják különböző rendszerkomponensekre (transzformátorokra, vezetékhálózatra, földelőrendszerekre).




*9. Ábra: Villámcsapás szimulációja az 5-ös csomóponton ATP-vel [6]*

A MATLAB előnye a könnyebb modellparaméterezés és a gyors vizualizáció, míg az ATP/EMTP nagyobb részletességet kínál a tranziens jelenségek leírásában. Az összehasonlításból kiderül, hogy mindkét eszköz kiegészíti egymást a precíz és hatékony modellezés érdekében.

A 3. esettanulmányban [7] a szerző egy épület villámvédelmi rendszerének a 10. ábrán látható áramköri modelljét alakította ki MATLAB, Simulink környezetben.




*10. Ábra: Villámvédelmi rendszer szimulációs modellje [7]*

A szimuláció célja az volt, hogy feltárja az egyes levezetőkön áthaladó áramok időbeli változását, és ezek kapcsolatát az eredő villámárammal. Az egyes vezetőszakaszokat az azok hosszával arányos impedanciák jellemzik (ellenállás és induktivitás). Az eredményekből következtetni lehet arra, mely szakaszoknál lehet kontrollálatlan átütés kockázata, és ezáltal hol szükséges árnyékolás vagy szerkezeti átalakítás a megfelelő védelem kialakításához.

## VILLÁMÁRAM-ELOSZLÁS NEMZETI FEJLŐDÉSE

Magyarországon a villámáram-eloszlás figyelembevételét az MSZ EN 62305 szabványsorozat, különösen annak negyedik részének (MSZ EN 62305-4) előírásai szabályozzák. Jelenleg nincs olyan előírás, ami kötelezővé tenné villámáram-eloszlás szimuláció készítését.

### Hazai publikációk

Az Elektroinstallateur folyóirat 2013 és 2014 során több részes cikksorozatot [8][9][10][11][12][13][14] publikált a villámáram-levezető rendszerek tervezési és beépítési szabályairól, amelyben részletesen foglalkoztak a villámáram-eloszlással is. Ez a cikksorozat különféle szempontokat tárgyalt, például a villámáram levezetési útvonalait, a túlfeszültség-védelmi készülékek kiválasztásának kritériumait, valamint a villámvédelem telepítésének gyakorlati kérdéseit. A sorozat célja az volt, hogy segítse a villamosipari szakembereket a szabványoknak megfelelő villámvédelmi rendszerek kialakításában és telepítésében.

A cikksorozatot a villámáram-eloszlás alapos vizsgálatára alapozták, amelyhez főként németországi és osztrák szabványok, kutatási eredmények és számítógépes szimulációk szolgáltatták az alapot. A cikksorozatban a villámáram-eloszlás elméleti és gyakorlati kérdéseit mutatták be, a cél az volt, hogy részletes útmutatást nyújtsanak a magyar villamos tervezőknek, különös tekintettel az MSZ EN 62305 és DIN EN 62305 szabványokra.

Az egyik legfőbb referencia a DIN EN 62305-4 szabvány 1. nemzeti melléklete volt, amely a német villámáram-eloszlás tervezési gyakorlatát tükrözi. Ezt a mellékletet 2012-ben frissítették, és különböző villámáram-szimulációk alapján részletes iránymutatásokat nyújt a villámvédelmi rendszerek és a túlfeszültség-védelem koordinált kialakítására, figyelembe véve az épületek földelő rendszereit és a villámáram eloszlásának modelljeit.

A cikksorozatban bemutattak olyan számítógépes szimulációkat is, amelyek az S1 (épületbe csapódó villám) és az S3 (vezetékeket érő villámcsapás) típusú kárforrásokat vizsgálják. A szimulációk az elektromos rendszerek különböző részeire vonatkozó árameloszlást modellezik, és figyelembe veszik a vezetékek impedanciáját, a földelőrendszerek ellenállását és a túlfeszültség-védelmi eszközök (SPD-k) szükséges beépítési helyeit.

A cikksorozat említést tesz az osztrák ALDIS villámkutató állomás vizsgálatairól, amelyek különösen a tartós villámkisülések esetében szolgáltattak hasznos adatokat. Ezek a kutatások rávilágítottak arra, hogy a téli zivatarok során keletkező hosszabb kisülések jelentős villámáramot generálnak, amelyeket a helyi szabványok alapján kiértékelve be lehet építeni a villámáram-eloszlási modellekbe.

A német szakirodalom több mintapéldát dolgozott ki az épületek és csatlakozó vezetékek villámáram-eloszlására, beleértve az 50-50%-os eloszlási alapfeltevést. Ez a megközelítés az egyes villámvédelmi szintekhez (LPL) kötődően különböző paraméterekkel számol, amelyek segítenek a tervezőknek a valósághoz közelebb álló eloszlási modellek kialakításában.

A cikksorozat célja, hogy részletes és gyakorlatias útmutatót nyújtson a magyar villámvédelmi rendszerek tervezéséhez, különös tekintettel a külföldi szabványokban megjelenő modellek és szimulációk alkalmazására. Az így szerzett tudás lehetővé teszi a hatékonyabb és biztonságosabb villámvédelmi megoldások kidolgozását a hazai villamosipari gyakorlatban.

**Hazai konferencia előadás**

Az Infoshow konferencián a villámáram-eloszlás témájában tartott előadás a villámáram eloszlásának vizsgálatára és az ennek alapján alkalmazandó túlfeszültség-védelmi megoldásokra fókuszált. Az előadást [15] Dr. Kovács Károly, a DEHN HUNGARY Kft. ügyvezetője tartotta, és bemutatta a túlfeszültség-védelem tervezési alapjait különböző épülettípusokra, például lakó-, iroda- és ipari épületekre. A fő cél az volt, hogy segítséget nyújtson a résztvevőknek a túlfeszültség-védelmi készülék kiválasztásában és telepítésében.

Az előadásban a különböző villám-lökőáramok hullámalakjait mutatták be (10/350 µs, 8/20 µs) és ezek összehasonlítását végezték el, mivel ezek az adatok alapvetően meghatározzák a megfelelő túlfeszültség-védelmi eszközök kiválasztását.

A villámcsapások különböző típusaiból eredő károk (pl. S1, S2, S3 kárforrás) szimulációját mutatták be. A bemutatott modellek szerint a kárforrások meghatározzák, hogy melyik villámvédelmi és túlfeszültség-védelmi intézkedések szükségesek az adott helyzetben, például a főelosztó és a csatlakozóvezetékek védelme érdekében.

Az előadásban különösen hangsúlyozták a villámáram levezetésének feltételezett eloszlását. Az MSZ EN 62305 szabvány alapján bemutatták az „50-50%” szabályt, amely a villámáram egyenletes elosztására szolgál, ám az előadás figyelmeztetett arra, hogy gyakran ettől eltérő eloszlási arányokat kell alkalmazni.

Az ipari és lakóépületek esetén bemutatták a megfelelő SPD (Surge Protection Device) típusokat és azok telepítési helyeit. Külön kiválasztási segédleteket is bemutattak a résztvevők számára, amelyek segítik a túlfeszültség-védelmi rendszerek optimális tervezését.

Az előadás során számítógépes szimulációk eredményeit is bemutatták, amelyek a villámáram időbeli eloszlását és a potenciálkülönbségek alakulását vizsgálták az épületek különböző pontjain.

## FELHASZNÁLT IRODALOM

[1] Magyar Mérnöki Kamara Kiadványsorozata, Elektrotechnikai és Épületvillamossági Tagozat: A nem norma szerinti villámvédelem egységes műszaki követelményrendszerének kialakítása és javaslat a teljes villámvédelmi szabályrendszer jövőbeli egységesítésére, FAP-2020/103-ELT, Budapest, Hungary, 2020.

[2] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról. Magyar Közlöny, Budapest, Hungary, 1996. [Online]. Available: https://njt.hu/jogszabaly/1996-31-00-00

[3] DEHN + SÖHNE GmbH + Co. KG, Lightning Protection Guide, 3rd updated ed. Neumarkt, Germany: DEHN + SÖHNE, 2014. https://www.dehn-international.com/sites/default/files/media/files/lpg-2015-e-complete.pdf

[4] EMTP

[5] S. M. Saleem and A. R. H. Hussein, “ATP-EMTP simulation of lightning protection system for multi-storey building,” J. Electr. Autom. Syst., vol. 4, no. 1, pp. 1–12, 2024. [Online]. Available: https://unec-jeas.com/articles/volume-4-no-1-2024/atp-emtp-simulation-of-lightning-protection-system-for-multi-storey-building

[6] M. H. Jassim and M. H. Naji, “Simulation and analysis of lightning strikes in electrical systems by MATLAB/Simulink and ATP/EMTP,” *Adv. Eng. Sci.*, vol. 3, no. 1, pp. 56–

66, 2023. [Online]. Available: https://advancedengineeringscience.com/article/pdf/2023/02-398.pdf

[7] B. Gradzki, "Analysis of lightning current distribution in the lightning protection system (LPS) with using numerical simulations," *Power Quality Blog*, Sep. 29, 2022. [Online]. Available: https://powerquality.blog/2022/09/29/analysis-of-lightning-current-distribution-in-the-lightning-protection-system-lps-with-using-numerical-simulations/

[8] Elektroinstallateur. (2013). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (I). Elektroinstallateur, XXI. évf., 4. sz., 28-33.

[9] Elektroinstallateur. (2013). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (II). Elektroinstallateur, XXI. évf., 5. sz., 30-34.

[10] Elektroinstallateur. (2013). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (III-IV). Elektroinstallateur, XXI. évf., 6-7. sz., 32-38.

[11] Elektroinstallateur. (2013). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (V). Elektroinstallateur, XXI. évf., 8-9. sz., 35-40.

[12] Elektroinstallateur. (2013). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (VI). Elektroinstallateur, XXI. évf., 10. sz., 30-34.

[13] Elektroinstallateur. (2014). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (VII). Elektroinstallateur, XXII. évf., 1-2. sz., 28-33.

[14] Elektroinstallateur. (2014). Villámáram-levezetők tervezési és beépítési szabályai – Kivitelezési szabályok (VIII). Elektroinstallateur, XXII. évf., 3. sz., 32-36.

[15] Dr. Kovács Károly (2023). Villámáram-eloszlás és túlfeszültség-védelem ipari létesítményekben. In: InfoShow Konferencia, Budapest, 2023. április 15-16., DEHN HUNGARY Kft., 45-52.

DOI: https://doi.org/10.12700/btsz.2025.7.3.113

# SAFETY CLASSIFICATION OF HYDROGEN TECHNOLOGIES: CONCEPT AND EMPIRICAL VALIDATION OF THE HISI MODEL

# HIDROGÉNTECHNOLÓGIÁK BIZTONSÁGI OSZTÁLYOZÁSA: A HISI-MODELL KONCEPCIÓJA ÉS EMPIRIKUS VALIDÁCIÓJA

SZÉN István[1] – BAKOSNÉ DIÓSZEGI Mónika[2] – RÁCZ Ervin[3]

**Abstract**

Hydrogen, a key energy carrier in the EU's green transition, is gaining an increasingly dominant role in modern energy systems. However, no unified, hydrogen-specific accident classification framework currently exists. We identified a research gap and found that existing industrial safety incident scales are unsuitable, without major compromises, for consequence-based and structured classification of hydrogen incidents. To address this, we developed the Hydrogen Incident Severity Indicator (HISI) scale. Its validity was confirmed through an empirical method by retrospectively classifying past incidents. HISI is objective, industry-independent, and interoperable, enabling the severity classification of hydrogen incidents and supporting consistent risk communication and regulatory harmonization

**Keywords**

hydrogen, industrial safety, industrial accident, malfunction, incident-scale

**Absztrakt**

A hidrogén, az EU által preferált zöldátmenet kulcsfontosságú energiahordozója, így egyre dominánsabban jelenik meg az energiarendszerekben. Azonban, jelenleg nem áll rendelkezésre egységes, hidrogénspecifikus, baleseti eseménybesorolási-rendszer. Ezzel kapcsolatban azonosítottunk egy kutatási rést, s megállapítottuk, hogy a meglévő iparbiztonsági eseményskálák, kompromisszumok nélkül nem alkalmasak a következményalapú és strukturált, hidrogénincidensek osztályozásra. Kutatásunk célja e hiány pótlása, ezért megalkottuk a Hydrogen Incident Severity Indicator (HISI) skálát. A HISI érvényességét empirikus módszerrel, korábban bekövetkezett események visszamenőleges besorolásával validáltuk. A HISI skála objektív, iparágfüggetlen és interoperábilis, képes a hidrogénesemények súlyossági osztályozására, valamint hozzájárul a kockázatok egységes kommunikációjához és a szabályozási folyamatok harmonizációjához.

**Kulcsszavak**

hidrogén, iparbiztonság, üzemi baleset, üzemzavar, incidens skála

[1]szen.istvan@kvk.uni-obuda.hu | ORCID: 0000-0002-1028-0005 | PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2]dioszegi.monika@bgk.uni-obuda.hu | ORCID: 0009-0000-3783-5691 | university associate professor, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai mérnöki Kar

[3]racz.ervin@kvk.uni-obuda.hu | ORCID: 0000-0002-7692-1397 | full professor, Obuda University, Kando Kalman Faculty of Electrical Engineering | egyetemi tanár, Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar

## BEVEZETÉS

A hidrogénalapú energiatechnológiák gyors fejlődése egyre jelentősebb szerepet kap a globális dekarbonizációs törekvésekben. A megújuló energiaforrások és a szektorintegráció révén megjelenő zöld- és kékhidrogén termelés területén tapasztalható előrelépések, valamint a hidrogén felhasználása az iparban, a mezőgazdaságban és a közlekedésben új típusú infrastruktúrák létrehozását teszi szükségessé. Tekintettel ezen folyamatokra, potenciálisan növekszik a hidrogén veszélyeivel kapcsolatos események gyakorisága és valószínűsége. A hidrogén, fizikai és kémiai sajátosságai, mint a rendkívül kis molekulatömeg, a nagy diffuzivitás, a széles gyulladási tartomány, valamint a láng szabad szemmel történő észlelésének nehézségei, egyedi biztonságtechnikai kihívásokat eredményeznek.

Az elmúlt évtized folyamán bekövetkezett hidrogénincidensek, valamint az ezekről készült eseményjelentések rámutattak arra, hogy hiányosságok vannak a gyorsan fejlődő és intenzíven terjedő, hidrogéntechnológia eseményeinek a dokumentálása terén. Az International Nuclear Event Scale (INES) [1] [2], a European Scale of Industrial Accidents (ESIA) [3] vagy az Analyse, Recherche et Information sur les Accidents (ARIA) [4] és a Hydrogen Incident and Accident Database (HIAD) [5], nem alkalmasak a hidrogénspecifikus események súlyosságának következetes, strukturált osztályozására, a következményalapú értékelésére és a súlyossági besorolására. A HIAD adatbázis, ugyan kifejezetten a hidrogéntechnológiához kapcsolódó eseményeket gyűjti és lehetőséget teremt az elemzésre is, ugyanakkor a HIAD egyik hiányossága, hogy nem rendelkezik strukturált súlyossági skálával. A közelmúltban bekövetkezett hidrogénrobbanások és balesetek, így például a 2019-es délkoreai Gangneung-i laborrobbanás, a 2019-es norvég Bærum község $H_2$ töltőállomásának robbanása vagy a 2019-es kaliforniai tartályszivárgás azt bizonyítják, hogy a meglévő rendszerek hiányosak a hidrogénre jellemző kockázatok szempontjából. A tanulás, szemléltetés és a tapasztalatok átadása nehézkes és akadozó. Meglátásunk szerint szükségessé vált egy új, hidrogénspecifikus súlyossági skála kidolgozása, amely alkalmas az események iparágfüggetlen összehasonlítására, objektív értékelésére és a kockázatkommunikáció támogatására. Kiemelten fontosnak tartjuk, hogy a HISI egy interoperábilis keretrendszer, így illeszthető más iparági vagy nemzetközi osztályozási rendszerekhez is, függetlenül azok technológiai hátterétől vagy iparági beágyazottságától. A fentiekből adódóan a HISI lehetővé teszi a hidrogénnel kapcsolatos balesetek objektív értékelését is, valamint használatával megvalósíthatunk egy egységes súlyossági besorolását, továbbá a HISI támogatásával integrálhatóvá tesszük az eredményeket és levont tapasztalatokat egy már meglévő biztonsági jelentési rendszerbe vagy egy auditálási és szabályozási keretbe.

## KUTATÁSI MÓDSZERTAN ÉS A VALIDÁCIÓS ELJÁRÁSOK

A szakirodalmi háttér feltárása során, a hidrogéntechnológiai események átfogó elemzésére törekedtünk. Kvalitatív elemzéseket végeztünk a hidrogénipari balesetekkel kapcsolatban, s ekkor tűn fel, hogy a különböző hidrogéntechnológia események nehezen vagy egyáltalán nem hasonlíthatók össze. A bevezető szakaszban említett adatbázisokkal kapcsolatban kerestünk releváns szakirodalmat a ScienceDirect és Scopus adatbázisban, valamint a Researchgate felületén. Az áttekintett szakirodalom alapján a következő megállapításokat fogalmazhatjuk meg:

- a jelenleg alkalmazott ipari eseményosztályozási rendszerek, legyenek általános ipari/nukleáris (pl. INES, ESIA, ARIA) vagy kifejezetten hidrogénre fókuszáló (pl. HIAD, HIRA) adatbázisok, egyaránt jelentős hiányosságokat mutatnak, amikor a hidrogénipari események sajátos kockázati dimenzióinak kezeléséről van szó.
- jellemző, a strukturált, kvantitatív és hidrogén-specifikus adatok hiánya
- hiányzik az egységes taxonómia és adatmező-struktúra
- jellemző az események aluljelentése, valamint a karbantartási, üzemeltetési és emberi tényezők nem megfelelő integrációja

**Hiányos, hidrogénspecifikus kockázati dimenziók**

A jelenleg használt hidrogénipari eseményosztályozási rendszerek jelentős lefedettségi hiányosságokkal küzdenek, amikor a hidrogén-specifikus kockázati dimenziók kezeléséről van szó.

- Sok modell nem foglalkozik kellő részletességgel az anyagok kompatibilitásával és ridegedési problémáival, pedig a hidrogén komoly ridegítő tényezőként lép fel a fémeknél, csökkentve a csövek vagy fémtartályok szerkezeti integritását és mechanikai ellenállóképességét.
- A karbantartási és üzemeltetési állapotok rendszeres ellenőrzésének hiánya miatt gyakran fordulnak elő szivárgások, tömítési és szelep-hibák, amelyek jelentősen növelik a balesetek kockázatát.

A vizsgált tanulmányok rámutatnak, hogy az emberi és menedzsment tényezők, mint például a nem megfelelő képzés, hibás üzemi protokollok vagy kommunikációs anomáliák, a jelenlegi keretrendszerekben alulreprezentáltak, pedig a legsúlyosabb események jelentős része ezen tényezőkre vezethetők vissza. További hiányosság, hogy a folyamatbiztonsági menedzsment elemei, mint például a kockázatcsökkentő intézkedések vagy a vészhelyzeti tervek sok esetben nem integráltak a meglévő rendszerekbe. A cseppfolyós hidrogén ($LH_2$) speciális veszélyeit csak kevéssé veszik figyelembe, holott ezek eltérő biztonsági megközelítést igényelnek. A hidrogénspecifikus incidensek összetettsége, mint például a gáz rendkívül gyors diffúziója, a láng észlelésének nehézsége vagy az alacsony gyulladási energia (0,017 mJ, levegőben), tovább növeli annak kockázatát, hogy a meglévő rendszerek nem tudják megfelelően modellezni és értékelni a valós veszélyt. A vizsgált módszerek, mint például a Failure Modes and Effects Safety Analysis (FMESA), a Management Oversight and Risk Tree (MORT), az Accidental Risk Assessment Methodology for Industries (ARAMIS) és a Hydrogen Component Reliability Database (HyCReD), általában korlátozott alkalmazási tartománnyal és technológiaspecifikus fókusszal rendelkeznek, és nem tesznek lehetővé átfogó, többdimenziós súlyossági osztályozást. A fentiek alapján megállapítottuk, hogy a szakirodalom a hidrogénre jellemző kockázati tényezők strukturáltabb, integráltabb és empirikusan validált feldolgozását igényli [6][7][8].

**Modellalkotás, alapkövetelmények**

Szakirodalomkutatásunk alapján megállapítottuk, hogy egy új, hidrogénspecifikus baleseti skálának strukturált, kvantitatív adatkeretre, egységes taxonómiára, hidrogénspecifikus kockázati dimenziók lefedésére és valós baleseti adatokon alapuló empirikus validációra kell épülnie, miközben kompatibilis marad fejlett elemző eszközökkel és rendszeresen frissített, nyílt adatbázissal biztosítja a naprakész kockázatértékelést [6][9][10].

### Validált és jelenleg használatban lévő osztályozási rendszerek hiányosságai

Ahogyan fent már említettük, a jelenlegi ipari eseményosztályozási rendszerek nem nyújtanak megfelelő keretet a hidrogéntechnológiákhoz kapcsolódó események súlyossági értékelésére.

- az INES kizárólag nukleáris eseményekre alkalmazható skála [1][2],
- az ESIA ugyan ipari balesetek kvantitatív értékelésére szolgál, de nem tartalmaz hidrogénspecifikus paramétereket [3],
- az ARIA egy iparibaleset-adatforrás és eseménytár, de önmagában nem alkalmas a hidrogénesemények szabványosított, többdimenziós súlyossági osztályozására,
- míg a HIAD ugyan hidrogén incidenseket gyűjt, de nem tartalmaz súlyossági besorolást és súlyossági skálát [5].

### Validációs eljárások

A vizsgált publikációk közös jellemzője, hogy a validációt, valós ipari események alapján végezték el, konkrét folyamatok feldolgozásával, elemzésével. Ez biztosította, hogy az osztályozási, előrejelző vagy kockázatelemző modellek ne csupán elméleti, hanem gyakorlati szempontból is relevánsak legyenek. Az így kapott modellek megbízható alapot szolgáltattak a szabványosításhoz, a kockázatcsökkentési stratégiák kialakításához és az új biztonsági protokollok kidolgozásához [6][7][9][10]. A most bemutatott modellünk validálását, mi is valós eseményekre alapoztuk, s a cikkben bemutatjuk a besorolás folyamatát és eredményeit majd a modellünkhez kapcsolódóan a validációs célok elérése érdekében elvégezzük a komplex konzisztencia analízist és az érzékenységvizsgálatot.

## A HISI-MODELL ALAPJAI

### A modell célja

A Hydrogen Incident Severity Indicatorral a célunk egy egységes, többdimenziós, strukturált súlyossági osztályozási rendszer megalkotása, hidrogéntechnológiai események objektív értékelésének a támogatásához. A HISI további célja, hogy lehetővé tegye az események következetes és összehasonlítható értékelését, elősegítve ezzel a biztonsági kommunikációt, a műszaki- és jogi szabályozást, valamint a kollektív kockázatkezelési stratégiák fejlesztését.

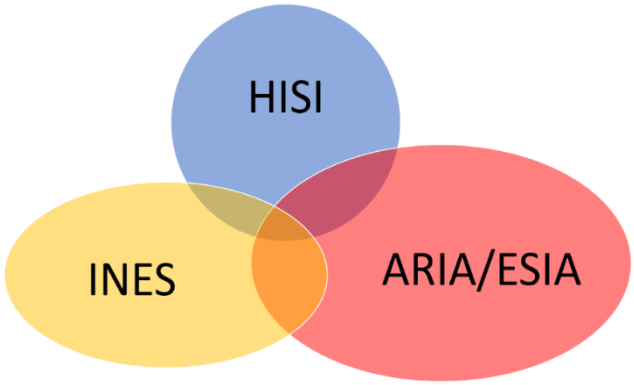
### A modell alkalmazási köre

A modell közvetlenül alkalmazható a már meglévő, valamint a jövőben létesülő hidrogéntechnológiai infrastruktúrára is. A kapcsolódó technológiai területek rendkívül dinamikusan fejlődnek és bővülnek, így az alkalmazási kör meghatározása jelenleg nem tekinthető véglegesnek, hiszen az alkalmazási területek sokrétűek. A hidrogén az elmúlt évtizedben megjelent az iparban, az energetikában, a mezőgazdaságban, a közlekedés számos területén és az innovációk révén folyamatosan bővül a felhasználási területe. A tudományos szempontok kielégítése érdekében, mi mégis definiáltunk néhány alkalmazási területet, ugyanakkor jelenleg nem tekinthető teljesnek és lezártnak a felsorolás, az alkalmazási kör így nyitott minden jövőbeni, hidrogénhez kapcsolódó fejlesztési irány előtt. Definiált alkalmazási területek:

- ipari, fosszilis bázisú hidrogénelőállítás (gőzreformálás, parciális oxidáció, elgázosítás, pirolízis),
- karbonszegény, úgynevezett zöld- és kékhidrogén előállítás (alkáli- és PEM elektrolízis),
- természetes, un. fehérhidrogén források és kitermelési infrastruktúra
- hidrogéntárolás (kis- és nagynyomású gáz valamint kriogén rendszerek),
- hidrogénszállítás (csővezetéki, kötegelt tartályok, tartálykocsik),
- hidrogénfelhasználás
    - közvetlen égetéses eljárások (robbanómotor, kazán, gázturbina),
    - elektrokémiai konverzió (tüzelőanyagcellák),
    - vegyipari felhasználás (ammóniagyártás, kőolajfinomítás, metanolgyártás, szintetikus üzemanyaggyártás),
    - ipari folyamatok (acélgyártás, üveg- és cementipar),
- kísérleti, laboratóriumi hidrogéntechnológiák (előállítás, tárolás, felhasználás, oktatás, kutatás-fejlesztés-innováció)

**A HISI pozícionálása a nemzetközi rendszerekbe**

A különböző iparágakban alkalmazott baleseti, súlyossági skálák eltérő célokra és jogi keretekre épülnek, ezért a hidrogénnel kapcsolatos események értékelése során a skálák alkalmazhatósága elsősorban az adott létesítmény típusától és a szabályozási környezettől függ. Nukleáris létesítményekben bekövetkező balesetek esetén, amennyiben az esemény a nukleáris biztonságot érinti, az INES az egyetlen hivatalosan elfogadott nemzetközi értékelési rendszer, amely kötelezően alkalmazandó a hivatalos jelentésekben. Ilyen esetekben a HISI skála csak kiegészítő szerepet tölthet be, lehetővé téve a hidrogénhez kapcsolódó incidens súlyosságának részletes és strukturált elemzését, amely az INES skálán belül gyakran rejtve marad.




*1. ábra: A HISI komplementer szerepe és integrálhatósága más rendszerekhez, saját szerkesztés*

A 2011-es fukusimai atomerőmű-baleset erre szemléletes példa, az INES skála szerinti 7-es fokozatú besorolás a teljes nukleáris katasztrófa súlyosságát tükrözte, ugyanakkor a reaktorépületekben történt hidrogénrobbanások önálló kockázati jellemzői nem kaptak külön kvantitatív besorolást. A HISI ilyen esetben kiegészítő információt adhatott volna a

hidrogénrobbanások fizikai sajátosságairól, következményeiről és azok biztonságtechnikai súlyosságáról, ezzel támogatva a baleset elemzését és a jövőbeni megelőző intézkedések kialakítását. Nem nukleáris, ipari létesítmények esetében, például a veszélyes anyagokkal foglalkozó üzemeknél, az ARIA vagy az ESIA keretrendszerek biztosítanak hivatalos baleseti adatgyűjtést és súlyossági értékelést, ezen rendszerekbe a HISI egy hidrogénspecifikus modulként értelmezhető, lehetővé téve, hogy a hidrogénincidensek összehasonlíthatóan, iparágfüggetlenül és kvantitatív módon kerüljenek értékelésre. Így a HISI nem váltja ki a meglévő skálákat, hanem komplementer eszközként működik közre (1. ábra), amely növeli a baleseti értékelések információtartalmát, javítja az interdiszciplináris kommunikációt és támogatja a szabályozási folyamatok harmonizációját.

## A HISI-MODELL KONCEPCIONÁLIS KIDOLGOZÁSA ÉS DIMENZIÓI

A HISI-skála alapjait a szakirodalmi forrásokra, a nyílt hozzáférésű adatbázisokra épített értékelési dimenziókkal kívánjuk biztosítani. Amint a bevezetőben kifejtettük, szakirodalmi áttekintésünk során jelentős kutatási rést azonosítottunk: a meglévő eseményskálák és adatbázisok nem tartalmaznak hidrogénspecifikus jellemzőket. Ennek megfelelően elsődleges célunk e sajátos kockázati profilhoz illeszkedő jellemzők kidolgozása és integrálása. Második fő célkitűzésként arra törekedtünk, hogy az általunk megalkotott rendszer illeszkedjen a már létező értékelési keretrendszerekhez, eseményskálákhoz, sőt kiegészítő funkciót és többlettartalmat biztosítson a HISI, ezáltal jogi, műszaki és biztonságtechnika szempontból is harmonizációs funkciót láthat el a hazai, európai és nemzetközi iparbiztonsági gyakorlatban.

Kiemelt jelentőségű az emberi hatások értékelése a nemzetközi szabványokban és biztonsági ajánlásokban. Az Egyesült Államokban az OSHA-PSM (Occupational Safety and Health Administration - Process Safety Management) kötelező előírásai és az API RP 754 (American Petroleum Institute Recommended Practice) ajánlásai a súlyos személyi sérüléseket és a haláleseteket, egyértelműen a legsúlyosabb kategóriába sorolja [11][12]. Az Európai Unióban a Seveso III irányelv és az eMARS (Major Accident Reporting System) adatbázis kötelezővé teszi a halálos és súlyos sérüléssel járó balesetek jelentését [13][14][15] [16][17]. A Center for Chemical Process Safety (CCPS) metodikái külön kezelik a robbanás, tűz és mérgezés okozta sérüléseket [18], az ARIA (Analyse, Recherche et Information sur les Accidents) pedig egy szisztematikus, előre definiált rendszert alkalmaz az emberi sérülések és halálesetek statisztikai értékelésére [4]. Ezen alapelvek mentén alkottuk meg azt a koncepciót, hogy a HISI-skála önálló dimenzióként kezelje személyi sérüléseket és a fokozatosság elvét betartva, egyre súlyosabb osztályozást valósítsunk meg, a súlyosbodó személyi sérülések bekövetkezése során, biztosítva a nemzetközi kompatibilitást és az objektív összehasonlíthatóságot.

A HISI, környezeti hatások dimenziója a Seveso III irányelv környezeti kritériumaira (talaj-, víz- és levegőszennyezés) épül, de kiterjeszti azokat a hidrogénspecifikus kibocsátásokra, például a vészhelyzet során a légkörbe jutó hidrogén mennyiségére és a kritikus környezeti receptorok (védett területek, ivóvízbázisok, lakott területek) érintettségére.

A fizikai károk értékelése összhangban van az API RP 754 negyedik szintű (Significant Property Damage) mutatójával, valamint az ARIA és a Chemical Safety Board (CSB) gyakorlatával, amelyek pénzbeli küszöbértékeket és robbanásienergia-értékelést (TNT-ekvivalencia, túlnyomási zónák) alkalmaznak [20][21].

A műszaki meghibásodások dimenzió a CCPS és az OSHA-PSM által meghatározott kritikus biztonsági funkciók működésének értékelésére épül, kiegészítve az ARIA és adatbázisokban szereplő eseménykezelési, un. sikerességi mutatókkal.

E négy dimenzió együttesen lefedi a hidrogénes balesetek minden releváns következményét és okát, lehetővé téve, hogy a HISI-skála egyszerre működjön technikai, jogi és kommunikációs eszközként, támogatva a biztonsági események objektív, összehasonlítható és nemzetközileg is összehangolt besorolását. A dimenziók kombinált értékelése biztosítja, hogy a HISI skála a baleset komplex következményprofilját mutathassa meg.


*1. ábra: A HISI-skála dimenziói, saját szerkesztés*

### A HISI-skála szintjeinek formális definíciói és a logikai alapelvek

A skála hét szintet tartalmaz, melyek fokozatosan növekvő súlyosságot tükröznek. A HISI-1 a legkevésbé súlyos esemény. A szintek meghatározása a dimenziók (2. ábra) együttes értékelésével történik. A skála kialakítása során a következő alapelveket vettük figyelembe:

- logaritmikus hatásszemlélet: adaptálva az INES skála ezen tulajdonságát, a magasabb szintek exponenciálisan növekvő következményeket reprezentálnak,
- ordinalitás: a szintek egyértelmű sorrendiséget követnek, kvalitatív és kvantitatív hatás szerint,
- pontosság: minden szintnél jól körülírt határérték található a dimenziók mentén,
- interoperabilitás: a skálát úgy terveztük, hogy az alkalmazható legyen a fent definiált alkalmazási körökben, sőt a meglévő skáláknak komplementer eszköze lehessen.

## A HISI-SKÁLA PONTOZÁSI RENDSZERE

A HISI-skála egy hétszintű, négydimenziós pontozásos rendszert alkalmazó skála. Minden dimenzióhoz egy 0–5-ig terjedő pontszám tartozik, ahol a magasabb pontszám súlyosabb következményeket jelez (3. ábra). Az egyes dimenziókra adott pontszámok összege

adja a HISI-összpontszámot, amely alapján, a szintdefiníciós táblázat (4. ábra) felhasználásával meghatározható a HISI súlyossági kategória. A rendszer célja, hogy a kvalitatív leírásokat és a kvantitatív küszöbértékeket ötvözve egy objektív, reprodukálható és összehasonlítható besorolást biztosítson a hidrogéntechnológiai eseményekre, így a HISI-skála egy eddig fennálló hiányosságot pótol.

| Dimenzió | 0 pont | 1 pont | 2 pont | 3 pont | 4 pont | 5 pont |
|---|---|---|---|---|---|---|
| **Emberi hatás** | Nincs sérülés | ≤1 könnyű sérült | ≥ 2 könnyű és/vagy 1 súlyos sérült | ≥ 2 súlyos sérült és/vagy 1 haláleset | 2–3 haláleset | >3 haláleset |
| **Környezeti hatás** *(elsődleges: légkörbe jutott $H_2$ tömeg; másodlagos: receptor érintettsége)* | <0,5–1,5 kg; nincs receptor | 1,5–5 kg; nincs receptor érintettség | 5–200 kg; nincs tartós égés; a hatás lokális és rövid idejű, receptort csak részben érintett | 200–500 kg; tartós égés, a hidrogénen kívül más éghető anyag is tartósan égett, receptor biztosan érintett | 500-1000 kg; tartós légköri/ökológiai hatás, lokális és regionális hatások, receptor biztosan érintett | >1000 kg; Tartós, regionális légköri/ökológiai hatás receptor biztosan érintett |
| **Fizikai kár** *(elsődleges: robbanás és/vagy tűz; másodlagos: kár mértéke)* | Nincs kár, nincs tűz, nincs robbanás, kár: <10k € | Kis tűz, kézi oltóval oltva; kár: 10k–100k € | Kis tűz, kis kiterjedés, mérsékelt kár: 100k–1 M€ | Komplex tűz, több oltási pont jelentős kár: >1 M€ | Robbanás, jelentős kár: >1 M€ | Robbanás, súlyos károk, az eszköz és/vagy a környezet már nem javítható, kár: >10 M€ |
| **Műszaki meghibásodás** *(elsődleges: emberi-másodlagos: műszaki tényező)* | Emberi mulasztás hiba/minden biztonsági rendszer jól működött | Marginális emberi hiba és részleges műszaki hiba, gyors beavatkozás | Emberi hiba/részleges műszaki hiba, az esemény lokális tűzzel vagy robbanással járt | Jelentős emberi hiba/kritikus hiba egy alrendszerben, késleltetett beavatkozás, kiterjedt tűz, robbanás | Több alrendszer hibája, nincs lehetőség megelőző beavatkozásra | Felelőtlen és jelentős emberi hiba és/vagy kritikus rendszerhiba (több fontos alrendszer hibája, hiányossága) |

*2. ábra: Dimenziók - hatások és pontok, saját szerkesztés*

| Szint | Összpontszám | Szöveges értékelés |
|---|---|---|
| HISI-7 | 19-20 | nagyon súlyos baleset |
| HISI-6 | 16-18 | súlyos baleset |
| HISI-5 | 13-15 | baleset – nagy kiterjedés |
| HISI-4 | 10-12 | baleset – kis kiterjedés |
| HISI-3 | 7-9 | súlyos üzemzavar – folyamatok ellenőrzése |
| HISI-2 | 4-6 | üzemzavar – fokozott figyelem + felülvizsgálatok |
| HISI-1 | 0-3 | eltérés – fokozott figyelem |

*3. ábra: Szintdefiníciós táblázat, saját szerkesztés*

Az események elemzése során, két eredményre számítunk. Az egyik eredmény a HISI-szint melyhez kapcsolódik még egy nagyon egyértelmű és szándékosan rövid szöveges értékelés is. A másik eredmény egy radardiagram, ami szemléletesen mutatja a bekövetkezett esemény jellegét. Mi ezt a diagrammot, az esemény következményprofiljának tekintjük és a HISI-Quadrilemma névvel azonosítjuk. A quadtrilemma egy szemléltető és kommunikációs eszköznek, a gyors tájékoztatás és összehasonlítás érdekében.

## EMPIRIKUS VALIDÁCIÓ

Egy új biztonsági, súlyossági skála - mint amilyen a Hydrogen Incident Severity Indicator - tudományos megalapozottsága és ipari alkalmazhatósága csak akkor biztosítható, ha annak elméleti felépítését és pontozási logikáját valós események adatain végzett empirikus validációval támasztjuk alá. Az empirikus validáció célja egyrészt a skála gyakorlati működésének ellenőrzése, másrészt a következetesség értékelése.

### Alkalmazott adatforrások és esettanulmányok

A validáció első lépéseként gondosan kiválasztott esettanulmányokat soroltunk be a HISI hétfokozatú skálájára. Az empirikus validációt több, eltérő jellegű és megbízható adatforrásra alapoztuk. Elsődleges kiindulópontként a HIAD szolgált, amelyet kiegészítettünk az ESIA és ARIA adatbázisok adataival, valamint számos nyílt forrásból és az Elsevier által gondozott tudományos adatbázisokból származó információval. A publikációhoz szándékosan olyan eseményeket választottunk, amelyek egyrészt széles körben és szabadon hozzáférhetők, másrészt jól reprezentálják a kimenetek közötti jelentős eltéréseket. Fontos kiválasztási szempont volt továbbá, hogy a vizsgálatok státusza lezárt legyen, vagyis a körülményeket a vizsgáló hatóságok teljes körűen feltárták, és az eseményekkel kapcsolatban új információ már nem várható. A kiválasztott esetek különböző országokból és létesítménytípusokból származnak, ami biztosítja a módszertani sokféleséget, és egyben növeli a modell robusztusságát. A vizsgálati példánkban szereplő három esemény:

- Kjørbo (2019.06.10.), Norvégia-Sandvika: töltőállomás-robbanás
- Santa Clara (2019.06.01.), USA: tartálykocsi robbanás és tűz
- Gangneung (2019.05.23.), Dél-Korea, laborrobbanás

### Rövid esettanulmány-összefoglalók:

**Kjørbo(Sandvika):** Nyílt téren, egy gyors diszperziós hatású, viszonylag rövid ideig tartó tűzeset történt egy hidrogén-töltőállomáson, A beszámolók szerint két személy könnyebb sérülést szenvedett, azonban mi ezt nem vesszük figyelembe mert megállapítható, hogy a sérülések nem közvetlen hatások voltak, hanem un.: másodlagos balesetek, autó légzsákjának a nyitása okozott könnyebb sérülést a 2 személynél. Az esemény mérsékelt, kis helyre koncentrálódó infrastrukturális károkat okozott, a nagynyomású hidrogéntároló tartály ugyan gyakorlatilag megsemmisült, de a tűz nem terjedt át sem a töltőállomás további részére sem a civil lakosság tulajdonára. A tűz 500 méteres körzetében lakott terület is található. A hivatalos vizsgálat megállapította, hogy a balesetet szerelési, telepítési hiba okozta (nem kellő nyomatékkal meghúzott csatlakozó csavarok a nagynyomású hidrogéntartályon). A hiba következménye szivárgás lett, de a vizsgálat során feltárták, hogy a tartály nyomásérzékelője nem működött megfelelően. A jelentések szerint a szivárgás huzamosabb ideig fennállhatott, s a levegő–hidrogén elegy meggyulladásához vezetett. Az eseményt követően az üzemeltető, a NEL Hydrogen, minden norvégiai és több európai állomását ideiglenesen bezárta, a szereléseket felülvizsgálta, és a szerelési folyamatra, valamint annak ellenőrzésére új, szigorított módszert vezetett be. [22][23].

**Santa Clara:** egy moduláris hidrogénszállító trailer töltése közben szivárgást észleltek a gépkocsi kezelői. A gépkocsikezelők, annak ellenére, hogy nem volt engedélyük ilyen tevékenységre, megpróbáltak javítani, cserélni a tömítést, de a biztonsági előírásokat nem tartották be (LockOut/TagOut), majd mindezt félreérthető kommunikációval tetézték,

amit a kevésbé tapasztalt személy nem jól értett és rossz működtetőgombot nyomott meg, így a hidrogén tömegáram megindult a szabadba, ahol a levegővel keveredve nagy erejű deflagrációs robbanást eredményezett. A folyamat során ezt követően kialakult egy sugárláng, s a tűz átterjedt a szomszédos, parkoló dízel üzemű teherautókra. A riportokban az is olvasható, hogy a kb. 40m-re lévő épület ablakai kitörtek a lökéshullám következtében. Személyi sérülés nem történt (fülzúgás és vállfájdalom volt, de a kezelők megmenekültek enyhébb sérülések nélkül). A károk: 4 teherautó és a szállítmányok, valamint 250 kg hidrogén szabadult ki,égett el. A cég elrendelte a biztonsági tréninget és felülvizsgálták a kommunikációs utasításokat és a munkafolyamatokat [24][25].

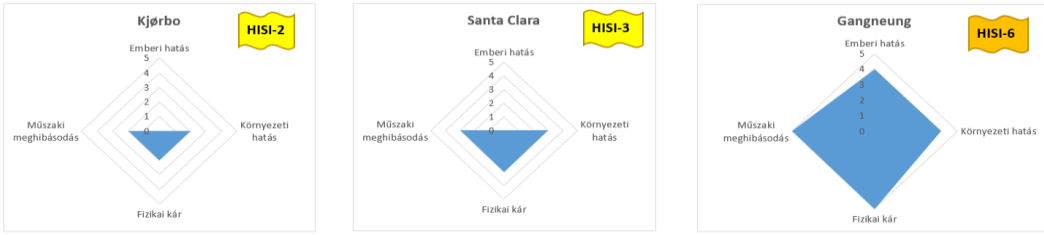
**Gangneung:** egy kísérleti laboratóriumban nagy erejű robbanás történt. A robbanást kiváltó oknak, egy elektrolizáló-cella membránjának a meghibásodását jelölték meg. A kezelők, a hibát nem észlelték időben, mert nem voltak beépített mérőműszerek és nem voltak kidolgozva erre az esetre ellenőrzési folyamatok. A sérült membrán nem választotta el tökéletesen a hidrogént és az oxigént, így a hidrogénáramba oxigén is keveredett, ami egy 40 $m^3$-es, 10 bar-os hidrogéntartályba halmozódott fel. A tartály tartalmát nem monitoringozták, így kialakulhatott a végzetes oxigén-hidrogén keverék, ami gyújtóforrással találkozva detonációt váltott ki. A számítások szerint a robbanás ereje, kb. 50kg TNT-egyenértéknek felelt meg, s a tartály valamint környezetének megsemmisülését okozta, valamint a lökéshullámot még 100m-el távolabb is érezni lehetett, ahol ablakok törtek ki. Sajnálatos módon két ember életét vesztette és további hat személy, sérüléseket szenvedett [26][27].


*4. ábra: Helyszíni fotók, sorrendben balról jobbra: Kjørbo [28], Santa Clara [29], Gangneung [30]*

## Esettanulmányok besorolása a HISI-skála alapján

A Kjørbo és Santa Clara esetén ugyan előfordultak kisebb sérülések, ezek azonban másodlagos vagy alig értékelhető sérülések voltak. A környezeti károk mindhárom esetben jelentősek voltak, Gangneung esetén a detonációs hatás különösen erőteljesen érvényesült. A részletes pontszámok, a súlyossági besorolások, valamint a HISI-quadrilemmák a 6. ábrán láthatók.

| Eset | Emberi hatás | Környezeti hatás | Fizikai kár | Műszaki meghibásodás | Összpontszám | HISI | Szöveges értékelés |
|---|---|---|---|---|---|---|---|
| **Kjørbo** | 0 | 2 | 2 | 2 | 6 | HISI-2 | Üzemzavar – fokozott figyelem + felülvizsgálatok |
| **Santa Clara** | 0 | 3 | 3 | 3 | 9 | HISI-3 | Súlyos üzemzavar – folyamatok ellenőrzése |
| **Gangneung** | 4 | 4 | 5 | 5 | 18 | HISI-6 | Súlyos baleset |




*5. ábra: Az esettanulmányok besorolása a HISI-skálára és a kapcsolódó quadrilemmák, saját szerkesztés*

A táblázatban látható pontszámok és szintek alapján a vizsgált esetek egyértelműen eltérő kockázati kategóriákba sorolhatók, ami igazolja a skála diszkriminációs képességét.

A mellékelt quadrilemma diagramoknak külön erőssége, hogy a négy dimenzió vizuálisan is összevethetővé válik, és a szintek azonnal értelmezhetők mind szakmai, mind kommunikációs szempontból. A központból kiinduló tengelyek hossza egyértelműen mutatja a domináns kockázati tényezőket, a feltüntetett HISI-szint pedig gyors tájékozódást biztosít a döntéshozók és a nyilvánosság számára is. Látható az is hogy az első két eset hasonló eseményprofillal rendelkezik, csak Kjørbon a tűz inkább maradt lokális jellegű, és mérsékelt károkat okozott, s ennek a következménye, hogy kedvezőbb az esemény besorolása, mint a Santa Clara esetben. A profilból és a HISI-skálából is látszik, hogy a laborrobbanás egy jelentősen kiterjedtebb és katasztrofális balesetnek minősíthető. Ez a vizualizációs forma nemcsak a technikai elemzést segíti, hanem a kockázatkommunikáció terén is új és hatékony eszköz lehet a hidrogénipari incidensek területén, hiszen egyetlen pillantással átláthatóvá teszi az esemény profilját és súlyosságát.

**Konzisztenciaanalízis és érzékenységvizsgálat célja**

A HISI-skála validálása több, egymást kiegészítő módszerrel is támogatható, melyek célja a modell megbízhatóságának, iparágfüggetlen alkalmazhatóságának igazolása. A konzisztenciavizsgálat a skála belső logikáját ellenőrzi, vagyis azt, hogy hasonló nagyságrendű és következményű események azonos kategóriába kerülnek-e, és hogy a pontozási rendszer belső ellentmondásoktól mentes-e?

Az érzékenységvizsgálat kvantitatívan teszteli, hogy kis bemeneti változások (például egy pontnyi növekedés a környezeti hatásban vagy egy haláleset megjelenése) okoz-e besorolási szintváltást, ezáltal mérve a skála finom-különbségekre adott reakcióját. E módszerek kombinációja biztosítja, hogy a HISI-modell robusztus, transzparens és döntéstámogatásra alkalmas maradjon különböző ipari környezetben.

**A konzisztenciavizsgálat - kvalitatív alapokon**

- A pontrendszer 0-5 közötti pontjai, a pontok jelentése világos definíciós különbségekkel bír.
- A mintaesetek kvalitatív leírása és a skála pontjai jól illeszkednek.
- Mindhárom incidensnél az egyedi dimenziókhoz köthető pontszámok és az összpontszám, valamint az értékelési táblázat belső konzisztenciát tükröz.
- A fotók (6. ábra) és a hivatkozott publikációk alapján a HISI-értékek reális közelítést adnak.
- A HISI-quadrilemmák (6. ábra) vizuális szempontból jól tükrözik az eseteket, az eseményprofil és a HISI-érték együttes megjelenése nagyon gyors és hatékony eseménykommunikációt tesznek lehetővé.

**Konzisztenciavizsgálat - Cronbach-α, kvantitatív módszerrel**

A Cronbach-alfa a belső konzisztencia mérőszáma és azt fejezi ki, hogy a skálát alkotó tételek (jelen esetben a HISI-skála dimenziókra adott pontszámok) mennyire mérnek egy közös, mögöttes konstruktumot. A közös konstruktum az a „rejtett változó”, amire a dimenziók együttesen utalnak, így a mi esetünkben ez a baleseti súlyosság. A módszer egyik megkötése, hogy nagyobb esetszámra pontosabb eredményeket ad [31]. A cikk terjedelmi

korlátai miatt mi most megmaradunk a három, eddig ismertetett esetnél, vállalva, hogy nem kapunk ideális eredményt.

| Eset | Emberi hatás | Környezeti hatás | Fizikai kár | Műszaki meghibásodás |
|---|---|---|---|---|
| Kjørbo | 0 | 2 | 2 | 2 |
| Santa Clara | 0 | 3 | 3 | 3 |
| Gangneung | 4 | 4 | 5 | 5 |

*6. ábra: A vizsgált esetek - kiindulási állapot a konzisztencia vizsgálathoz, saját szerkesztés*

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_i^2}{\sigma_{total}^2}\right)$$

*ahol*:
$k - a\ dimenziók\ száma$
$\sigma_i^2 - az\ egyes\ dimenziók\ varianciája$
$\sigma_{total}^2 - az\ összpontszám\ varianciája$

Események összpontszáma:

- Kjærbo: 0+2+2+2 = 6,0
- Santa Clara: 0+3+3+3 = 9,0
- Gangneung: 4+4+5+5 = 18

Dimenziók varianciája:

- Emberi hatás: (0, 0, 4): átlag: 1,33 variancia: 5,33
- Környezeti hatás: (2, 3, 4): átlag: 3,00 variancia: 1,00
- Fizikai kár (2, 3, 5): átlag: 3,33 variancia: 2,33
- Műszaki meghib. (2, 3, 5): átlag: 3,33 variancia: 2,33

A dimenziók varianciájának összege: 5,33 + 1 + 2,33 + 2,33 = 10,99 ~ 11

Összesített pontsz. (6, 9, 18): átlag: 11, variancia: 39

A számítás:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k}\sigma_i^2}{\sigma_{total}^2}\right) = \frac{4}{3}\left(1 - \frac{11}{39}\right) = 1{,}333 \times (1 - 0{,}282) = 1{,}333 \times 0{,}718 = 0{,}957$$

A kapott Cronbach-α eredmény: 0,957, a Cronbach-alfa elméleti tartománya 0 és 1 között van, ahol az 1 érték a maximális belső konzisztenciát jelenti a skálán szereplő tételek között. Ha az érték 0,5 alatt van, akkor a belső konzisztencia nem fogadható el. A gyakorlatban 0,75-től elfogadhatónak tekintjük a konzisztencia értékét, 0,9 felett pedig kiváló. A 0,957-es érték egyértelműen mutatja már a három mintára is a rendszer belső konzisztenciája kiváló.

**Érzékenységvizsgálat**

Az érzékenységvizsgálat célja, hogy feltárja, a vizsgált modell kimenete mennyire változik a bemeneti paraméterek kismértékű módosítására. Az ipari kockázatelemzésben és a HISI-hez hasonló skálarendszerekben ez különösen fontos, mert segítségével meghatározható, hogy a skála mennyire érzékeny egy-egy dimenzió pontszámának változására. Az érzékenységvizsgálat során azonosíthatók a kritikus tényezők, amelyek a legnagyobb hatást

gyakorolják a végső besorolásra, és ez alapot ad a döntéshozatal és a biztonsági intézkedések optimalizálásához.

A One-at-a-Time (OAT) módszer az egyik legegyszerűbb és legszélesebb körben használt érzékenységvizsgálati technika. Lényege, hogy a modell bemeneti paramétereit egyenként változtatjuk meg egy előre meghatározott lépésközzel, miközben a többi változó értékét rögzítjük. Így megfigyelhető, hogy az adott bemenet módosítása milyen mértékben befolyásolja a kimenetet. Az OAT előnye a könnyű implementáció és az eredmények egyértelmű értelmezhetősége, hátránya viszont, hogy nem veszi figyelembe a paraméterek közötti kölcsönhatásokat. Tekintettel, hogy a módszer ezen hátrányával tisztában voltunk, ezért végeztük el megelőző validációs módszerként a konzisztencia vizsgálatot. Az OAT-módszert számos ipari, közgazdasági, orvosi és mérnöki elemzésben alkalmazzák, például Saltelli és munkatársai összefoglaló tanulmányában is részletesen bemutatják alkalmazását [32] [33]. A szintdefiníciós táblázatot és a dimenziókhoz kacsolódó pontozási rendszert úgy alakítottuk ki, hogy a HISI-modell optimálisan, mérsékelt érzékenységgel rendelkezzen. A túlzott reakciót és a lomha viselkedést is el szerettük volna kerülni, így a definíciós táblában látható, hogy van egy stabil érték az adott szint középső értéke, viszont a határértékek közelében érzékeny a rendszer.

- Kjørbo (0, 2, 2, 2 → összesen 6 pont, HISI-2) – stabil állapotban
  +1 pont bármely dimenzióban → 7 pont, HISI-3
  –1 pont bármely dimenzióban → 5 pont, HISI-2 marad
- Santa Clara (0, 3, 3, 3 → összesen 9 pont, HISI-3) – stabil állapotban
  +1 pont bármely dimenzióban → 10 pont, HISI-4
  –1 pont bármely dimenzióban → 8 pont, HISI-3 marad
- Gangneung (4, 4, 5, 5 → összesen 18 pont, HISI-6) – stabil állapotban
  +1 pont bármely dimenzióban → 19 pont, HISI-7
  –1 pont bármely dimenzióban → 17 pont, HISI-6 marad

A validációs tapasztalatok megerősítik, hogy a HISI skála strukturált logikája alkalmas iparágfüggetlen eseményosztályozásra, és érzékenyen reagál a súlyossági tényezők kombinációjára.

## ÖSSZEFOGLALÁS

A kutatásunk célja a Hydrogen Incident Severity Indicator (HISI) skála kidolgozása volt, amely hidrogéntechnológiai események többdimenziós, súlyossági osztályozását teszi lehetővé. A modell felépítését és működését, valamint eredményeit bemutattuk.

A validációs folyamat során előbb esettanulmányok és szakértői elemzések kerültek felhasználásra, melyeket besoroltunk, majd a kapott eredmények lehetővétették, hogy a validációs folyamatot konzisztenciaanalízissel és érzékenységelemzéssel folytassuk.

Tudományos módszerekkel igazoltuk a konzisztenciáját, érzékenységét és iparágfüggetlen alkalmazhatóságát. A HISI modell túlmutat az egyszerű technikai osztályozáson: lehetőséget ad a kockázati kommunikáció, szabályozás, oktatás és biztonsági auditálás területén is. A HISI-modell hozzájárulhat ahhoz, hogy a hidrogéngazdaság fejlődése ne csak fenntartható, hanem biztonságos is legyen – megelőzve ezzel azokat a kockázatokat, amelyek az új technológiák gyors bevezetésével járnak.

A kutatás jövőképe

- A rendszer finomítása és egy nagy adatbázis létrehozása 50-100 minősített esettanulmány feldolgozása, ami alapján a HISI-skála paraméterei finomíthatók.
- Tervezzük, hogy elkészítjük a skála webes, és táblagépes változatát, annak érdekében, hogy a minősítés távolról, felmérési helyekről is elvégezhető legyen.
- Bízunk benne, hogy a további minősítések, olyan mértékben fogják növelni a tapasztalatunk, ami a további skálafejlesztések folyamatába előnyösen hasznosíthatók.

## FELHASZNÁLT IRODALOM

[1] International Atomic Energy Agency (IAEA), "INES – The International Nuclear and Radiological Event Scale User's Manual," IAEA, Vienna, 2013.
[2] OECD/NEA, "The International Nuclear and Radiological Event Scale (INES) – A Guide for Communicators," OECD Publishing, Paris, 2008.
[3] European Commission, "ESIA – The European Scale of Industrial Accidents: Technical Description," JRC, Seville, 2010.
[4] French Ministry for the Ecological Transition, "ARIA – Analysis, Research and Information on Accidents Database," Ministère de la Transition écologique, [Online]. https://www.aria.developpement-durable.gouv.fr [megtekintve: 2024. október 12.]
[5] M. C. Galassi, E. Papanikolaou, D. Baraldi, E. Funnemark, E. Håland, A. Engebø, G. P. Haugom, T. Jordan, and A. V. Tchouvelev, "HIAD – hydrogen incident and accident database," Int. J. Hydrogen Energy, vol. 37, no. 22, pp. 17351–17357, Nov. 2012.
[6] A. Campari, E. Stefana, D. Ferrazzano, and N. Paltrinieri, "Analyzing Hydrogen-Related Undesired Events: A Systematic Database for Safety Assessment," in Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023), 2023.
[7] A. Khanal, N. Chaudhary, B. Pandey, and B. S. Thapa, "Review of Hydrogen-Related Accidents: Root Causes, Mitigation Strategies, and Recommendations for Secure Utilization," IOP Conference Series: Earth and Environmental Science, vol. 1254, no. 1, p. 012021, 2024.
[8] C. Correa-Jullian and K. Groth, "Data Requirements for Improving the Quantitative Risk Assessment of Liquid Hydrogen Storage Systems," International Journal of Hydrogen Energy, vol. 46, no. 75, pp. 37349–37361, 2021.
[9] J. Wen, M. Maroño, P. Moretto, E. Reinecke, P. Sathiah, E. Studer, és E. Vyazmina, "Statistics, Lessons Learnt and Recommendations from Analysis of HIAD 2.0 Database," 2021.
[10] J. Wen, M. Maroño, P. Moretto, E. Reinecke, P. Sathiah, E. Studer, E. Vyazmina, és D. Melideo, "Statistics, Lessons Learned and Recommendations from Analysis of HIAD 2.0 Database," International Journal of Hydrogen Energy, 2022.
[11] U.S. Occupational Safety and Health Administration, "Process Safety Management" [Online]. Available: https://www.osha.gov/process-safety-management. [megtekintve: 2024. október 15].
[12] American Petroleum Institute, "Recommended Practice 754 Fact Sheet: Process Safety Indicators for the Refining and Petrochemical Industries," Szeptember 2021. [Online]. elérhető:https://www.api.org/-/media/Files/Oil-and-Natural-Gas/Refining/Process%20Safety/RP-754-Fact-Sheet.pdf

[13] Directive 2012/18/EU – Seveso III, Európai Unió, "Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances," Official Journal of the European Union L197, o. 1–37, 2012. júl. 24. [Online]. Elérhető: https://eur-lex.europa.eu/eli/dir/2012/18/oj/eng. [Hozzáférés dátuma: 2025. aug. 02.]
[14] Major Accident Reporting System (eMARS) Európai Bizottság, Joint Research Centre, "Major Accident Reporting System (eMARS)," 2018. ápr. 25. [Online]. Elérhető: https://knowledge4policy.ec.europa.eu/projects-activities/major-accident-reporting-system-emars_en. [Hozzáférés dátuma: 2025. aug. 02.].
[15] Introduction to EU Environmental Law – ERA Module, European Academy of Law (ERA), "Introduction to EU Environmental Law – Module 8, Part 2," [Online]. Elérhető: https://www.era-comm.eu/Introduction_EU_Environmental_Law/EN/module_8/part_2/part_2_1.html. [Hozzáférés dátuma: 2025. aug. 02.].
[16] eMARS Statisztikák - European Commission, Joint Research Centre (JRC), "eMARS Statistics," [Online]. Elérhető: https://emars.jrc.ec.europa.eu/en/emars/statistics/statistics. [Hozzáférés dátuma: 2025. aug. 03.].
[17] eMARS Balesetkereső oldal - European Commission, Joint Research Centre (JRC), "eMARS Accident Search," [Online]. Elérhető: https://emars.jrc.ec.europa.eu/en/emars/accident/search. [Hozzáférés dátuma: 2025. aug. 03.].
[18] R.C. Stokes, Q.A. Baker, M.P. Broadribb, T.V. Rodante, C.A. Grounds, "CCPS Incident Investigation Book, Third Edition," Hazards 29, IChemE, 2019. [Online]. Elérhető: https://www.icheme.org/media/19410/hazards-29-paper-30.pdf. [Hozzáférés dátuma: 2024. november 05.].
[19] Sydney Water, "HSP-014: HIDRA Health and Safety Procedure," 2007. febr. [Online]. Elérhető: https://www.sydneywater.com.au/content/dam/sydneywater/documents/health-and-safety-procedure-HIDRA.pdf. [Hozzáférés dátuma: 2024. december 21.].
[20] G.V. Poje, I. Rosenthal, "The role of the chemical safety board in preventing chemical accidents," Hazards XVI, IChemE, 2001. [Online]. Elérhető: https://www.icheme.org/media/10150/xvi-paper-05.pdf. [Hozzáférés dátuma: 2025. január. 12.].
[21] U.S. Chemical Safety Board (CSB), "CSB Best Practice Guidance," [Online]. Elérhető: https://www.csb.gov/csb-best-practice-guidance/. [Hozzáférés dátuma: 2024. október 15].
[22] Nel Hydrogen, "Status and Q&A regarding the Kjørbo incident," 2019. jún.–júl. [Online]. Elérhető: https://nelhydrogen.com/status-and-qa-regarding-the-kjorbo-incident/. [Hozzáférés dátuma: 2024. aug. 02.].
[23] N. Ade, B. Wilhite, and H. Goyette, "An integrated approach for safer and economical design of Hydrogen refueling stations," Int. J. Hydrogen Energy, vol. 45, no. 58, pp. 32713–32727, 2020, doi: 10.1016/j.ijhydene.2020.09.105.
[24] H2Tools – Santa Clara Incident Review Report Hydrogen Safety Panel, "AP Santa Clara Incident Review Report Rev1," 2021. jún. [Online]. Elérhető: https://h2tools.org/sites/default/files/2021-06/AP_Santa_Clara_Incident_Review_Report_Rev1.pdf. [Hozzáférés dátuma: 2024. aug. 02.].
[25] P. Marsh, "Santa Clara Incident Summary: Hydrogen Trailer Transfill Facility Explosion, 1 June 2019," Individual Incident Summary Report Rev. 0, XBP Refining Con-

sultants Ltd., Santa Clara, CA, Aug. 2023. [Online]. Elérhető https://www.icheme.org/media/24670/santa-clara-incident-summary-01-jun-19.pdf [Hozzáférés dátuma: 2024. aug. 02.].
[26] Y. Lee, M.H. Cho, M.C. Lee, and Y.J. Kim, "Evaluating hydrogen risk management policy PR: Lessons learned from three hydrogen accidents in South Korea," International Journal of Hydrogen Energy, vol. 48, pp. 24536–24547, 2023
[27] S.I. Kim, Y. Kim, "Review: Hydrogen Tank Explosion in Gangneung, South Korea," Center for Hydrogen Safety Conference, AIChE, 2019. [Online]. Elérhető: https://proceedings.aiche.org/chs/conferences/international-center-hydrogen-safety-conference/2019/proceeding/paper/review-hydrogen-tank-explosion-gangneung-south-korea. [[Hozzáférés dátuma: 2024. aug. 02.].].
[28] Fotó: insideevs.com, "Hydrogen Fueling Station Explodes," InsideEVs, May 23, 2019. [Online]. Elérhető: https://insideevs.com/news/354223/hydrogen-fueling-station-explodes/
[29] Fotó: abc7news.com, "Hydrogen explosion shakes Santa Clara neighborhood," ABC7 News, June 3, 2019. [Online]. Elérhető: https://abc7news.com/post/hydrogen-explosion-shakes-santa-clara-neighborhood/5326601/
[30] Fotó: www.koreatimes.co.kr, "Hydrogen tank explosion kills 2 in Gangneung," The Korea Times, May 23, 2019. [Online]. Elérhető: https://www.koreatimes.co.kr/southkorea/society/20190523/hydrogen-tank-explosion-kills-2-in-gangneung
[31] G. Ursachi, I. Horodnic, C. Zait, "How reliable are measurement scales? External factors with influence on Cronbach's alpha," Procedia Economics and Finance, vol.23, pp.679–686, 2015.
[32] G. Ursachi, I. A. Horodnic, and A. Zait, "How reliable are measurement scales? External factors with indirect influence on reliability estimators," Procedia Economics and Finance, vol. 20, pp. 679–686, 2015, doi: 10.1016/S2212-5671(15)00123-9
[33] A. Saltelli, S. Tarantola, F. Campolongo, and M. Ratto, Sensitivity Analysis in Practice: A Guide to Assessing Scientific Models. Chichester, U.K.: John Wiley & Sons, 2004.

DOI: https://doi.org/10.12700/btsz.2025.7.3.129

# RELIABLE AND SAFE COMMUNICATION FOR CONTEMPORARY RAILWAY SYSTEMS

# MEGBÍZHATÓ ÉS BIZTONSÁGOS KOMMUNIKÁCIÓ A KORSZERŰ VASÚTI RENDSZEREKBEN

KÚN Gergely[1] – WÜHRL Tibor[2]

**Abstract**

Digital communication technologies play an important role in the data networks that support modern railway transport. Contemporary railway systems—especially those employing automated train control solutions—place strict requirements on the underlying communication infrastructure. These include high reliability, deterministic behavior, and rapid recovery in the event of connection failures. This paper examines both the operational conditions, technologies, and protocols applied in railway communication infrastructures, and the most important safety-related risks. It provides an in-depth, component-level analysis of latency as a critical hazard. By identifying the different causes of communication delay, it becomes possible to establish clear technical requirements and protocol-level solutions aimed at enhancing reliability and safety. The approaches presented support future network design and contribute to the sustainable development of railway transport.

**Keywords**

telecommunication, railway, ETCS, safety-critical, digital, reliability

**Absztrakt**

A digitális kommunikációs technológiák a korszerű vasúti közlekedést kiszolgáló adathálózatokban is meghatározó szerepet töltenek be. A modern vasúti rendszerek, elsősorban az automatizált vonatbefolyásoló megoldások, szigorú követelményeket támasztanak a kommunikációs hálózatokkal szemben. Alapvető elvárás a magas megbízhatóság, a determinisztikus viselkedés, valamint kapcsolati hiba esetén a gyors helyreállás. A cikk egyrészt a vasúti infokommunikációs infrastruktúrák működési feltételeit, alkalmazott technológiáit és protokolljait vizsgálja, másrészt elemzi a biztonságkritikus szempontból felmerülő legfontosabb veszélyforrásokat is. A késleltetést, mint veszélyforrást részletesen, összetevőire bontva tárgyalja. A késleltetésre ható tényezők feltárása lehetőséget teremt konkrét követelmények meghatározására, valamint olyan technológiai és protokollszintű megoldások kidolgozására, amelyek a megbízhatóság és a biztonság növelését szolgálják. A bemutatott megközelítések támogatják a jövőbeli hálózattervezést, és hozzájárulnak a vasúti közlekedés fenntartható fejlődéséhez.

**Kulcsszavak**

telekommunikáció, vasút, ETCS, biztonságkritikus, digitális, megbízhatóság

[1] kun.gergely@kvk.uni-obuda.hu, kun.gergely@kti.hu | ORCID: 0000-0003-0572-5177 | assistant lecturer, Óbuda University | egyetemi tanársegéd, Óbudai Egyetem | technical expert, Institute for Transport Sciences | megfelelőségértékelési szakértő, Közlekedéstudományi Intézet

[2] wuhrl.tibor@kvk.uni-obuda.hu, wuhrl.tibor@kti.hu | ORCID: 0000-0002-7522-3511 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem | technical expert, Institute for Transport Sciences | megfelelőségértékelési szakértő, Közlekedéstudományi Intézet

## INTRODUCTION

The reliable and safe operation of critical infrastructure is very important at the national level, as failures can lead to serious social and economic consequences. The railway system—including tracks, control equipment, and communication networks—is also considered as critical infrastructure [1]. The role of railway transport is continuously increasing, as it is becoming increasingly important in both passenger and freight transportation.

Modern railway systems increasingly rely on computer-based, automated monitoring and control solutions, where communication networks play a key role. Automatic Train Control (ATC) systems [2] are based on continuous data exchange between the train and the trackside control systems. For these systems in order to function reliably, it is essential that the transmitted information should reach its destination in a secure manner, on time, , and without distortion.

With the rise of digital communication technologies, new challenges have emerged for industrial and safety-critical systems—including the railway sector. Traditionally long life cycle and static systems are increasingly being replaced by rapidly evolving solutions, many of which were originally designed for commercial use. While these new technologies may offer cost advantages, their integration requires a fundamentally different design approach, particularly in the areas of reliability, availability, and risk management.

In railway communication networks, it is very important to classify information based on its criticality, to identify potential hazards accurately, and to apply appropriate protective actions. Technological advancements and standardization efforts jointly create new opportunities as well as new expectations. The goal is to align these aspects in order to implement a robust communication architecture that meets railway safety requirements over long term.

## CONCEPTUAL BACKGROUND AND RELATED WORK

Initially, the key components of railway supervision systems are reviewed. In the early stages of railway supervision and control, signaling devices appeared first. Their function was limited to simple information transmission, without direct intervention in train operations.

### Interlocking systems

The next major advancement was the introduction of interlocking systems, which established logical dependencies between the state of the railway infrastructure and control actions. Unlike basic signaling, interlocking systems do not only provide information but also implement active safety logic—for example, they prevent a switch from being moved if a train occupies the corresponding track.

The central unit of the interlocking system collects and evaluates data from trackside sensors. Based on the gathered information, it performs control actions in accordance with railway safety regulations. A railway infrastructure operator typically has multiple interlocking centers, each responsible for supervising a specific geographical area. These centers are connected via data network that enables information exchange between them [2] [3].

A Computer-Based Interlocking (CBI) system consists of a central server, associated trackside equipment, and the communication network. From the perspective of safe railway operations, it is considered the most critical system.

**Centralized traffic supervision and control**

Central traffic supervision enables the automated monitoring of larger traffic areas, junctions, or longer railway line sections from a central location [4]. In contrast, Centralized Traffic Control (CTC) allows remote supervision and control of train movements from a centralized control center. The centralized control is executed via local interlocking systems, which carry out the issued commands. The primary goal of CTC is to increase the efficiency and flexibility of railway operations.

**Track circuits and axle counters**

One of the fundamental components of railway interlocking systems is track occupancy detection, which reliably identifies whether a train is occupying a specific track or track section. The most common solutions include track circuits and axle counters. In modern railway networks, reliable track occupancy detection is essential for providing accurate track status information, which is required by ETCS (European Train Control System) or other onboard train control systems.

**European Railway Traffic Management System**

The ERTMS (European Rail Traffic Management System) aims to establish a unified train control and management system across national borders. It has three parts:

The ETML (European Traffic Management Layer) covers tasks related to traffic management and control. EIRENE (European Integrated Railway Radio Enhanced Network) provides the radio communication link between onboard and trackside equipment. This role is currently fulfilled by the GSM-R (Global System for Mobile Communications – Railway) system, which will be replaced in the future by the 5G-based FRMCS (Future Railway Mobile Communication System).

The third component is the European Train Control System (ETCS), the elements of which are presented in the following sections. The goal of ETCS is to provide a standardized automatic train protection system and a comprehensive train control solution across Europe, supporting cross-border interoperability.

The implementation of the ETCS system is progressing gradually, and it currently everywhere operates former national systems in parallel. ETCS offers three levels of service capability that will be detailed below. Nowadays Level 2 is the most widely deployed and used, primarily in Europe but increasingly all over the world [5] [6].

**Components in ETCS - Balise**

A balise is a passive device between the rails in a fixed position. It operates based on electromagnetic principles and transmits data by radio waves to a locomotive passing above it. The energy required for data transmission is supplied inductively by the balise transmission unit installed on the locomotive. The transmitted data may include information such as kilometer positions, movement authority, braking commands, or signal states.

In the ETCS system, two types of balises are present: fixed- and controlled balises. Controlled balises are capable of transmitting variable data, which are managed by the LEU (Lineside Electronic Unit). The LEU enables data flow between the interlocking system and

the controlled balise, allowing context-dependent, targeted information transmission based on the current traffic situation. It is applied in ETCS Level 1, and performs point-wise train control. In contrast, fixed balises can only transmit static data and are typically used to provide location reference information, especially in ETCS Levels 2 and 3.

**Radio Block Center**

At ETCS Levels 2 and 3, the Radio Block Center (RBC) is introduced as the central trackside control unit of the system. A railway infrastructure operator may use multiple RBCs. The number of RBCs depends on how many trains could be managed simultaneously by a single RBC (typically between 50 and 100). An RBC can communicate with adjacent RBCs and may have also interfaces to the local CBI systems, the CTC center, and other system components.

The tasks of the RBCs include managing movement authorities for trains and generating control commands based on information received from the interlocking system and trackside equipment. These instructions are transmitted to the onboard equipment by the GSM-R radio network.

**Temporary Speed Restriction System**

The Temporary Speed Restriction System (TSRS) is an optional supplementary function of the ETCS. Its purpose is to manage temporary speed restrictions in the event of maintenance work, track defects, or other temporary safety-related risks. The related control commands are transmitted via the RBC to the onboard units of the affected trains.

**ETCS levels**

ETCS Level 1 (L1) implements point wise train control and it is based on conventional interlocking systems. In this setup, information—such as the current state of a lineside signal—is transmitted to the trains typically via controlled balises managed by LEUs. This version does not use data communication solutions.

ETCS Level 2 (L2) is also based on conventional interlocking systems, meaning that train detection based on track circuits or axle counters. The interlocking system communicates with the RBC, which manages movement authorities within its control area and thereby automates traffic control. Movement authorities, as well as control and status information, are transmitted to the onboard unit by the GSM-R network. Accurate train positioning is very important in ETCS L2, and it is achieved by the onboard system using data received from passed balises. This research focuses specifically on systems operating at this level.

ETCS Level 3 (L3) represents the most advanced version of the system, offering the highest level of functionality. At this level, full radio-based train control is implemented, including continuous speed supervision and moving block operation, which allows dynamic train separation instead of traditional fixed blocks. ETCS Level 3 enables removing all of trackside signaling equipment, as all necessary information is transmitted to the onboard unit via radio communication. Thus, in theory, the role of the train driver could be reduced to a minimum.

A new feature in ETCS L3 that the responsibility of train integrity supervision is assigned to the onboard system. As a result, the vehicles coupled behind the locomotive become integrated into the onboard communication network and maintain a continuous data

transfer to the integrity monitoring unit. This introduces new requirements for the onboard architecture and communication systems.

Reducing the number of trackside devices can lead to significantly lower maintenance costs. Although ETCS L3 has not yet been deployed in regular operation, pilot projects are underway in several European countries [7].

**Communication links among system components**

Modern computer-based systems in railway supervision use information and communication technologies. They improve both infrastructure capacity and operational safety. The operation of such systems requires highly reliable, stable communication networks with continuously increasing transmission capacity. Figure 1 illustrates the interconnections between the components of an ETCS L2 system:

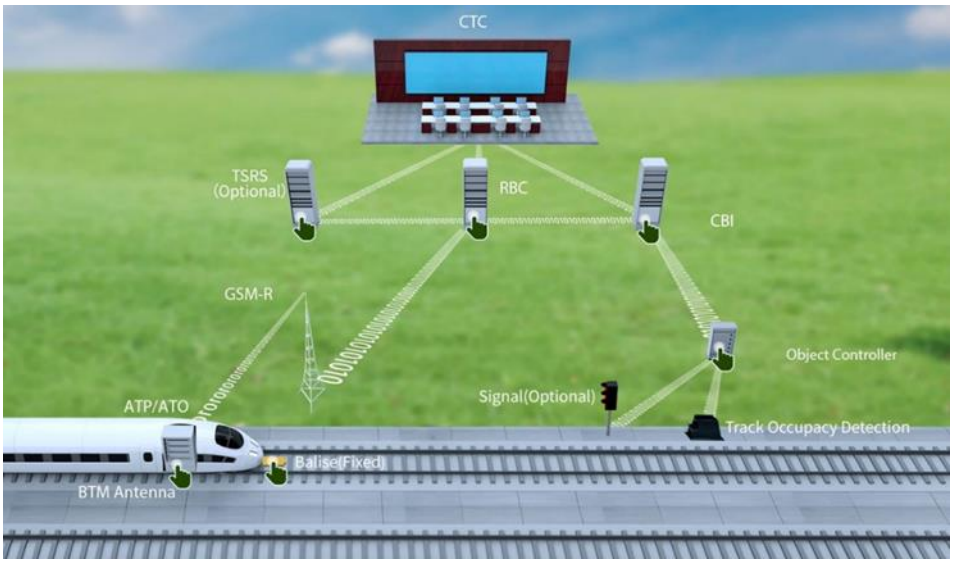



*Figure 1: Communication links among functional components of ETCS L2 system [8]*

From a functional view, the communication links between the system components can be classified based on their importance and safety-critical nature. The following sections present the properties of the connections shown in the figure.

**Safety-critical communication networks**

A safety-critical communication network refers to a type of communication infrastructure whose failure, outage, or performance degradation has a direct and severe impact on the operation and safety of the railway system—potentially posing a direct threat to human life. These networks must typically meet strict reliability, availability, and safety requirements, and are generally required to comply with SIL4 (Safety Integrity Level 4) certification, issued by an independent assessment body. To fulfill the relevant standards, such networks commonly incorporate redundancy, latency optimization, and various error correction or signaling mechanisms.

The CBI–RBC interface (in ETCS Level 2 and Level 3 systems) is responsible for enabling the RBC to calculate and transmit movement authorities and other train operation-

related information in real time. The necessary trackside data—such as the status of switches, signals, and other interlocking elements—is provided by the CBI system through this interface.

The RBC–GSM-R (and in the future, FRMCS) interface facilitates communication between the RBC and the onboard ETCS units via the GSM-R mobile network. This connection ensures the continuous transmission of movement authorities and other operational data to the trains.

The purpose of the radio link between the GSM-R network and the onboard equipment is to ensure continuous data communication between the ETCS onboard unit—namely the Automatic Train Protection (ATP) system and the Automatic Train Operation (ATO) system—and the Radio Block Center (RBC) via the radio channel.

The purpose of the connection between neighboring RBCs is to ensure the seamless handover of ETCS L2 trains from one control area to another, maintaining the continuity of movement authorities and uninterrupted train control.

CBI–Trackside equipment controller connection ensure continuous data flow from track occupancy detection devices (such as track circuits and axle counters) to CBI. The CBI processes data received and controls the associated trackside equipment. Since this communication affects the safety-critical layer of railway control, the interface must meet strict safety requirements and is vital for system operation.

The TSRS–RBC connection allows the RBC to send up-to-date temporary speed restriction information to trains running under ETCS L2 and L3, using data from the TSRS.

**Non-safety-critical communication networks**

A non-safety-critical communication network, in contrast to the previous one, is a network whose failure, temporary outage, or performance degradation does not significantly affect core operational processes. These networks are typically subject to less stringent requirements in terms of reliability, availability, and latency.

The purpose of the CTC–RBC connection is to provide the RBC with operational and time schedule-related data from the CTC system. This information can be taken into account when issuing movement authorities. In case of an interface failure, the RBC can continue to function based on trackside data from the CBI, but traffic management becomes significantly more difficult and may require manual intervention.

The purpose of the CTC–CBI connection is to enable the CTC system to monitor remotely the status of the CBI and, when necessary, to control switches and signals. Although the CBI can operate independently via local control, a loss of the central connection may significantly reduce traffic management efficiency.

The purpose of the TSRS–CTC connection is to allow the CTC system to monitor and manage temporary speed restrictions via this interface, which are stored and maintained by the TSRS. This connection enables the CTC to query, update, or modify speed restrictions, for example in cases of track maintenance or adverse weather conditions. If the interface fails, the CTC can no longer directly manage or verify temporary speed restrictions; however, basic railway operations can still continue.

In addition for normal operation of the system several other non-safety-critical connections are included, which are not shown in the diagram. These are maintenance and diagnostic interfaces, as well as operational communication links, which are present at each

system component. Although these interfaces are not part of the real-time safety chain of train control, they are essential for sustainable operation and for ensuring long-term system reliability.

**Challenges of technological advancement**

To establish the connections between the system components introduced earlier, reliable network solutions are applied. Following the emergence of digital data transmission, synchronous transmission technologies—particularly SDH (Synchronous Digital Hierarchy)—served as the basis of backbone network infrastructures over a long period. These systems were primarily used over optical transmission media, though earlier implementations included copper-based and microwave links as well.

SDH technology provides real-time fault detection and automatic switching to redundant paths, ensuring highly reliable data transmission. It also served as an underlying transport backbone for classical E1 and ATM (Asynchronous Transfer Mode) systems, and later for IP-based networks. Although its use is gradually declining, SDH still plays an active role in many existing railway communication infrastructures.

One of the key features of SDH technology is that the containers transmitted at the data link layer are transferred according to a strictly timed, synchronous system. All transmission nodes are synchronized to a central clock, enabling highly precise timing and deterministic data transfer. As a result, SDH is particularly well suited for serving delay-sensitive applications, such as critical railway communication systems.

A clear trend can be observed today: communication networks are increasingly built on Ethernet-IP foundations. This development is not limited to office and home environments but is also evident in industrial systems, including railway communication networks. The use of Ethernet-IP networks in the railway sector offers several advantages, such as higher data transfer capacity, cost-effective operation, and the use of standardized and widely available equipment. However, this approach also raises significant technical and security challenges, particularly in terms of reliability and protection of safety-critical systems.

Compared to the synchronized communication systems, Ethernet-IP packet-switched networks are fundamentally based on a best-effort transmission model. This means by default, there is no guarantee on the delivery, integrity, or latency of data packets. From a timing perspective, such networks inherently lack the precision required for critical applications. However, significant advancements in network capacity have enabled the introduction of compensating mechanisms that improve the reliability and accuracy of time synchronization. In the future, the role of timing and synchronization will become even more important, especially with the emergence of next-generation standards such as Time-Sensitive Networking (TSN). TSN integrates precise traffic scheduling into Ethernet-based systems, aiming to provide deterministic, predictable, and latency-controlled data transmission—an essential requirement for safety-critical railway applications.

The railway context imposes very strict safety requirements on communication systems. These regulations typically do not prescribe specific technologies, but rather define performance indicators, functional requirements, operational parameters, as well as recommended procedures and solutions.

A similar approach can be observed in other industrial sectors, where standardized requirement frameworks have been developed to ensure the reliability and stable operation of equipment and systems, as well as to protect human health and safety. Depending on the sector, these standards may contain mandatory or optional provisions, and they play a fundamental role in ensuring the compliance of products supplied by manufacturers and vendors.

The IEC 61508 international standard [9], issued by the International Electrotechnical Commission (IEC), provides a general framework for the design, application, maintenance, and operation of electrical, electronic, and programmable electronic safety systems. It covers the entire lifecycle of a product. The standard defines the required input information and expected output results for each lifecycle phase.

Furthermore, it mandates the identification of hazardous events and the assessment of associated risks, taking into account their probability, frequency, and the severity of potential consequences. The application of IEC 61508 is recommended or required in cases, where the operation involves risks that could endanger human life, health, or environmental safety.

Functional safety standards based on IEC 61508 adopt a risk-based approach to achieve the required level of process and system safety. Safety targets are defined using quantitative metrics derived from risk assessments. One such metric is the THR (Tolerable Hazard Rate), which indicates the maximum acceptable probability of occurrence for a hazardous event. In contrast, the TFFR (Tolerable Functional Failure Rate) specifies the acceptable frequency of functional failures.

These standards define four Safety Integrity Levels (SIL), where SIL1 represents the lowest, and SIL4 the most stringent safety requirements. SIL0 is not covered by the standard, as it does not provide formally recognized functional safety. Devices corresponding to each SIL level are classified into two categories by the standard, based on the nature of their usage:

- For low-demand devices, safety performance is characterized by the probability of failure. These systems are typically activated only occasionally—for example, a monitoring system in a power plant that engages only when an operational parameter deviates from the allowed range. If such a system is classified as SIL1, its allowable probability of failure must fall between 0.01 and 0.1.
- For high-demand or continuously operating devices, performance is measured by the frequency of failure occurrence, typically expressed in hours$^{-1}$ (1/h). An example of this would be a route-setting system in railway operations, where the acceptable failure frequency for SIL1 ranges between $10^{-6}$ and $10^{-5}$ failures per hour.

The MSZ EN 50159:2011 standard [10] defines the IT and safety requirements that communication networks supporting railway applications must meet. These networks can be categorized as either closed or open and may interconnect both safety-critical and non-safety-critical system components.

The primary goal of the standard is to ensure the reliability, data security, and resilience of railway communication systems. To this end, it prescribes the use of various security mechanisms, such as encryption, authentication, data integrity checks, redundancy, and fault tolerance. Additionally, the standard specifies documentation requirements that ensure

traceability and transparency, which are essential for the auditability and safety compliance of communication systems.

## RESEARCH RESULTS

A reliable and secure design of communication networks requires a thorough understanding of the potential hazards and failure sources associated with the system. The MSZ EN 50159:2011 standard [10] specifically addresses the identification of risks relevant to communication. Given the broad scope of the topic, present study focuses exclusively on communication and technological aspects.

The standard identifies numerous potential events that may pose a threat to the operation of the transmission system and determines which "basic message errors" they can cause. The most typical of these errors are as follows:

- repetition;
- deletion;
- insertion;
- re-sequencing;
- corruption;
- delay;
- masquerade.

The network infrastructure of safety-critical railway systems must meet strict timing, reliability, and synchronization requirements. A network is considered deterministic primarily if its data transmission times are predictable and guaranteed—this is essential for critical applications.

The delay, which the standard classifies as a "basic message error", should be analyzed by breaking it down into components. This approach allows the various causes of delay to be linked to specific entities involved in the communication process. As a result, the direct effects of these delays can be identified, and corresponding prevention strategies can be defined.

For instance, in Hungary, in case of ETCS L2 implementation, the communication between the onboard equipment and the trackside system may not be interrupted for more than 18 seconds. If the time elapsed since the last valid received message exceeds this threshold, the onboard system automatically initiates a predefined safety action—such as braking or emergency braking. Within this time window—assuming the worst-case scenario—the communication system must be capable of reestablishing the transmission channel. During this process, the GSM-R system must ensure the availability of the radio channel and maintain the connection toward the RBC through the aggregation network.

Regarding latency, several factors contribute to the overall delay, with the following being the most significant:

- connection establishment time or delay;
- transmission delay;
- congestion-induced delay;
- recovery time in case of link or network failure;
- mobility-related delays (e.g., handover).

In the following sections, proven methods and practical recommendations are reviewed to mitigate the effects of these latency components.

**Reduction of call establish time**

The time required to establish a communication path can be minimized by using static IP address allocation, TSN-based preconfigured network schemes, MPLS (Multiprotocol Label Switching) label-based routing, or equivalent solutions. It is strongly recommended to avoid dynamic IP allocation—such as the use of the DHCP (Dynamic Host Configuration Protocol)—because this method introduces uncertainty in both the connection setup time and the recovery time in case of failure. DHCP address allocation is handled by a dedicated server. However, even with redundant configurations, network issues can make the servers unreachable, which may cause unstable network operation.

**Minimizing transmission delay**

Transmission delay refers to the time it takes for a message to travel from the sender to the receiver. This quality parameter is one of critical importance in train control systems, and therefore strict limits apply. It is closely linked to the requirements of real-time operation and is one of the most important factors in the design of deterministic networks. Consequently, not all commonly used network protocols are suitable for application in such a demanding environment.

In wired communication systems, from the perspective of access to the transmission medium, protocols that allow shared medium access are not permitted. In such cases, a competition may arise between frames attempting to transmit simultaneously, which introduces random delays. This excludes the possibility of deterministic operation, as it cannot be guaranteed how long it will take for a given frame to pass through the network segment.

Based on this, it can be stated that in safety-critical networks, the use of shared access protocols (such as Carrier Sense Multiple Access with Collosion Detection or Avoidance - CSMA/CD, CSMA/CA) at Layer 2 is not allowed. Although these access methods are still technically available at the device level, they can—and should—be effectively avoided through appropriate network design, such as the use of point-to-point links, star topologies, and Layer 2 switched paths.

When using a radio channel, access to the shared medium cannot be avoided, so a different approach is required to achieve deterministic operation. A proven solution to this challenge is the use of a strictly time-division-based access method, known as Time Division Multiple Access (TDMA), which assigns predefined time slots to each communicating party. This enables collision-free and predictable data transmission and ensures that time-critical information is delivered reliably and within the required timeframe.

At the network level, the use of Network Address Translation (NAT) should be avoided, as address translation not only slows down and complicates the transmission of data packets but also hinders error detection and traffic tracing—issues that are particularly critical in safety-related systems. The use of VPN-based solutions should also be carefully considered, as they can significantly increase both connection setup time and transmission latency, especially when multi-level encryption or complex tunneling mechanisms are involved. (In non-closed networks, their use may be necessary to ensure adequate data security; in such cases, the increased latency must be taken into account.)

### Increasing availability and reducing recovery time

To ensure high availability, a proven method is the redundant design of communication networks, such as implementing duplicated networks or using ring or dual-ring topologies. These solutions allow data transmission to continue via alternative paths in the event of a network failure.

In commonly used Ethernet networks, early solutions relied on various spanning tree-based protocols, which could handle redundant paths but typically required several seconds for recovery in failure scenarios. However, in safety-critical applications, the recovery time of redundancy-handling protocols must not exceed the millisecond range. Therefore, in Layer 2 switched networks, Spanning Tree Protocol (STP) [11], Rapid STP (RSTP) [12], and Multiple STP (MSTP) [13] are not suitable, as their recovery times are too long for these stringent requirements.

At the network level, when using MPLS technology, it is also possible to define redundant paths using the MPLS Fast Reroute (FRR) mechanism. FRR allows a preconfigured backup Label Switched Path (LSP) to be automatically activated if a failure occurs at any point on the primary route. This switchover typically happens within 50 milliseconds, making MPLS suitable even for latency-sensitive, safety-critical applications. One major advantage of MPLS is that routes can be preplanned, eliminating the need for route calculation during failure, thereby reducing network convergence time in case of a disruption.

While the recovery time provided by MPLS is sufficiently low for most applications, redundancy solutions implemented at lower protocol layers—such as PRP (Parallel Redundancy Protocol) and HSR (High-availability Seamless Redundancy) [14], along with certain vendor-specific implementations [15]—can achieve near-zero (0 milliseconds) recovery time. The key principle of these approaches is that Ethernet frames are sent in duplicate from the sender along diverse paths. On the receiver side, the first-arriving frame is processed, while the second is discarded.

One of the main advantages of these solutions is that they are fully transparent to higher protocol layers. This means that no changes are needed in the upper-layer communication systems when the underlying transport network is replaced by these redundancy mechanisms.

### Acceleration of routing

The timing issues of route selection can be effectively mitigated by implementing the mechanism at lower protocol layers and using simplified algorithms. One of the most widely used solutions today is MPLS, which uses predefined label-switched paths to forward packets, thereby reducing decision-making time. In addition, MPLS enables the integration of Quality of Service (QoS) functions, such as priority-based traffic management, theoretically allowing both critical and non-critical traffic to be handled appropriately over the same physical network. When combined with Ethernet–IP-based infrastructure, this approach provides a fast and reliable route selection mechanism that meets the demands of modern railway communication systems.

## CONCLUSIONS

The fast evolution of communication technologies has become a key factor in the context of railway communication. Modern railway communication systems are required to

meet strict performance requirements, including high reliability, safe operation, and deterministic network behavior, along with extremely fast recovery capabilities.

In analyzation of the communication links between train control systems, interlockings, and other trackside elements, I examined both current and potential technologies and protocols. Based on this, it can be concluded that while Ethernet–IP-based technologies are widely adopted, they cannot fully meet the specific requirements of the railway environment on their own. Their application must therefore be supplemented with additional mechanisms, furthermore, non-deterministic protocols must be entirely avoided in networks that carry safety-critical information.

Through a review of standards for safety-critical systems and communication networks, I identified common risk factors, with a particular focus on latency. The analysis shows that a detailed breakdown of latency components is essential to define precise requirements for the entities and protocols involved in communication. In addition, I have provided recommendations and best practices—based on both literature and personal experience—for mitigating the impact of these risks. The purpose of this analysis was to enhance the reliability of safety-critical communication systems and to support the planning and design of future railway networks.

## SUMMARY

Digital technologies used in railway communication networks enable efficient and automated operation. However, the adoption of new technologies and protocols requires a different perspective on safety, reliability, and performance expectations. Ensuring deterministic network behavior, error-free and secure information delivery, and the integration of appropriate redundancy mechanisms are essential for both current and future railway systems. The reliability of railway communication systems depends on the choice of appropriate technologies and protocols, the careful design of network architecture, and the consistent application of relevant standards. The harmonized implementation of these factors ensures that the systems remain compliant with increasing traffic demands, expanding service requirements, and tightening safety regulations over the long term.

## REFERENCES

[1] Z. Haig, B. Hajnal, L. Kovács and Z. Muha, “A kritikus információs infrastruktúrák meghatározásának módszertana,” Budapest, Hungary: ENO Avisory Kft., 2009. Accessed: Feb. 28, 2024. [Online]. Available: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

[2] P. Baczoni, “Vonali biztosítóberendezések,” Budapest, Hungary, MÁV Szolgáltató Központ Zrt. Baross Gábor Oktatási Központ, 2019.

[3] B. Jóvér, “ETCS, Az Egységes Európai Vonatbefolyásoló Rendszer,” Budapest, Hungary, MÁV Szolgáltató Központ Zrt. Baross Gábor Oktatási Központ, 2006.

[4] G. Tarnai, “Távvezérlés, KÖFE, KÖFI,” Budapest, Hungary, BME Közlekedésautomatikai Tanszék, 2012, Accessed: Jan. 7, 2025. [Online]. Available: https://kjit.bme.hu/images/Tantargyak/Bsc_(2016_elott)_targyak/Vasuti_ir._es_komm._rendsz._I/kfe_kfi_2012_februr_ltalnos_rsz.pdf

[5] *MÁV Feltétfüzet - Az ETCS L1 és L2 pályamenti alrendszerére vonatkozó alkalmazási követelményeire*, MÁV P-5600, 0.1.1. verzió, 2008.
[6] D. Kurhan, M. Kurhan and N. Hmelevska, "Development of the High-Speed Running of Trains in Ukraine for Integration with the International Railway Network," Acta Polytechnica Hungarica, vol. 1/3, pp. 207-218, March. 2022, DOI: 10.12700/APH.19.3.2022.3.16
[7] E. Kretschmer, "ETCS Hybrid Level 3," in *ETCS in Deutschland*, Hamburg, Germany, Eurailpress, 2020, pp. 351–360.
[8] HolySys. "ERTMS/ETCS LEVEL 1/2 Solution." HolySys, Accessed: 6/23/2024 Nov. 11. 2024. [Online.] Available: https://www.hollysys.com/industries/industries/transportation/main-line-railway/railway/22
[9] *Functional safety of electrical / electronic / programmable electronic safety-related systems, International Electrotechnical Commission*, IEC 61508, 2010.
[10] *Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems*, MSZ EN 50159:2011, 2011.
[11] *Local Area Network MAC (Media Access Control) Bridges*, IEEE 802.1D, 1998.
[12] *Local and metropolitan area networks—Common specifications, Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration*, IEEE 802.1w, 2001.
[13] *Local and Metropolitan Area Networks - Amendment to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees*, IEEE 802.1s, 2002.
[14] M. Ostertag, "Seamless Redundancy with PRP and HSR", Accessed: Feb. 1. 2024. [Online.] Available: https://www.zhaw.ch/en/engineering/institutes-centres/ines/communication-network-engineering/seamless-redundancy-with-prp-and-hsr
[15] Moxa Inc., "Redundancy Technologies Application Note", Moxa Inc., Accessed: Jan. 17. 2025. [Online.] Available: https://www.moxa.com/en/literature-library/redundancy-technologies-application-note

DOI: https://doi.org/10.12700/btsz.2025.7.3.143

# CONSUMER SURVEY ON SELF-DRIVING TECHNOLOGY, BROKEN DOWN BY GENDER

# ÖNVEZETŐ TECHNOLÓGIA FOGYASZTÓI VIZSGÁLATA NEMEK SZERINTI BONTÁSBAN

VIKTOR Patrik[1] – KISS Gábor[2]

**Abstract**

Self-driving vehicle technology is receiving increasing attention in the development of modern transport systems, particularly as a result of growing demand for sustainable mobility solutions and technological innovations. However, understanding consumer acceptance is essential for the successful social integration of this technology, with particular regard to gender differences in attitudes, trust and safety expectations. This study presents the results of a comprehensive consumer survey, in which we used the Mann-Whitney U test to analyse how men and women's opinions differ on the use of self-driving technology. The results show that although there are no significant differences between the sexes on many issues, significant differences can be observed in certain areas, such as passenger safety. Based on the results of the research, specific recommendations can be made to decision-makers and technology developers to promote the acceptance of self-driving technologies, improve safety perceptions and ensure the successful integration of the technology into transport systems.

**Keywords**

Self-driving vehicles, Mann-Whitney U-test, generations

**Absztrakt**

Az önvezető járművek technológiája egyre nagyobb figyelmet kap a modern közlekedési rendszerek fejlesztésében, különösen a fenntartható mobilitási megoldások iránti növekvő igény és a technológiai innovációk eredményeként. E technológia sikeres társadalmi integrációjához azonban elengedhetetlen a fogyasztói elfogadás megértése, különös tekintettel a nemek közötti különbségekre az attitűdökben, bizalomban és biztonsági elvárásokban. Jelen tanulmány egy átfogó fogyasztói vizsgálat eredményeit ismerteti, amely során Mann-Whitney U próba segítségével elemeztük, hogyan térnek el a férfiak és a nők vélemények az önvezető technológia alkalmazásáról. Az eredmények rávilágítanak arra, hogy bár számos kérdésben nincs jelentős különbség a nemek között, bizonyos területeken, mint például az utasbiztonság, szignifikáns eltérések figyelhetők meg. A kutatás eredményei alapján konkrét ajánlások fogalmazhatók meg a döntéshozók és a technológiafejlesztők számára, amelyek elősegíthetik az önvezető technológiák elfogadottságát, a biztonsági percepció javítását és a technológia sikeres integrációját a közlekedési rendszerekbe.

**Keywords**

Önvezető járművek, generációk, Mann-Whitney u-próba

[1] viktor.patrik@uni-obuda.hu | 0000-0002-8689-2753| Assistant lecture, Óbuda University | Tanársegéd, Óbudai Egyetem
[2] kiss.gabor@uni-obuda.hu | 0000-0002-0447-9376 | Assistant professor, Óbuda University | Egyetemi docens, Óbudai Egyetem

## INTRODUCTION

Self-driving technologies have developed at an almost unprecedented pace over the past decades, and are now a major focus not only for technological innovation but also for sustainable transport. The worldwide demand for intelligent transport systems has led to new developments that have made autonomous vehicles (AVs) a key driver of mobility innovation. These vehicles are enabled by a combination of sophisticated sensor systems, artificial intelligence and machine learning algorithms, which ensure that they are able to react accurately and reliably to changes in their environment, even in complex traffic situations. One of the most critical aspects of the development of such systems is reliability - a factor that fundamentally determines not only their acceptance, but also road safety as a whole.

However, technological progress alone is not enough - it is just as important to understand how users relate to this new form of transport. Social acceptance does not always keep pace with the rapid spread of technological innovation. Research has consistently shown that people's perception of safety and their trust in technology are key determinants of the social embeddedness of autonomous systems. The issue of safety is particularly pronounced, as many people still fear that these vehicles will not be able to operate reliably and safely in traffic - especially when it comes to their ability to avoid accidents.

In addition, the proliferation of self-driving vehicles raises serious legal, ethical and societal challenges. It's not simply a question of who is liable in the event of an accident - there are also questions about the protection of personal data and protection against cyber-attacks. And we haven't even touched on classic ethical dilemmas such as the famous "trolley problem", where autonomous decisions can be interpreted in moral terms.

The issue of social acceptance is linked not only to overall trust but also to certain demographic differences. A prominent example is the gender gap, which is also reflected in attitudes towards technology. Previous research has shown that women tend to be more cautious, often expressing stronger concerns about safety, while men tend to be more open to new technologies and more likely to try or purchase such vehicles.[1] This gender difference can provide valuable guidance for those working to promote and market technology.

Against this background, the aim of the present study is to examine in depth the consumer acceptance of self-driving vehicles, with a particular focus on gender differences in the dimensions of safety and technological attitudes. The Mann-Whitney U test was used in the research, as this non-parametric statistical method is an excellent way to compare ranked values of independent samples - especially when the distribution of the data does not meet the requirements of normality, which is often the case in social science studies.

Our results provide useful guidance for decision-makers, developers and transport policy makers. The detailed data analysis revealed that although there were no significant differences between male and female respondents on a number of aspects, there were some areas where gender differences were noticeable, such as passenger safety. The conclusions of the study provide some suggestions that could help to promote the social acceptance of autonomous vehicles, contribute to safer transport and increase confidence in the technology.

To sum up, the take-up of self-driving technology is a complex process whose success goes beyond the world of technical innovation. Social support, a sense of security and

the continued building of consumer confidence, taking into account gender differences in opinions, are essential.

## LITERARY PROCESSING

Self-driving vehicles (AVs) are increasingly becoming an integral part of the modern transport system, with technological advances and a growing demand for sustainable mobility solutions. The autonomous vehicle group can be grouped under the following key points: technological development, consumer acceptance, and social, legal and ethical issues.

First of all, technological advances in self-driving vehicles are playing a prominent role in their uptake. AVs are composed of a variety of sensor and control systems that enable accurate perception of their environment and safe navigation [2][3][4]. Reliability is a key factor in the development of such systems, which is achieved by using various algorithms and machine learning techniques [3]. The integration of urban infrastructures with self-driving technologies is essential as it helps to reduce traffic congestion and CO2 emissions [5].

Secondly, consumer acceptance is a key factor in the uptake of self-driving vehicles. Several research studies show that user comfort and safety are essential for the success of the technology [6][7][8]. For example, safety is cited as the most important aspect of self-driving cars, alongside functional and subjective factors [6]. In this regard, it is highlighted that social pressure and the development of trust in the technology will influence consumer behaviour. The current pace of technological innovation is outpacing consumer adoption, which may be a barrier to future uptake [9].

Third, the introduction of self-driving cars raises a number of legal, ethical and social issues. Issues such as liability in the event of accidents, as well as personal data protection and cybersecurity, play a key role in the social discourse [10][11]. Discussing ethical dilemmas, such as the "trolley problem", is essential for the social acceptance of the technology, and the decision-making of vehicles in potentially dangerous situations may be ethically questionable [11].

The future of self-driving vehicles will therefore be shaped by technological innovation, increasing social acceptance and strengthening the legal framework to respond effectively to the challenges of modern mobility.

### Safety of self-driving vehicles

The safety of self-driving vehicles is a major issue in modern mobility, as the introduction of autonomous technologies creates many new challenges and opportunities. The discourse around the development, social acceptance and safety issues of self-driving vehicles has intensified in recent years, as both the benefits and challenges of the technology need to be considered.

The safety of autonomous vehicles is based on technological developments to reduce road accidents and increase transport efficiency. The expectation is that self-driving technology such as sensors and artificial intelligence will enable vehicles to collect and analyse real-time data on traffic conditions, which will improve the decision-making process [12][13]. In this way, autonomous vehicles will be able to anticipate and possibly avoid accident-prone situations, thus reducing the occurrence of road accidents [14].

In addition to technological progress, social acceptance is also a key factor influencing the perception of the safety of self-driving vehicles. Consumers' attitudes and fears about safety play an important role in the extent to which they trust autonomous technologies [15][16]. Some research shows that increasing consumer acceptance requires improving technology and social communication to ensure that users understand and accept new solutions in transport [17][18].

To address security risks, manufacturers and research institutes are working to ensure that cybersecurity concerns are adequately addressed, as autonomous vehicles are interconnected systems whose vulnerability can pose risks to vehicle integrity and user safety [13][19][20]. Cybersecurity is crucial to protect vehicles, as hackers have the potential to manipulate control systems, potentially leading to accidents [15][21]. Implementing robust cybersecurity solutions is essential to strengthen user trust and to successfully integrate autonomous vehicles into the transport ecosystem [22].

In summary, the safety of self-driving vehicles is a complex issue that relies on a combination of technological advances, social acceptance and cybersecurity challenges. For autonomous vehicles to become truly safe, it is essential to continuously develop technological innovations and strengthen the social dialogue.

**Confidence in self-driving cars**

Confidence in self-driving vehicles is a key factor for the successful introduction and uptake of the technology. In order to develop trust, it is important to understand the feelings and attitudes of users, shape the general acceptance of vehicles and their willingness to use the technology.

Building trust depends in part on how people perceive the safety and reliability of self-driving vehicles. Research has shown that the safety and promise of reduced traffic accidents provided by vehicles is closely related to the level of trust [23]. The increased sense of safety promised by self-driving vehicles contributes to users' positive attitudes towards them [24][25][26]. The confident and cautious driving style of vehicles can increase trust among users [27][28].

Further analysis shows that user experience has a significant impact on trust. People who have already tried autonomous vehicles tend to be more positive about the technology, while those who have not and are more sceptical about the reliability of the vehicles [29][30]. During interactions, users may be potentially disappointed if self-driving vehicles do not meet their expectations, which may lead to a decrease in trust [31][32]. Several researches suggest that if vehicles do not perform flawlessly, users tend to lose trust in them in the long run, which may be a barrier to technology adoption [31][32].

| Factor | Characteristics, effects | Examples from the literature |
|---|---|---|
| Technological reliability | Sensor sophistication, use of artificial intelligence, machine vision capability, reliability of real-time data analysis | [2],[3],[14] |
| Cybersecurity | Protection against external attacks, integrity of control systems, protection of personal data | [10],[13],[15] |

| Factor | Characteristics, effects | Examples from the literature |
|---|---|---|
| User experiences | The impact of personal testing and experience, handling system errors, meeting user expectations | [8],[29],[30] |
| Social context | Gender and age differences in attitudes, the role of social norms and cultural factors | [26],[34],[37] |
| Communication, information | Impact of quality of information on technology adoption, importance of marketing communication, effectiveness of education campaigns | [7],[17],[35] |

*Table 1: Factors affecting confidence in self-driving vehicles. Source: own ed.*

The social and cultural context of trust also plays a role. For example, taking into account differences between women and men and age-related differences, studies have shown that women are more prone to mistrust self-driving vehicles, while men tend to have a more positive view of autonomous technologies [34][35]. The attitudes of different groups towards trust provide important social support for vehicle design and transport policy making.

Overall, trust in self-driving vehicles is a complex issue that depends on a number of factors, including technological performance, user experience and social context. Increasing confidence to continuously improve the safety and reliability of vehicles and taking into account user interactions and experiences is a key priority in the deployment of this new transport technology.

**Perception of self-driving cars by women and men**

The gender gap in the perception of self-driving cars is of particular interest, as there are significant differences between men and women in attitudes and risk perception towards self-driving cars. Research shows that women tend to be more cautious, while men are more willing to use self-driving cars [36].

Men have a higher perception of the risks associated with self-driving vehicles and are more likely to perceive these vehicles as less risky. Conversely, women show more concern when it comes to autonomous vehicles, due to their concerns about safety and reliability [36]. Research often cites the social construction of gender roles and the stronger positive correlation between men's technological knowledge and experience [36].

Female respondents often emphasise the importance of professional and personal safety, while for men, technological advances and vehicle reliability predominate [36]. These differences are also reflected in driving habits: female car users often take a more conservative approach and avoid potentially dangerous situations, while men are more likely to take risks [36].

Gender differences are therefore not only reflected in the statistics, but also in the user experience. The different patterns of attitudes of men and women towards vehicles, especially self-driving technologies, can reshape transport policy and vehicle manufacturers' developments. Increasingly, developments should take into account the need to increase the confidence of different groups in autonomous vehicles [36].

Overall, examining the differences in attitudes between men and women is essential in the design and application of future autonomous vehicle technologies to ensure that they are acceptably safe for all user groups.

**Distribution of self-driving car use by gender**

The gender distribution in the use of self-driving vehicles is an important issue that will influence the adoption of the technology and the development of transport policies. There are different perspectives and attitudes between men and women, which influence brand preferences and their feelings about safety.

Several studies have shown that women are generally more cautious about self-driving vehicles than men. Part of the explanation for this effect lies in the fact that women tend to be more risk-averse and concerned about the reliability of the technology [37][38]. While men are more confident, female respondents tend to approach technological innovations with a more cautious attitude, paying particular attention to safety concerns about the vehicles [39].

It is also interesting to note that women often consider social and environmental impacts, while men focus more on technological benefits and vehicle performance [40]. Men dominate interest in vehicles because of the social norms associated with motor vehicles and the influence of driving as a masculine activity [41].

The make and type of vehicle also affect the gender distribution. In addition to sports cars and SUVs, which are traditionally preferred by men, women are more interested in more practical, safer vehicles, the use of which is more suited to their lifestyle and family situation [42]. These views also influence manufacturers' marketing strategies, which try to take into account the needs of different target groups [43].

The process of trust and acceptance is closely linked to the risk assessment of different genders. Men tend to be quicker to adopt new technologies and innovations, while for women, experience and reliability are more important, which can lead to a delay in adoption [44][45]. By taking into account the differences between men and women, it is possible to optimise vehicle design, safety features and marketing campaigns [39][45].

Overall, men's and women's perceptions of self-driving vehicles are not only based on technological utility, but also take into account social norms, risk-assessing attitudes and subjective trust. In this way, it is possible to promote the success not only of the technology, but also of related business policies and strategies.

**Safety of self-driving technology**

The safety of self-driving technology is a key issue in modern transport systems, as it affects not only the efficiency of vehicles on the road, but also the protection of road users. The advancement of self-driving vehicles is constantly creating new challenges that need to be addressed in order to ensure social acceptance and widespread uptake of the technology.

Reliability of the technology and safe operation are the main criteria. The development of self-driving vehicles has seen significant advances in the use of sensors, machine vision and artificial intelligence [46][47]. Vehicles are able to sense their surroundings in real time, assess traffic situations and make optimal decisions to avoid accidents [48].

From a safety perspective, it is essential that self-driving vehicles not only reduce the risk of accidents, but are also able to dynamically manage different environmental and

traffic situations. Driver and pedestrian interactions must be taken into account in the development process, as they have a significant impact on vehicle safety [49][50]. When testing self-driving vehicles, it is important to simulate different environmental conditions and traffic situations to ensure that the technology is truly reliable in real-life situations.

Another key issue is the relationship between transport security and cyber security. The vulnerability of connected self-driving vehicles can be affected by external attacks, such as hacking, if the vehicles are not properly protected [51][52]. Developers must therefore pay attention not only to the mechanical reliability of vehicles, but also to the continuous improvement of cybersecurity systems.

It is important to note that security raises not only technical but also social aspects. The success of the deployment of self-driving technologies is largely influenced by consumer confidence. Recent research has shown that trust and attitudes towards the technology contribute significantly to user acceptance, so social discourse and information is essential [52][53]. It is important for vehicle manufacturers and research institutions to address societal expectations and concerns, otherwise the uptake of the technology may be stalled.

In summary, the security of self-driving technology is a multidimensional issue, including technological reliability, cyber security and social acceptance. A holistic approach that integrates these aspects is therefore essential for future developments.

## MATERIAL AND METHODOLOGY

The Mann-Whitney U test, also known as the Mann-Whitney U test or Mann-Whitney-Wilcoxon test, is a non-parametric statistical test used to test the difference between two independent samples. Nonparametric tests are statistical methods that do not assume a normal distribution of populations.

The Mann-Whitney U test examines whether there is a significant difference between two samples based on the ranked values. The method involves comparing the ranking of all the items in the two samples and calculating which sample has a higher average rank. On this basis, it determines whether there is a statistically significant difference between the two samples.

The basis of the Mann-Whitney U test is that if there is no difference between the two samples, the sum of the ranks of the items in one sample will be similar to the ranks of the items in the other sample. However, if there is a difference between the samples, the sum of the ranks of the items in one sample will tend to be higher than the other.

This test can be used when the variables are not normally distributed or when the measurement scales provide only ranked data. It is often used, for example, in medicine or the social sciences when examining differences between two groups.

The Mann-Whitney U test is usually used to test the following hypotheses:

- Null hypothesis (H0): No significant difference between the two samples.
- Alternative hypothesis (H1): There is a significant difference between the two samples.

The result of the test is a U statistic, which allows us to decide whether to reject the null hypothesis or not. We usually use the critical values or p-values to evaluate the results. The Mann-Whitney U test examines whether there is a significant difference between the results, but does not tell us anything about the causes or correlations.

### The Mann-Whitney U test for comparing genders

While human behaviour plays a key role in road accidents, it is important to look at gender differences in driving habits and accident statistics. Several studies have highlighted differences in driving styles and behaviour between men and women. In general, men tend to have more aggressive driving styles, while women tend to prefer safer and more cautious driving habits.

In addition, accident statistics also reveal some non-specific trends. Although men tend to drive more and are more likely to be involved in accidents, certain types of crashes, such as slow-speed collisions or parking incidents, may be more common for female drivers. Understanding such differences can help to develop more targeted measures to improve road safety [54][55]. Of course, the parametric or non-parametric nature of the data is a key consideration in the choice of the method of analysis. The non-parametric nature of the gender distribution justifies the use of the Mann-Whitney U test.

In general, non-parametric data analysis offers a more flexible approach to data sets that do not meet the conditions imposed by parametric statistical tests. Non-parametric tests, such as the Mann-Whitney U test, do not require knowledge of the exact distribution of the data and are less sensitive to possible outliers in the data or small sample sizes.

Gender analysis is often important in areas where data do not have a normal distribution and/or where variables can be ranked but not measured in intervals or proportions. When working with this type of data, the Mann-Whitney U test can be a powerful tool for examining gender differences and making them statistically meaningful.

Since the data are non-parametric for the distribution of gender, the Mann-Whitney U test is an appropriate tool for statistically assessing and detecting potential differences. The test allows us to draw reliable conclusions about potential differences between genders without distorting the data or ignoring their characteristics.

Differences in the nature of self-driving and their significance are of paramount importance for the development of technology and the uptake of self-driving vehicles. Studies that address the nature of self-driving will contribute to technological developments and to making self-driving vehicles safer. In terms of safety, research on self-driving vehicles is key to shaping the future of road transport. In areas where there is no significant difference between self-driving and conventional driving, the focus should be on safety measures and design elements that improve the safety of self-driving vehicles and user confidence in these technologies. Detailed studies, covering only those areas where there is a difference in the nature of self-driving, will provide relevant and valuable information for designers, engineers and decision-makers. These results will allow them to fine-tune self-driving systems, optimise the user experience and further improve the safety and efficiency of self-driving vehicles. Thus, the differences in the nature of self-driving and their significant relevance are of paramount importance for both technology development and road safety. The results of such studies can help to advance the design and development of self-driving vehicles to make future transport safer and more efficient (Table 2).

| | Male | | Female | | |
|---|---|---|---|---|---|
| | Ave-rage | Source | Ave-rage | So-urce | p |
| Would you use a self-driving car? | 2,65 | 1,202 | 2,50 | 1,165 | **0,000** |
| Would you like to buy self-driving features for your vehicle? | 1,71 | 0,785 | 1,63 | 0,712 | **0,000** |
| How much would you spend on a self-driving feature? | 1,59 | 1,602 | 1,40 | 1,461 | **0,000** |
| Self-driving system should be cheap | 2,57 | 1,087 | 2,50 | 1,070 | **0,007** |
| Self-driving system to simplify driving | 3,11 | 0,870 | 3,16 | 0,855 | **0,003** |
| A self-driving system to make transport faster | 2,85 | 0,996 | 2,86 | 0,982 | 0,793 |
| Self-driving system to increase road safety | 3,44 | 0,791 | 3,41 | 0,845 | 0,662 |
| Self-driving system to increase the value of your car | 2,45 | 1,096 | 2,46 | 1,095 | 0,601 |
| Self-driving system to increase passenger safety | 3,43 | 0,815 | 3,46 | 0,816 | **0,007** |
| Self-driving system to reduce the number of accidents | 3,52 | 0,802 | 3,51 | 0,831 | 0,918 |
| How much would you trust a self-driving system? | 2,86 | 1,361 | 2,83 | 1,362 | 0,284 |
| How much self-driving technology is changing driving safety | 2,97 | 1,338 | 2,93 | 1,346 | 0,092 |
| How safe would you feel in a self-driving car? | 2,86 | 1,373 | 2,80 | 1,356 | 0,050 |

*Table 2 Mean and standard deviation of responses for men and women and Mann-Whitney U test results. Source: own survey N=8663.*

Hypothesis I assumed that there are no differences between men and women in the safety issues expected from self-driving technology.

After conducting the data analysis, the results of which are presented in Table 2, it was found that there were significant differences between men's and women's expectations of self-driving technology in some of the questions asked.

Men would prefer to buy and use a self-driving car, and spend more on it. Women would rather expect self-driving technology to simplify transport. On the question of safety, there is typically no difference between men and women, who are equally likely to expect an increase in road safety, a reduction in accidents from self-driving technology and the same level of safety in a vehicle with this feature. There is one safety issue where there is a significant difference, with women having higher expectations for passenger safety, presumably related to increased protection of children, as no gender difference was found for the question on their own safety [56]

Based on the results of the Mann-Whitney U test, my hypothesis I is confirmed, there are no differences between men and women on the safety issues expected from self-driving technology, except for the issue related to passengers, which is associated with the transport of children.

## SUMMARY

In recent years, the technology of self-driving vehicles has increasingly become the focus of attention in the modernisation of transport. This is not only due to increasingly pressing sustainability needs, but also to technological breakthroughs. This innovation has the potential to become a cornerstone of the future of transport, as it has great potential to reduce accidents, improve road safety and reduce environmental pollution. At the same time, social acceptance is key, especially if we want to talk about a successful introduction in the long term. Therefore, the attitude of different social groups, especially men and women, to this new approach to transport is not an insignificant question. This study presents the results of a large-scale consumer survey in which the researchers used the Mann-Whitney U test. This non-parametric statistical method was ideally suited to this case, as it does not assume a normal distribution of the data - something that is often lacking in the social sciences.

The survey found that while there were significant differences between male and female respondents on a number of points, most of these did not suggest that radically different approaches to promoting or developing technology were needed. Of particular interest was the issue of openness to technology, with men showing stronger acceptance, being more inclined to try or buy self-driving vehicles and not shying away from digging deeper into their pockets to do so. In contrast, female respondents were somewhat more down-to-earth in their approach. They were particularly attracted by the potential of self-driving technology to simplify the everyday challenges of transport, offering convenience and ease. This difference illustrates the societal picture that men are more attracted by the allure and prestige of technological novelty, while women tend to value practicality, comfort and safety more. The issue of safety was also given special emphasis in the analysis, as one of the most important factors in the social acceptance of self-driving systems is the degree to which we feel they are reliable. The data shows a surprisingly even balance: both women and men consider it important that these vehicles actually increase overall road safety, reduce the risk of accidents and make passengers feel safe. This finding is particularly important as it suggests that safety expectations do not really differ by gender - at least in broad terms. The only area where there was some difference was in passenger safety, where women had slightly higher expectations. The study explained this by the fact that women may be more sensitive to passenger protection, especially when it comes to family members or children - an attitude that is understandable and could be an important feedback for developers.

One of the key lessons of the research is that while there are indeed differences in the way men and women approach technology, these are not insurmountable barriers to its social embedding. Rather, they can provide guidance for those responsible for development, deployment or communication. By keeping these differences in mind, they can address users more effectively and facilitate the social integration of self-driving systems. The results of this research will not only provide a basis for technological development, but also for improving the user experience, refining the perception of safety and ultimately making these vehicles an integral part of the transport of the future. In conclusion, the study provides important information for technology developers, manufacturers and transport policy makers. These findings can help to shape policies that take into account the needs of both genders and thus support the successful and widespread uptake of self-driving vehicles.

## LITERATURE


[1] Axios, "Women are less trusting of self-driving cars," Aug. 7, 2019. [Online]. Available: https://www.axios.com/2019/08/07/self-driving-cars-women-trust-survey. [Accessed: June 9, 2025].

[2] M. Lukovics, "Az összekapcsolt autonóm járművek mibenlétéről", Közlekedés És Mobilitás, vol. 2, no. 2, p. 79-88, 2023. https://doi.org/10.55348/km.33

[3] O. Törő and T. Bécsi, "Közúti jármű mozgásmodelljének meghatározása kényszerezett multimodelles szűrő eljárásokkal", Közlekedéstudományi Szemle, vol. 71, no. 6, p. 17-28, 2021. https://doi.org/10.24228/ktsz.2021.6.2

[4] C. Csiszár, D. Földes, & T. Tettamanti, "Mobilitási szolgáltatások komplex automatizálási szintjei", Közlekedéstudományi Szemle, vol. 69, no. 4, p. 33-48, 2019. https://doi.org/10.24228/ktsz.2019.4.3

[5] M. Lukovics, "Összekapcsolt autonóm járművek: kihívások és válaszok a városfejlesztésben", Comitatus, vol. 33, no. 245, p. 73-90, 2023. https://doi.org/10.59809/comitatus.2023.33-245.73

[6] T. Ujházi, "Fogyasztói preferenciák vizsgálata választás alapú conjoint elemzéssel: vásárolna-e önvezető autót?",, 2023. https://doi.org/10.62561/emok-2023-28

[7] B. Zuti and M. Lukovics, "Az önvezető járművek elfogadása viselkedés-gazdaságtani szemléletben. a nudge szerepe a fenntartható városi mobilitás kialakításában", Közgazdasági Szemle, vol. 70, no. 2, p. 149-166, 2023. https://doi.org/10.18414/ksz.2023.2.149

[8] T. Ujházi, M. Lukovics, Z. Majó-Petri, & S. Prónay, "Önvezető járművekkel szembeni fogyasztói preferenciák vizsgálata tényleges próbautat követően",, 2023. https://doi.org/10.62561/emok-2023-29

[9] T. Ujházi, "Önvezető járművekhez kapcsolódó fogyasztói preferenciák vizsgálata", Marketing & Menedzsment, vol. 57, no. Különszám EMOK 2, p. 65-73, 2023. https://doi.org/10.15170/mm.2023.57.ksz.02.07

[10] C. Herke, "A kriminalisztika alapkérdései és az önvezető járművek", Belügyi Szemle, vol. 69, no. 1, p. 87-105, 2021. https://doi.org/10.38146/bsz.2021.1.4

[11] M. Lukovics and N. Nádas, "A felelősségteljes innováció szerepe az autonóm járművek és a társadalom viszonyrendszerében", Polgári Szemle, vol. 18, no. 4-6, p. 295-317, 2022. https://doi.org/10.24307/psz.2022.1221

[12] T. Ujházi, "Önvezető járművekhez kapcsolódó fogyasztói preferenciák vizsgálata", Marketing & Menedzsment, vol. 57, no. Különszám EMOK 2, p. 65-73, 2023. https://doi.org/10.15170/mm.2023.57.ksz.02.07

[13] G. Katona, "Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése (1. rész)", Hadmérnök, vol. 18, no. 3, p. 161-176, 2023. https://doi.org/10.32567/hm.2023.3.11

[14] L. Gál and T. Sipos, "Autonóm gépjárművek elterjedésének hatása a fajlagos nemzetgazdasági veszteségértékekre vonatkozóan", Közlekedéstudományi Szemle, vol. 68, no. 4, p. 74-82, 2018. https://doi.org/10.24228/ktsz.2018.4.6

[15] M. Lukovics, T. Ujházi, & S. Prónay, "Az önvezető járművek elfogadásának társadalomtudományi vetületei: kutatási lehetőségek és módszertani korlátok", Polgári Szemle, vol. 19, no. 4-6, p. 266-280, 2023. https://doi.org/10.24307/psz.2023.1220

[16] B. Zuti and M. Lukovics, "Az önvezető járművek elfogadása viselkedés-gazdaságtani szemléletben. a nudge szerepe a fenntartható városi mobilitás kialakításában", Közgazdasági Szemle, vol. 70, no. 2, p. 149-166, 2023. https://doi.org/10.18414/ksz.2023.2.149
[17] M. Miskolczi, A. Munkácsy, & D. Földes, "Önvezető járművek a turizmusban – technológiaelfogadás a turisták szemszögéből", Turizmus Bulletin, p. 4-15, 2022. https://doi.org/10.14267/turbull.2022v22n4.1
[18] B. Gábor, "Az intelligens közlekedési rendszerek szerepe az okos városok fejlesztésében", Észak-Magyarországi Stratégiai Füzetek, vol. 19, no. 3, p. 100-116, 2022. https://doi.org/10.32976/stratfuz.2022.38
[19] M. Lukovics, "Az összekapcsolt autonóm járművek mibenlétéről", Közlekedés És Mobilitás, vol. 2, no. 2, p. 79-88, 2023. https://doi.org/10.55348/km.33
[20] G. Kiss, „External Manipulation of Autonomous Vehicles,", 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, Leicester, UK, 2019, pp. 248-252, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00085"
[21] G. Kiss, „Manchurian artificial intelligence in autonomous vehicles", Journal of Intelligent & Fuzzy Systems, vol. 38, no. 5, p. 5841-5845, 2020 doi: 10.3233/JIFS-179671
[22] G. Kiss, "External manipulation recognition modul in self-driving vehicles,", 2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 2019, pp. 231-234, doi: 10.1109/SISY47553.2019.9111547.
[23] M. Lukovics, "Összekapcsolt autonóm járművek: kihívások és válaszok a városfejlesztésben", Comitatus, vol. 33, no. 245, p. 73-90, 2023. https://doi.org/10.59809/comitatus.2023.33-245.73
[24] M. Raue, L. D'Ambrosio, C. Ward, C. Lee, C. Jacquillat, & J. Coughlin, "The influence of feelings while driving regular cars on the perception and acceptance of self-driving cars", Risk Analysis, vol. 39, no. 2, p. 358-374, 2019. https://doi.org/10.1111/risa.13267
[25] T. Brell, R. Philipsen, & M. Ziefle, "Scary! risk perceptions in autonomous driving: the influence of experience on perceived benefits and barriers", Risk Analysis, vol. 39, no. 2, p. 342-357, 2018. https://doi.org/10.1111/risa.13190
[26] K. Othman, "Public acceptance and perception of autonomous vehicles: a comprehensive review", Ai and Ethics, vol. 1, no. 3, p. 355-387, 2021. https://doi.org/10.1007/s43681-021-00041-8
[27] S. Tolbert and M. Nojoumian, "Cross-cultural expectations from self-driving cars",, 2023. https://doi.org/10.21203/rs.3.rs-2432387/v1
[28] C. Basu, Q. Yang, D. Hungerman, M. Singhal, & A. Dragan, "Do you want your autonomous car to drive like you?",, p. 417-425, 2017. https://doi.org/10.1145/2909824.3020250
[29] F. Walker, A. Boelhouwer, T. Alkim, W. Verwey, & M. Martens, "Changes in trust after driving level 2 automated cars", Journal of Advanced Transportation, vol. 2018, p. 1-9, 2018. https://doi.org/10.1155/2018/1045186

[30] A. Rezaei and B. Caulfield, "Examining public acceptance of autonomous mobility", Travel Behaviour and Society, vol. 21, p. 235-246, 2020. https://doi.org/10.1016/j.tbs.2020.07.002
[31] M. Nees, "Acceptance of self-driving cars", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 60, no. 1, p. 1449-1453, 2016. https://doi.org/10.1177/1541931213601332
[32] F. Hartwich, C. Hollander, D. Johannmeyer, & J. Krems, "Improving passenger experience and trust in automated vehicles through user-adaptive hmis: “the more the better” does not apply to everyone", Frontiers in Human Dynamics, vol. 3, 2021. https://doi.org/10.3389/fhumd.2021.669030
[33] N. Neef, K. Kastner, M. Schmidt, & S. Schmidt, "On optimizing driving patterns of autonomous cargo bikes as a function of distance and speed—a psychological study", Ieee Open Journal of Intelligent Transportation Systems, vol. 3, p. 592-601, 2022. https://doi.org/10.1109/ojits.2022.3198120
[34] L. Hulse, H. Xie, & E. Galea, "Perceptions of autonomous vehicles: relationships with road users, risk, gender and age", Safety Science, vol. 102, p. 1-13, 2018. https://doi.org/10.1016/j.ssci.2017.10.001
[35] P. Jing, G. Xu, Y. Chen, Y. Shi, & F. Zhan, "The determinants behind the acceptance of autonomous vehicles: a systematic review", Sustainability, vol. 12, no. 5, p. 1719, 2020. https://doi.org/10.3390/su12051719
[36] L. Hulse, H. Xie, & E. Galea, "Perceptions of autonomous vehicles: relationships with road users, risk, gender and age", Safety Science, vol. 102, p. 1-13, 2018. https://doi.org/10.1016/j.ssci.2017.10.001
[37] M. Raue, L. D’Ambrosio, C. Ward, C. Lee, C. Jacquillat, & J. Coughlin, "The influence of feelings while driving regular cars on the perception and acceptance of self-driving cars", Risk Analysis, vol. 39, no. 2, p. 358-374, 2019. https://doi.org/10.1111/risa.13267
[38] K. Othman, "Public acceptance and perception of autonomous vehicles: a comprehensive review", Ai and Ethics, vol. 1, no. 3, p. 355-387, 2021. https://doi.org/10.1007/s43681-021-00041-8
[39] N. Chen, Y. Zu, & J. Song, "Research on the influence and mechanism of human–vehicle moral matching on trust in autonomous vehicles", Frontiers in Psychology, vol. 14, 2023. https://doi.org/10.3389/fpsyg.2023.1071872
[40] A. Chu and G. Huang, "The intersection of voice assistants and autonomous vehicles: a scoping review", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 68, no. 1, p. 1795-1801, 2024. https://doi.org/10.1177/10711813241275908
[41] L. Dundes, "“even more than that, men love cars”: “car guy” memes and hegemonic masculinity", Frontiers in Sociology, vol. 7, 2023. https://doi.org/10.3389/fsoc.2022.1034669
[42] S. Hsieh, A. Wang, A. Madison, C. Tossell, & E. Visser, "Adaptive driving assistant model (adam) for advising drivers of autonomous vehicles", Acm Transactions on Interactive Intelligent Systems, vol. 12, no. 3, p. 1-28, 2022. https://doi.org/10.1145/3545994

[43] F. Camara and C. Fox, "Space invaders: pedestrian proxemic utility functions and trust zones for autonomous vehicle interactions", International Journal of Social Robotics, vol. 13, no. 8, p. 1929-1949, 2020. https://doi.org/10.1007/s12369-020-00717-x
[44] D. NIU, J. Terken, & B. Eggen, "Anthropomorphizing information to enhance trust in autonomous vehicles", Human Factors and Ergonomics in Manufacturing & Service Industries, vol. 28, no. 6, p. 352-359, 2018. https://doi.org/10.1002/hfm.20745
[45] S. Pettigrew, C. Worrall, Z. Talati, L. Fritschi, & R. Norman, "Dimensions of attitudes to autonomous vehicles", Urban Planning and Transport Research, vol. 7, no. 1, p. 19-33, 2019. https://doi.org/10.1080/21650020.2019.1604155
[46] B. Nagy, S. Prónay, & M. Lukovics, "Én vezessek, te vezetsz vagy önvezet? – az önvezetőjármű-elfogadás öt perszóna típusa magyarországon", Marketing & Menedzsment, vol. 56, no. 2, p. 23-34, 2022. https://doi.org/10.15170/mm.2022.56.02.03
[47] E. Kecskés and M. Lukovics, "Az önvezetőflotta-használat költségelőnyeinek lehetséges hatása a magyar városok mobilitására", Észak-Magyarországi Stratégiai Füzetek, vol. 21, no. 1, p. 82-97, 2024. https://doi.org/10.32976/stratfuz.2024.7
[48] M. Miskolczi, A. Munkácsy, & D. Földes, "Önvezető járművek a turizmusban – technológiaelfogadás a turisták szemszögéből", Turizmus Bulletin, p. 4-15, 2022. https://doi.org/10.14267/turbull.2022v22n4.1
[49] T. Ujházi, "Fogyasztói preferenciák vizsgálata választás alapú conjoint elemzéssel : vásárolna-e önvezető autót?",, 2023. https://doi.org/10.62561/emok-2023-28
[50] [T. Ujházi, M. Lukovics, Z. Majó-Petri, & S. Prónay, "Önvezető járművekkel szembeni fogyasztói preferenciák vizsgálata tényleges próbautat követően",, 2023. https://doi.org/10.62561/emok-2023-29
[51] M. Lukovics and N. Nádas, "A felelősségteljes innováció szerepe az autonóm járművek és a társadalom viszonyrendszerében", Polgári Szemle, vol. 18, no. 4-6, p. 295-317, 2022. https://doi.org/10.24307/psz.2022.1221
[52] B. Nagy, S. Prónay, & M. Lukovics, "A szem a technológia elfogadás tükre: az önvezető járművek iránti bizalom szegmentált megragadása szemmozgás-követéssel", Marketing & Menedzsment, vol. 58, no. 1, p. 5-14, 2024. https://doi.org/10.15170/mm.2024.58.01.01
[53] M. Lukovics, T. Ujházi, & S. Prónay, "Az önvezető járművek elfogadásának társadalomtudományi vetületei: kutatási lehetőségek és módszertani korlátok", Polgári Szemle, vol. 19, no. 4-6, p. 266-280, 2023. https://doi.org/10.24307/psz.2023.1220
[54] X. Song, Y. Yin, H. Cao, S. Zhao, M. Li, and B. Yi, 'The mediating effect of driver characteristics on risky driving behaviors moderated by gender, and the classification model of driver's driving risk', Accid. Anal. Prev., vol. 153, p. 106038, Apr. 2021, doi: 10.1016/j.aap.2021.106038.
[55] K. B. Coffman, C. L. Exley, and M. Niederle, 'The Role of Beliefs in Driving Gender Discrimination', Manag. Sci., vol. 67, no. 6, pp. 3551–3569, Jun. 2021, doi: 10.1287/mnsc.2020.3660.
[56] R. K. Lafta, S. A. Al-Shatari, and S. Abass, 'Mothers' knowledge of domestic accident prevention involving children in Baghdad City', Qatar Med. J., vol. 2013, no. 2, p. 17, May 2014, doi: 10.5339/qmj.2013.17.

DOI: https://doi.org/10.12700/btsz.2025.7.3.157

# MANAGING INFORMATION SECURITY RISKS AND CORE VULNERABILITIES OF LARGE LANGUAGE MODELS

# NAGY NYELVI MODELLEK ŐSSEBEZHETŐSÉGEINEK INFORMÁCIÓBIZTONSÁGI KOCKÁZATAI ÉS KEZELÉSÜK

BOTTYÁN Sándor[1]

**Abstract**

The spread of large language models (LLMs) has created new opportunities in information management and enterprise efficiency, while simultaneously exposing a several of new cybersecurity vulnerabilities. This study aims to map the most critical risks associated with LLMs, with particular emphasis on the protection of organizational information assets and the assurance of electronic information security. Based on a comparative analysis of the OWASP Top 10 for LLM publications, the research identifies "core vulnerabilities" that persistently feature within the constantly evolving threat landscape. The study analyzes the technical and organizational risks associated with these vulnerabilities, as well as their impact on the confidentiality, integrity, and availability of LLM ecosystems. Furthermore, it proposes the introduction of risk management and compliance mechanisms that holistically address the security challenges arising from LLMs at both organizational and technological levels.

**Keywords**

LLM vulnerabilities, prompt injection, data leakage, model poisoning, risk management

**Absztrakt**

A nagy nyelvi modellek (LLM-ek) elterjedése új lehetőségeket teremt az információkezelésben és a szervezeti hatékonyságnövelésben, azonban számos új típusú kiberbiztonsági sebezhetőséget is felszínre hozott. Jelen tanulmány célja, hogy feltérképezze az LLM-ek legkritikusabb kockázatait, különös tekintettel a szervezeti adatvagyon védelmére és az elektronikus információbiztonság biztosítására. A kutatás az OWASP Top 10 for LLM kiadványok összehasonlító elemzésén alapulva meghatározza azon „őssebezhetőségeket”, amelyek az állandóan változó fenyegetési környezet permanens szereplői. A tanulmány elemzi e sebezhetőségek technikai és szervezeti kockázatait, valamint azok hatásait az LLM-ökoszisztémák bizalmasságára, integritására és rendelkezésre állására. Ezen túlmenően javaslatot tesz olyan kockázatkezelési és megfelelőségi mechanizmusok bevezetésére, amelyek holisztikus módon, szervezeti és technológiai szinten egyaránt kezelik az LLM-ekből fakadó biztonsági kihívásokat.

**Kulcsszavak**

LLM sebezhetőségek, prompt injektálás, adatszivárgás, modellmérgezés, kockázatkezelés

[1] bottyan.sandor@gmail.com | ORCID: 0000-0002-9195-447X | PhD Student, University of Public Service Doctoral School of Military Engineering | doktorandusz, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola munkakör magyarul, munkahely magyarul

## BEVEZETÉS

Napjaink információs társadalmának legfőbb mozgatórugója az információ előállítása, terjesztése, valamint annak eredményes felhasználása. E fundamentum védelme, vagyis az információbiztonsági tevékenység kiemelt jelentőséggel bír. Az utóbbi évtizedek során tapasztalt digitalizáció eredményeként egyre nagyobb hangsúly helyeződik a kibertéri reziliencia kialakítására is, amelynek fontosságát a 2025. január 01-jén hatályba lépő, Magyarország kiberbiztonságáról szóló törvény megalkotásával a jogalkotó hangsúlyozta [1]. Ez az új szabályozó a NIS2 irányelvben meghatározott kiemelten kritikus és egyéb kritikus ágazatok szabályozásával párhuzamosan, részben azonos szervezet- és rendszerszintű védelmi intézkedéseket követel meg hazánk államigazgatási szerveitől és többségi állami tulajdonban lévő szervezetektől egyaránt [2]. Közismert tény, hogy a jog jellemzően a technológia után követője, hiszen folyamatosan jelennek meg olyan új, innovatív megoldások, amelyek túllépnek a már szabályozott kereteken. Ilyen jelenséget képviselnek napjainkban a nagy nyelvi modellek (large language models, a továbbiakban: LLM-ek) is, amelyekkel leginkább a népszerű csevegőrobotok (például: ChatGPT, Gemini, DeepSeek AI stb.) architektúrájában találkozhatunk és amelyek az utóbbi időszakban jelentős társadalmi népszerűségre és gazdasági térnyerésre tettek szert. Ez a technológia várhatóan rövid időn belül a szervezeti hatékonyság egyik alappillérévé válhat, hiszen az alkalmazásukban rejlő előnyök – például a fejlett információfeldolgozó képesség vagy a generatív funkciók – könnyen integrálhatók az információkezelési folyamatokba. Mindazonáltal az LLM-ek alkalmazása egyedi kockázatok formájában új kihívásokat jelent az elektronikus információbiztonság számára. Egyrészt annak sebezhetőségei által közvetlen veszélybe kerülhet a technológiát alkalmazó szervezet eddig kezelt adatvagyona, másrészt a saját tulajdonban működtetett nagy nyelvi modellek és rendszerkörnyezetük önmagában is jelentős értékű adatvagyon. Ennek okán az információvédelem szempontjából is kritikus jelentőségű az LLM-ekkel kapcsolatos biztonsági kérdések kezelése, ennek érdekében ez tanulmány röviden áttekinti a nagy nyelvi modellek legjelentősebb kiberbiztonsági sérülékenységeit, valamint javaslatokat fogalmaz meg ezek hatékony kezelésére.

## A NAGY NYELVI MODELLEK TÉRNYERÉSE A SZERVEZETI TEVÉKENYSÉGEKBEN

A köznyelvben megfogalmazott mesterséges intelligencia népszerűségének egyik fő mozgatórugója a piacvezető chatbotok képességei. Ezek kifejezetten olyan emberi társalgásra finomhangolt (fine-tuned) LLM modellt és egyéb funkciókat is integráló architektúrák, amelyek ingyenesen bárki számára elérhetőek és természetes nyelveken, emberszerű vállaszokkal képesek valós időben kommunikálni a felhasználókkal. Mindemellett széleskörű tudással rendelkeznek a világunkról és képesek a kérésünknek megfelelő kreatív tartalmat generálni, ezáltal hasznosak a mindennapi tevékenységek (például: munkavégzés, tanulás, szórakozás) során. Ezt az előnyt minden versenyképességre törekvő szervezet, vagy állami feladatokat ellátó aparátus szívesen látná saját eszköztárában, így egyre elterjedtebb jelenség az LLM alkalmazása önálló szervezeti folyamatokban. A szoftvergyártók körében is egyre gyakoribb az asszisztencia jellegű felhasználása, több munkakörnyezeti szoftverben jelenik meg (pl. Microsoft Office 365 – Copilot, Google Workspace – Assistant). Kétségtelen, hogy ez a technológia hamarosan a szervezeti folyamatok technikai támogatójává

válik, ezáltal a szervezeti adatvagyonnal való jelentős kölcsönhatása elkerülhetetlen. Emiatt az elektronikus információbiztonságot érintő modell-sebezhetőségek, valamint a kapcsolódó kockázatok feltérképezése kifejezetten ajánlott tevékenység azon szereplők számára, amelyek eltökéltek az információbiztonsági politikában gyakorta foglalt alapelvek érvényesítésében.

## A NAGY NYELVI MODELLEK RENDSZERSZINTŰ SEBEZHETŐSÉGEI

Az LLM-ek számottevő szervezeti szintű alkalmazása a ChatGPT (GPT-3.5) 2022 novemberi megjelenésével indult, hiszen ezt követően vált széles körben ismerté. Megkezdődött az interaktív webes felület jelentős használata, valamint az API eléréssel történő alkalmazása. A szervezeti alkalmazás ez esetben nem egyfajta szabályozott eljárásként, vagy saját fejlesztésként értelmezendő, hanem az úgynevezett „shadow AI" jelenség megjelenésére, amely az AI eszközök – informatikai vagy információbiztonsági szakterület jóváhagyása vagy felügyelete nélküli – alkalmazását jelenti a munkavállalók által. Az új technológia biztonsági tesztelésére számos önjelölt szakértő mellett kiberbiztonsági szervezetek is vállalkoztak. Az elmúlt években (2023-2024) az Open Web Application Security Project (OWASP) nemzetközi csapata több száz szakértővel és szervezettel (pl. AI óriásvállalatok, kiberbiztonsági vállatok, hardvergyártók, egyetemi kutatólaborok) együttműködve meghatározta a nagy nyelvi modellekkel működő alkalmazások legkritikusabbnak gondolt sebezhetőségeinek listáját. Tekintettel arra, hogy az LLM alkalmazások közege is folyamatosan változó környezet, vagyis úgynevezett „mooving landscape" (a kifejezés a kiberbiztonsági kockázatelemzésben arra utal, hogy az informatikai és technológiai környezet folyamatosan változik, ezért a kockázatok is állandóan átalakulnak), az eltérő verziójú listákban (0.1.0, 0.5.0, 0.9.0, 1.0.0, 1.0.1, 1.1.0 és 2025) rögzített LLM sebezhetőségek természetesen nem mutatnak homogén képet. Azonban egy mátrixban megjelenítve könnyen megállapíthatók azon típusú sebezhetőségek, amelyek az eltérő időszakokban történt felülvizsgálat alkalmával minden esetben megjelentek. Ezeket nevezhetjük úgymond „ősszebezhetőségeknek" is. (1. táblázat).

| Kiadás éve | 2023 | | | 2024 |
|---|---|---|---|---|
| Verzió | 0.1.0 | 0.5.0 | 0.9.0-1.1.0 | 2025 |
| 1. | Utasítás injektálás | Utasítás injektálás | Utasítás injektálás | Utasítás injektálás |
| 2. | Adatszivárgás | Nem biztonságos kimenetkezelés | Nem biztonságos kimenetkezelés | Adatszivárgás |
| 3. | Nem megfelelő sandbox izoláció | Tanítóadat-mérgezés | Tanítóadat-mérgezés | Ellátási lánc |
| 4. | Jogosulatlan kódfuttatás | Szolgáltatás-megtagadás | Modell-szintű szolgáltatás-megtagadás | Adat- és modellmérgezés |
| 5. | SSRF-sebezhetőségek | Ellátási lánc | Ellátási lánc | Helytelen kimenetkezelés |
| 6. | Túlzott függőség | Jogosultsági problémák | Adatszivárgás | Túlzott önállóság |
| 7. | Nem megfelelő MI-összehangolás | Adatszivárgás | Nem biztonságos bővítmények | Rendszerprompt-kiszivárgás |
| 8. | Nem megfelelő hozzáférés-ellenőrzés | Túlzott önállóság | Túlzott önállóság | Vektor- és beágyazási gyengeségek |

| Kiadás éve | 2023 | | | 2024 |
|---|---|---|---|---|
| Verzió | 0.1.0 | 0.5.0 | 0.9.0-1.1.0 | 2025 |
| 9. | Helytelen hibakezelés | Túlzott függőség | Túlzott függőség | Félrevezető információ |
| 10. | Tanítóadat-mérgezés | Nem biztonságos bővítmények | Modell-lopás | Korlátlan erőforrás-felhasználás |

*1. Táblázat: a nagy nyelvi modellek legjelentősebb kiberbiztonsági sebezhetőségei. Forrás: a szerző szerkesztése*

A fenti mátrixban rögzített sebezhetőségek mindegyike egyaránt kiemelten magas kockázatot képvisel, de a megjelenések gyakorisága alapján az alábbi három kritikus kockázatú össsebezhetőségeket határozhatjuk meg:

1. Prompt injektálás (prompt injection);
2. Adatszivárgás (data leakage or sensitive information disclosure);
3. Tanítóadat- és modellmérgezés (training data poisoning and model poisoning).

Ezek a sérülékenységek jellemzőik alapján kifejezetten differenciálhatók, továbbá az LLM architektúrák életciklusának több szakaszán is értelmezhetők. Az alábbiakban e sérülékenységek jellemzőinek részletes kifejtése következik.

**Utasítás injektálás (prompt injection)**

Az utasítás injektálás egyértelműen a nagy nyelvi modellek legkritikusabb sérülékenysége, amely során olyan speciálisan összeállított bemenetekkel (promptokkal) manipulálják a modellt, hogy annak működése kikerülje a rendszer alapvető biztonsági mechanizmusait, és a támadó által kívánt módon viselkedjen. A támadópromptok célja, hogy az architektúra valamely pontján megváltoztassa a modell működését. Két típusa ismert: a közvetlen és a közvetett. A közvetlen prompt injektálás során az LLM architektúra bemenetén (input) keresztül történik a sérülékenység-kihasználás. Ezzel szemben a közvetett prompt injection a modellnek egy későbbi működési folyamata során jut be az architektúra működésbe (például: plugineken vagy weboldalak forráskódján keresztül, beolvastatott fájl forráskódjában vagy szöveges tartalmában). [5] Szándék szerint ezek a támadások lehetnek szándékosak vagy szándékolatlanok. Előbbi esetében kifejezetten az sérülékenység kihasználásán érvényesül a rosszindulatú akarat, utóbbi esetében viszont valamilyen véletlen, előre nem várt esemény téríti el az alapértelmezett működést [6].

Ilyen típusú támadások során a támadók sikeresen kikerülhetik az LLM biztonsági mechanizmusait (safety layers), és legrosszabb esetben képesek felhasználni annak erőforrásait (például: számítási kapacitás, hálózati kapcsolatok), valamint különféle adatforrásokhoz (például: adatbázisok, konfigurációs beállítások stb.) való hozzáféréseit. Ez sajnos lehetőséget biztosít további rosszindulatú tevékenységek végrehajtására, például adatlopásra vagy social engineering típusú támadásokra is. Komplex támadási forgatókönyvekben egy kompromittált személyes LLM-asszisztens akár jelentős mennyiségű érzékeny információ kiszivárgását is eredményezheti, mivel hozzáfér a személyes levelezésünkben található információkhoz [7].

Kihasználása az alábbi főbb negatív hatásokat eredményezheti:

- Érzékeny információk kiszivárgása (például: tanítóanyag-, architektúra-, infrastruktúra információk; rendszer-promptok; személyes adatok; belső felhasználású és üzleti titkok stb.).
- Hibás vagy manipulált kimenetek létrehozása (például: döntéshozatali folyamatok manipulálása, genaratív funkciók érvényesülése hibás vagy manipulatív tartalommal, dezinformáció stb.).
- Jogosultság kiterjesztés (privilege escalation). A rosszindulatú személy a biztonsági funkciókat megkerülve többletjogosultságokat szerez az adott munkamenet (session) során, amellyel hozzáférhet a rendszer alapvető funkcióihoz és képessé válik tetszőleges parancsokat végrehajtattni, amely további kritikus hatásokat eredményezhet [6].

**Adatszivárgás**

Egy szervezeti adatvagyon integritásának és bizalmasságának megőrzése a nagy nyelvi modellek alkalmazása mellett tekintélyes információbiztonsági kihívás. Egyrészről az LLM generált kimenetén megjelenhetnek olyan szenzitív szervezeti adatok (például: személyes adatok, üzleti titkok), amelyek az előtanítás (pre-training), vagy a finomhangolási (fine-tuning) életciklus szakaszok során a tanítóanyagban – az adattisztítást követően is – megmaradtak. Másrészről a tanítóanyag – kiváltképp a webkaparással megalkotott korpuszok – tartalmazhatnak harmadik félre vonatkozó különleges adatokat (például: személyes adatok, jelszavak), amelyek jogtalan kezelésével és továbbításával adatvédelmi incidens jöhet létre [8]. Továbbá léteznek úgynevezett modell extrakciós támadások (model extraction attacks), amelyekkel meghatározható az LLM belső architektúrája és paraméterei, vagy akár tréningadatainak részleges rekonstrukciója is létrehozható. Amennyiben nem on-premise (olyan szoftvermegoldás, amely fizikailag kizárólag a szervezet saját infrastruktúráján található, nem pedig felhőalapú vagy külső szolgáltatónál), hanem úgynevezett hostolt modellek (például: ChatGPT, Gemini) képességét csatornázzuk be saját ügynök-alkalmazásunkba, ezen a kapcsolaton védett adatokhoz [9] férhet hozzá a harmadik fél (LLM üzemeltető). Ezeket az adatokat akár a modellek további fejlesztésére és tanítására is felhasználhatják [6].

Továbbá érdemes figyelembe venni az olyan humánkockázatokat, mint az architektúra jellemzőket tartalmazó rendszerterv dokumentációk szándékos kiszivárogtatása, vagy az ezt célzó social engineering támadás. Adatszivárgás jöhet létre továbbá a modellek hibás konfigurációs beállításaiból is, ez esetben „túlbeszélhet" a modell, vagyis a fejlesztési környezetben alkalmazott diagnosztikai vagy technikai információkat is megoszthat [6].

A sérülékenység kihasználása az alábbi főbb negatív hatásokat eredményezheti:

1. Személyes adatok (personal identifiable informations), illetve védett adatok kiszivárgása, amely a korábbi tanítóanyag rekonstruálásával, vagy az architektúrán keresztülhaladó adatfolyam (data stream) lecsapolásával történik.
2. Modellszivárgás (model leakage). A modell – akár szabadalom alatt álló –forráskódjainak, algoritmusainak, paramétereinek részbeni kiszivárgása, belső működésre vonatkozó információk kijutása [6].

### Adatmérgezés vagy modellmérgezés

A modellek életciklusuk több pontján dolgoznak fel jelentős mértékű adatot, ezek az előtanítás (pre-traine), a finomhangolás (fine-tune), valamint az üzemelés alatti beágyazás (embedding). Adatmérgezésről beszélünk akkor, amikor a feldolgozandó adatkészletet rosszindulatú szándékkal úgy manipulálják, hogy az alapértelmezett modellműködés során konkrét sérülékenység, hátsó kapu (back door), vagy modell-elfogultság jöjjön létre. Egy sikeres adatmérgezés sajnos szignifikáns hatásokkal bír. Drasztikusan csökkenti a modell kiberbiztonsági állapotát és megítélését, ronthatja annak teljesítményét, eltérítheti a kívánt etikus viselkedési normáktól, közvetett hatásként számottevő kockázatot jelenthet a kapcsolódó ökoszisztémák biztonságára is. A legnépszerűbb, óriásvállatok által üzemeltett (hostolt) modellek kevésbé érzékenyek a modellmérgezésre a jelentős számban foganasított biztonsági intézkedésnek köszönhetően, míg a bárki számára elérhető nyílt forráskódú modellek (például: LLaMa, Mistral stb.) esetében valószínűbb mérgezési kockázatokkal kell számolnunk.

A sérülékenység kihasználása az alábbi főbb negatív hatásokat eredményezheti:

1. Eltérített modellműködés (1). A támadók előzetesen manipulálják a tanítóanyagot, amelyet később a modell képzéséhez a fejlesztők felhasználnak, ezt követően ez a generatív funkciók során befolyásolt kimeneteket eredményez.
2. Eltérített modellműködés (2). A támadók a rosszindulatú kódokat tartalmazó tartalmakat (például: weboldalak forráskódjai) állítanak elő (például: lejárt domainek újra vásárlása, Wikipedia oldal szerkesztése), amelyre az interakció során ráirányítják a modellt. A modell által beágyazott a káros kód eltéríti az alapértelmezett modellműködést.

## KONKLÚZIÓ

A nagy nyelvi modellek gyors ütemű elterjedése és fejlődési üteme rendszeresen új típusú kiberbiztonsági sebezhetőségeket hoz felszínre, amelyek az LLM-ek életciklusának több pontján (például: tanítóanyag, előtanítás, finomhangolás, beágyazási folyamatok és interakció), is azonosíthatók. Hatásuk kiterjed a szervezeti adatvagyon bizalmasságára és sértetlenségére, a modelleket használó alkalmazások ökoszisztémájára és erőforrásaira, illetve a további kapcsolt rendszerekre egyaránt. Ebből adódóan az LLM ágensek (ügynökök) kiberbiztonsági kockázatkezelése összetett szakmai kihívás, hiszen egyaránt tartalmaz technológiai és szervezeti szintű intézkedéseket is. Előbbi csoportba olyan szükséges intézkedéseket sorolhatunk, mint az adattitkosítás, az adat-anonimizálás, a hozzáférés-ellenőrzés, az API (application programming interface) kezelés, az erős szintű autentikáció és autorizáció, valamint a sebezhetőség felderítés és a „secure by design” tevékenység. Míg az utóbbiba sorolható intézkedési kör többnyire a szervezetszintű információbiztonsági kockázatmenedzsment rendszer e tekintetben (pl. LLM sebezhetőség azonosítás, LLM incidensmenedzsment folyamatok való bővítését. Továbbá ide sorolható az AI compliance tevékenység, amely a GDPR, az AI Act követelményeknek való megfeleltetés mellett az etikai elvek alkalmazását, a folyamatok teljes átlátható dokumentálása is jelenti [3] [4]. A szervezetszintű biztonságos és felelős alkalmazásuk csak akkor biztosítható, ha a technológiai fejlődést a jogalkotás, a szakpolitika és a szervezeti gyakorlat egyaránt proaktívan követi és alakítja.Természetesen ez a tanulmány nem kívánja eme komplex rendszer minden elemét és

eljárását vizsgálni, megállapításaival leginkább a legfőbb LLM sebezhetőségekkel kapcsolatos kockázatkezelésen alapuló védekezéséhez kíván ajánlásokat megfogalmazni.

Ennek érdekében a tanulmány az alábbi fő megállapításokat tette:

- a különböző OWASP Top10 for LLM kiadások összehasonlításával megállapítható, hogy a LLM threat landscape dinamikusan változik, ugyanakkor az azonosított „őssebezhetőségek" tartós jelenléte kiemelt elemzési és kezelési fókuszt igényel,
- az egyes sérülékenységek konkrét, szervezeti szintű kockázati hatásai (például: jogosulatlan hozzáférés, adatlopás, működésmanipuláció stb.) azonosíthatók, hatásuk megbecsülhető. Ez lehetőséget ad a célzott védelmi és ellenőrzési mechanizmusok kialakítására.
- Az őssebezhetőségek szervezetszintű hatásai okán az LLM biztonságos alkalmazása csak holisztikus, szervezeti és technológiai szinten egyaránt összehangolt kockázatkezelési gyakorlat révén biztosítható.

## JAVASLATOK

A hazánkban is érvényesített európai kiberbiztonsági, adatvédelmi vagy mesterséges intelligencia témában létrejött szabályozási irányelvek és rendeletek (például: NIS2, GDPR, AI Act) alapvető kiindulópontot nyújtanak ugyan, azonban nem reflektálnak teljes mértékben az LLM-ek sajátos működésére és életciklusából fakadó kiberbiztonsági kihívásaira. Az LLM-ek biztonsági és megfelelőségi követelményei a technológia működési sajátosságait is figyelembe vevő, szervezet és rendszerszintű szabályozási megközelítést igényelnek – különösen a magas kockázatú szektorok (pl. pénzügy, egészségügy, államigazgatás) esetében. Érdemes lehet a GRC (governance, risk management, and compliance) fogalomhoz köthető eljárásokat a nagy nyelvi modellek teljes életciklusát figyelembe véve megvalósítani. Szervezetszinten az AI irányítási rendszer (artificial Intelligence management system, AIMS), az adatvédelem, az információbiztonsági kockázatkezelés (különösen: information security managment system, ISMS), valamint a jogszabályi megfeleltetés folyamatait létrehozni. Míg rendszerszinten az architektúra-biztonság, az adatforrás-kontroll és a modellkimenetek validálhatósága válik a központi elemekké. Az ennek érdekében kialakított szervezeti eljárások létrehozása figyelembe vehetők az alábbi szabványok, ajánlások és jógyakorlatok:

- Az ISO/IEC 27000:2023 szabványcsalád alkalmazása. Különösen az ISO/IEC 27090 szabvány, amely útmutatást nyújt a szervezetek részére az mesterséges intelligencia rendszerek biztonsági fenyegetéseinek és hibáinak azonosítására és a kezelésére, és több más LLM sebezhetőség mellett az őssebezhetőségeket is kezeli [10]. Továbbá a kockázatok kezeléséhez járul hozzá az ISO/IEC 42000:2023 szabványcsalád is, amely e mellett támogatja a felelős és átlátható irányítást, valamint a jogszabályi megfelelést is.
- A NIST AI 600-1 szabvány, vagyis a mesterséges intelligencia kockázatmenedzsment keretrendszer (artificial risk management framework) az információbiztonság témáján belül szintén feldolgozza az tanulmány által megállapított főbb sebezhetőségeket. A szabvány alkalmazása az ISO/IEC 27000 alternatívájaként szintén segíthet a szervezeteknek azonosítani a generatív mesterséges intelligencia kockázatait,

és a szervezeti célokhoz illeszkedő kockázatkezelési mechanizmusok érvényre juttatását. [11]

- A Google Secure AI Framework (SAIF) biztonsági keretrendszerében foglalt kontrollok szintén alkalmazhatók az őssebezhetőségek kockázatainak kezelésére, a nagy nyelvi modellek biztonságos bevezetésére és működtetésére.
- Az LLM sebezhetőségekkel járó kockázatok csökkentésére, a sérülékenységek kihasználásának megelőzésére az OWASP ajánl konkrét stratégiákat, amelyek módszertanokat és technikai javaslatokat egyaránt tartalmaznak [6].
- A saját tervezésű LLM architektúrák megbiztonsági határainak megállapításához segítséget nyújthat az adatfolyam diagram (data flow diagram) alkalmazása, valamint a STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege) módszertan is hozzájárulhat a sebezhetőségek azonosításához, ezátal a megfelelő védelmi intézkedések kidolgozásához [12].

## FELHASZNÁLT IRODALOM

[1] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.
[2] Az Európai Parlament és a Tanács 2022. december 14-ei (eu) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról.
[3] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).
[4] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) (EGT-vonatkozású szöveg)
[5] „Wunderwuzzi's blog. Plugin Vulnerabilities: Visit a Website and Have Your Source Code Stolen," [Online]. Available: https://embracethered.com/blog/posts/2023/chat-gpt-plugin-vulns-chat-with-code/.
[6] „OWASP Top 10 for Large Language Model Applications.," [Online]. Available: https://owasp.org/www-project-top-10-for-large-language-model-applications/.
[7] K. Greshake, S. Abdelnabi, S. Mishra, C. Endres, T. Holz és M. Fritz, Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection., https://doi.org/10.48550/arXiv.2302.12173, 2023.
[8] H. Nihad, „Explore mitigation strategies for 10 LLM vulnerabilities.," 2024. [Online]. Available: https://www.techtarget.com/searchEnterpriseAI/tip/Explore-mitigation-strategies-for-LLMvulnerabilities..
[9] 2023. évi CI. törvény a nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról.

[10] „ISO/IEC DIS 27090(en). Cybersecurity – Artificial Intelligence – Guidance for addressingsecurity threats and failures in artificial intelligence system," [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27090:dis:ed-1:v1:en.
[11] „NIST InformationTechnology Laboratory. AI Risk Managment Framework.," [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework.
[12] G. Klondik, „Threat Modeling LLM Applications.," 2023. [Online]. Available: https://aivillage.org/large%20language%20models/threat-modeling-llm/.
[13] „NIST Trustworthy and Responsible AI NIST AI 600-1 Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

DOI: https://doi.org/10.12700/btsz.2025.7.3.167

# ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: ANOMALIES IN THE TRACKING (APPLICATION OF MACHINE LEARNING TECHNIQUES TO DETECT NETWORK ANOMALIES)

# MESTERSÉGES INTELLIGENCIA A KIBERBIZTONSÁGBAN: ANOMÁLIÁK NYOMÁBAN (GÉPI TANULÁSI TECHNIKÁK ALKALMAZÁSA HÁLÓZATI ANOMÁLIÁK DETEKTÁLÁSÁRA)

OLÁH Róbert[1]

**Abstract**

With the rise of digitalization, cybersecurity has become one of the most critical areas of our time. The IT infrastructures of corporate and government systems are exposed to various cyber attacks every day, such as DDoS attacks, data leaks, network penetration attempts or even internal unauthorized activities. These events can cause serious damage not only financially but also in terms of reputation. Network models and their operation play an important role in building IT infrastructures. The reliable operation of modern IT systems fundamentally depends on the stability and protection of network infrastructures. With the increase in digital traffic, threats to networks are also becoming increasingly complex and frequent. In the IT network, countless network devices have a role in the operation of the network. Network anomalies are becoming an increasingly challenging issue in network traffic. The aim of the research is to investigate the effectiveness of various machine learning algorithms for detecting network anomalies in the cybersecurity context.

**Keywords**

anomalies, detecting, cybersecurity, various machine,network traffic

**Absztrakt**

A digitalizáció térnyerésével a kiberbiztonság napjaink egyik legkritikusabb területévé vált. A vállalati és állami rendszerek informatikai infrastruktúrái nap mint nap ki vannak téve különféle kibertámadásoknak, mint például DDoS támadásoknak, adatszivárgásoknak, hálózati penetrációs próbálkozásoknak vagy akár belső jogosulatlan tevékenységeknek. Ezek az események súlyos károkat okozhatnak nemcsak anyagi, de reputációs szempontból is. A hálózati modellek és annak működése fontos szerepet játszanak az informatikai infrastruktúrák építésében. A modern informatikai rendszerek megbízható működése alapvetően a hálózati infrastruktúrák stabilitásán és védelmén múlik. A digitális forgalom növekedésével a hálózatokat érő fenyegetések is egyre összetettebbé és gyakoribbá válnak. Az informatikai hálózatban számtalan hálózati eszköz működhet, amelynek szerepe van a hálózat működésében. A hálózati forgalomban egyre nagyobb kihívást jelentenek a hálózati anomáliák. A kutatás célja annak vizsgálata, hogy milyen hatékonysággal alkalmazhatók különböző gépi tanulási algoritmusok a hálózati anomáliák detektálására a kiberbiztonság kontextusában.

**Kulcsszavak**

anomália detektálása, gépi tanulás, hálózati modellek, hálózati forgalom

[1] olah.robert0721@gmail.com | ORCID: 0009-0007-9134-9521 | IT teacher, Center of Erd Education | Informatika oktató, Érdi Tankerületi Központ

# BEVEZETÉS - A TÉMA ELMÉLETI BEMUTATÁSA (SZAKIRODALOM-FELDOLGOZÁS)

## Háttér és problémafelvetés

A kutatásom témája a mesterséges intelligencia a kiberbiztonságban gépi tanulási technikák alkalmazásával az informatikai hálózati anomáliák detektálására. A témakör fontos szerepet játszhat a hálózat biztonságos működésére tekintve.

A digitalizáció térnyerésével a kiberbiztonság napjaink egyik legkritikusabb területévé vált. A vállalati és állami rendszerek informatikai infrastruktúrái nap mint nap ki vannak téve különféle kibertámadásoknak, [8] mint például DDoS támadásoknak, adatszivárgásoknak, hálózati penetrációs próbálkozásoknak vagy akár belső jogosulatlan tevékenységeknek [13]. Ezek az események súlyos károkat okozhatnak nemcsak anyagi, de reputációs szempontból is. A hálózati modellek és annak működése fontos szerepet játszanak az informatikai infrastuktúrák építésében. A modern informatikai rendszerek megbízható működése alapvetően a hálózati infrastruktúrák stabilitásán és védelmén múlik. A digitális forgalom növekedésével a hálózatokat érő fenyegetések is egyre összetettebbé és gyakoribbá válnak. Az informatikai hálózatban számtalan hálózati eszköz működhet, amelynek szerepe van a hálózat működésében. A hálózati forgalomban egyre nagyobb kihívást jelentenek a hálózati anomáliák. A hálózati anomáliák – mint például az elosztott szolgáltatásmegtagadásos (DDoS) támadások, jogosulatlan behatolások vagy hibás konfigurációk – jelentős kockázatot jelentenek a szolgáltatások folyamatosságára és az adatok biztonságára nézve. [13] A hagyományos, szabályalapú forgalomelemző rendszerek korlátozottan képesek kezelni a dinamikusan változó és ismeretlen támadási mintákat. Ezek az eszközök jellemzően múltbeli minták alapján működnek, így nem alkalmasak előre nem látott fenyegetések azonosítására. Mindez rámutat arra, hogy a hálózati biztonság jövője a prediktív, adaptív technológiák felé mutat, ahol kiemelt szerepet kapnak a mesterséges intelligencián és gépi tanuláson alapuló megközelítések.

A hagyományos, szabályalapú biztonsági rendszerek – például tűzfalak vagy behatolásérzékelő rendszerek (IDS) – egyre kevésbé bizonyulnak hatékonynak a folyamatosan fejlődő fenyegetések ellen. Ezzel párhuzamosan megjelent az igény olyan adaptív, tanulásra képes rendszerek iránt, amelyek képesek ismeretlen támadási minták felismerésére is. A mesterséges intelligencia (MI/AI) és azon belül a gépi tanulás (ML) lehetőséget kínál arra, hogy a hálózati viselkedést folyamatosan monitorozzuk. [20]

## Célkitűzés és hipotézis

Jelenlegi kutatásom célja gépi tanuláson alapuló megközelítések bemutatása hálózati forgalmi anomáliák észlelésére, figyelembe véve az algoritmikus hatékonyságot és a hálózati forgalom optimalizálás és AI alapú eszközkonfiguráció. A kutatás során különböző gépi tanulási algoritmusokat kívánok alkalmazni az anomáliadetektálás pontosságának és hatékonyságának javítása érdekében. Azt állítom, hogy a gépi tanulási algoritmusok pozitív hatással lehetnek a hálózati forgalmi anomáliák észlelésére.

Hogyan viszonyul a felügyelt és a felügyelet nélküli tanulás teljesítménye a hálózati adatok elemzésében?

A kutatás hipotézise az, hogy a mélytanulási modellek (pl. autoenkóderek, rekurzív neurális hálózatok) hatékonyabbak az összetett és rejtett anomáliák észlelésében, mint a hagyományos, szabályalapú vagy klasszikus gépi tanulási módszerek (pl. döntési fák,

SVM). A hálózati forgalom folyamatos növekedésével egyre nagyobb kihívást jelent a hálózati anomáliák, például a DDoS-támadások és a nem szándékos hálózati hibák időben történő észlelése. Az ilyen anomáliák veszélyeztethetik az informatikai rendszerek biztonságát és működését is. A hagyományos forgalomelemző rendszerek gyakran nem képesek hatékonyan észlelni a dinamikusan változó, ismeretlen támadásokat, mivel nem használnak adaptív algoritmusokat. Ezért gépi tanulási technikák alkalmazása szükséges a hálózati anomáliák észleléséhez. [4]

## MÓDSZERTAN

A kutatás során kvantitatív megközelítést alkalmazok. A kutatás során többféle gépi tanulási algoritmust fogok alkalmazni, beleértve a felügyelt és felügyelet nélküli tanulást, mint például a döntési fákat, k-means klaszterezést, illetve a mély tanulási modelleket, mint az autoencoder-eket és neurális hálózatokat. A hálózati forgalom elemzéséhez nyilvános adatokat fogok használni (például KDD99 vagy NSL-KDD), melyeket előfeldolgozott, hogy megfelelő bemeneteket kapjanak a modellek számára. [16]

A vizsgálathoz nyílt forrású hálózati forgalom-adatbázisokat használunk, például:

- **NSL-KDD** – kiegyensúlyozott hálózati forgalomadatok különféle támadásokkal
- **CICIDS2017** – modern, valósághű hálózati viselkedések és támadások. [16]

USN-NB15-komplex, új típusú hálózati fenyegetések. A felügyelt és felügyelet nélküli tanulást, mint például a döntési fákat, k-means klaszterezést, illetve a mély tanulási modelleket, mint az autóencodereket és neurális hálózatokat. Az NS-KDD az egyik legismertebb behatolásérzékelésre felkészített adatbázis. Több különböző informatikai hálózati forgalom van benne, amely normál és támadó pozíciót felvevő viselkedésre utaló jellemzők vannak.

A CICIDS2017 adatbázis a hálózati forgalomra van specializálva, modern támadási mintákat tartalmaz, ami hatékonyan használható és hálózati felderítésre alkalmazható a biztonsági intézkedések során, amely gyakorlatban is előfordulhatnak. Támadástípusok botnet, port scan, DDDoS, webes támadás, brute force. Több mint 80 attributúmal ad jellemzést az eseményről. Mélytanulásnál kiemeleten jól alkalmazható.

Az UNSW-NB15 az Australian Centre for Cyber Security által létrehozott adatbázis, amely tartalmaz modern támadási módszereket, a normál informatikai hálózati forgalom reprezentációjához alkalmas. 9 különböző támadási mintáét tartalmaz, pl: DoS, backdoor, shelcode. A hálózati esemény több mint 40 jellemzővel bír, az OSI modell alapján a hálózati réteg, csomaginformációk, és hálózati forgalmakat is tekintve kerülnek levonásra. Az adatbázis jól **alkalmazható gépi tanulásra, és alhálózat teljesítmény mérésére.** Azonban jobb választás lehet TON_IoT Datasets adatbázis, ami megfelel a kor szellemének és folyamatosan frissítik. Az adatbázis az MI-re van készítve hálózat támadások ellen. Többnyire logok és hálózati forgalom van benne. Támadástípusok amire alkalmas az adatbázis rendszerbeli alkalmazásra (injection,scanning, DoS, DDoS, ransomware). A modell alkalmas mélytanulásra.

**CSE-CIC-IDS2021**

Ez az adatbázis heterogén forgalomra is alkalmas, megfelel a modern támadási típusoknak pl. brute-force, SQL injection. Ennek segítségével valós hálózati környezetet tudunk szimulálni. Többdimenziós adattal rendelkezik, amit betanításra fel tudunk használni, mélytanulásra alkalmas az adatbázis. Számos helyen alkalmazzák. A következő támadástípusokat ismerjük: Brute-force (SSH, FTP), Web alapú támadások (XSS, SQL injection),Malware / RansomwareBotnet / Command and Control (C&C), Denial of Service (DoS, DDoS),Infiltration / Backdoor Phishing,Man-in-the-Middle (MITM), VPN-alapú elrejtett forgalmakat is kezel. Célunk, hogy az adatbázis segítségével alkalmazzuk a rendszerben a lehetséges adatbázis minták segítségével a hálózati sérülékenység és a támadás lehetőségét. Az NSL-KDD különféle hálózati forgalmakat tartalmaz, amelyeket normál és támadó viselkedésekre osztanak

## ALGORITMUSOK

Az algoritmusok fontos szerepe van a programok létrehozása során. Az alábbi táblázat tartalmazza azokat az algoritmus típusokat, amelyek felderíthetik az informatikai hálózat anomáliákat, amelynek jelentős hatása van a hálózat biztonságos működésében. Az alábbi 6 szempontot vizsgáltam meg, előnyök és hátrányokat is figyelembe véve, amely alapján besoroltam osztályzási szintet is. A táblázat jól összefoglalja melyik algoritmus milyen szempontokat helyez előtérbe, és annak alkalmazásának lehetőségét.

| | Algoritmus / módszer | Miért hasznos egy működő hálózat hibakezelésében? |
|---|---|---|
| 1 | Bayes-hálók (Bayesian Networks) | Hibák okainak valószínűségi modellezése (pl. router, kapcsolat, eszközhiba). Diagnózisban kiváló. |
| 2 | Reinforcement Learning (megerősítéses tanulás) | A rendszer tanul, hogyan javítsa ki önmagát – például útvonalváltás vagy újrakonfigurálás automatikusan. |
| 3 | Root Cause Analysis + Decision Trees | Hibák okainak automatikus feltérképezése szabály-alapú vagy tanuló döntési fákkal. |
| 4 | Autoencoder + hibajelzések monitorozása | Ismeretlen hibák és viselkedések feltárása automatikusan a hálózati viselkedésből. |
| 5 | LSTM (idősoros hálózati log elemzéshez) | Hálózati eseménysorokból időben felismeri, ha hibába fut a rendszer – megelőző figyelmeztetés/javítás. |
| 6. | Graph Neural Networks (GNN) | A hálózat mint gráf modelle zése. Képes lokalizálni, hogy a topológia mely pontján lép fel hiba. |
| 7. | Runbook Automation Anomaly Detection + | Pl. egy szabály-alapú motor (pl. Runbook Automation) az észlelt anomáliák automatikus orvoslására. |
| 8. | Predictive Maintenance modellek (ML alapú) | Előrejelzi, mikor és hol lesz esedékes egy hiba (pl. router túlterhelés, sávszélesség telítődés). |
| 9. | Configuration Drift Detection (pl. diff modellek) | Gépi tanulással figyeli, ha a konfiguráció eltér az optimálistól, és visszaállítja. |
| 10. | AI-Ops rendszerek (pl. IBM Watson, Moogsoft, Dynatrace) | Gépi tanulással figyelik, diagnosztizálják és javítják az IT infrastruktúra problémáit, valós időben. |

*1. táblázat Ajánlott algoritmusok és módszerek önjavító hálózati rendszerekhez, saját szerkesztés*

A fenti táblázatot az alábbi szempontok szerint osztályoztam vizsgálva a hatékonyságot is. A hálózati anomáliák felderítésében fontos, hogy a feladat specifikációjához mérten válaszunk algoritmust. Az alábbi táblázat jól összefoglalja az előnyöket és hátrányokat is, amely kutatásom egyik fő szempontja.

| | Algoritmus | Előnyök | Hátrányok |
|---|---|---|---|
| 1. | *Bayes-hálók* | *- Képes valószínűségi hibadiagnózisra<br>- Jól modellezi az ok-okozati kapcsolatokat* | *- Szükség van részletes hálózati modellezésre<br>- Nehéz karbantartani komplex rendszernél* |
| 2. | *Reinforcement Learning (RL)* | *Jól alkalmazható dinamikus hálózatokra<br>- Képes tanulni javító lépéseket* | *- Nehéz visszavonni hibás „döntéseket”<br>- Lassú tanulás, sok próbálkozás kell* |
| 3. | *Decision Tree / Root Cause Analysis* | *-Hatékony ismert hibák felismerésére<br>-egyszerű logikai struktúra* | *- Nehezen skálázható<br>- Új típusú hibák esetén nem működik jól* |
| 4. | *Autoencoder (deep learning)* | *-Ismeretlen hibákat is felismer<br>-Nem igényel címkézett adatot* | *-Csak azonosít, nem javít* |
| 5. | *LSTM (idősoros elemzéshez)* | *Előrejelezhetőek a hibák<br>Felismeri időbeli mintázatokat* | *Nehéz értelmezni és tréningezni<br>Sok adat kell* |
| 6. | *Graph Neural Network (GNN)* | *Lokalizálja a hibapontokat<br>A hálózat topológiáját természetesen modellezi* | *Nagy számítási igény<br>Fejlett implementáció szükséges* |
| 7. | Anomaly Detection + Runbook Automation | Szabályokkal jól kezelhető visszatérő hibák<br>Gyors beavatkozás | - Kézzel kell karbantartani a szabályokat<br>- Korlátozott rugalmasság |
| 8. | Predictive Maintenance (ML) | Csökkenti a leállásokat<br>Előre jelzi a hibákat | Pontos előrejelzéshez sok jó adat kell<br>- Csak ismétlődő, trendalapú hibáknál hasznos |
| 9. | Configuration Drift Detection | Könnyen automatizálható<br>- Megőrzi a hálózati állapot stabilitását | - Manuális beavatkozás szükséges lehet<br>- Nem minden hiba konfigurációs |
| 10. | AI-Ops rendszerek (pl. Moogsoft, Dynatrace, Watson) | Több technológiát integrál<br>- Komplett megoldás valós idejű és automatikus beavatkozással | -komplex bevezetés |

*2. táblázat Algoritmusok előnyök és hátrányok, saját szerkesztés*

## Hálózati algoritmusok értékelése kutatási elemzés alapján

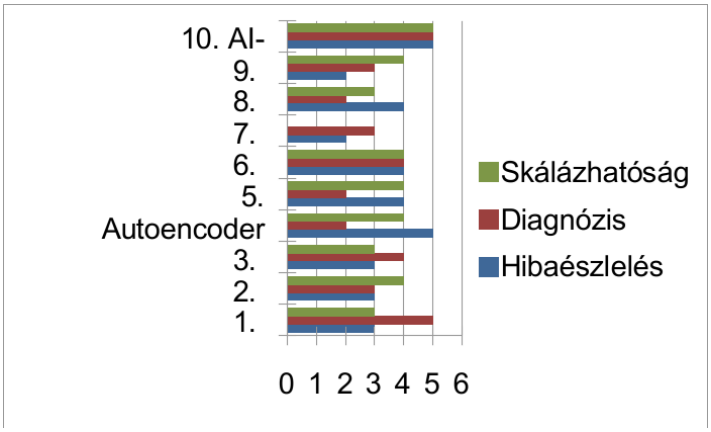
- Hibaészlelés pontossága, Diagnosztikai képesség (hiba okának azonosítása)
- Automatikus javítás lehetősége, Skálázhatóság (nagy hálózatokon való használhatóság)

**Magyarázhatóság (mennyire érthető az eredmény)** 1 = gyenge / nem jellemző, 5 = kiváló / erős képesség

| *Algoritmus / Módszer* | *Hibaészlelés* | *Diagnózis* | *Skálázhatóság* |
|---|---|---|---|
| *1. Bayes-hálók* | *3* | *5* | *3* |
| *2. Reinforcement Learning* | *3* | *3* | *4* |
| *3. Decision Tree* | *3* | *4* | *3* |
| *4. Autoencoder* | *5* | *2* | *4* |
| *5. LSTM (idősor)* | *4* | *2* | *4* |
| *6. Graph Neural Network* | *4* | *4* | *4* |
| *7. Runbook Automation* | *2* | *3* | *3* |
| *8. Predictive Maintenance* | *4* | *2* | *3* |
| *9. Config Drift Detection* | *2* | *3* | *4* |
| *10. AI-Ops rendszerek* | *5* | *5* | *5* |

*2. táblázat (algoritmusok osztályzás) saját szerkesztés*

Grafikonon ábrázolva:




*1. grafikon algoritmusok kiértékelése, saját szerkesztés*

## HÁLÓZATI FORGALOM OPTIMALIZÁLÁS

AI-algoritmusok képesek folyamatosan monitorozni a hálózati forgalmat, és automatikusan módosítani az adatátviteli irányokat, hogy csökkentsék a torlódásokat vagy op-

timalizálják a késleltetést. Ilyen algoritmusok például a gépi tanulás (ML) alapú forgalomelőrejelzés, amely segíthet a dinamikus útvonalválasztásban. A hálózati forgalom optimalizálására vizsgálat alá venném az alábbi algoritmusokat.

- **Reinforcement Learning (DRL, Q-learning)**,
- **LSTM**,
- **GNN**,

**Képesek optimalizálni a hálózati forgalmat**, **csökkenteni a torlódást**, **javítani a válaszidőt**, és **önálló döntéseket hozni** az adatútvonalakról – még **valós időben is**.

**Q -learning algoritmus**

Ez táblázatban tárolja az **állapot–akció értékeket (Q-értékeket).** Q(s, a) – megtanulja, hogy egy adott **állapotban (s)** melyik **akció (a)** a legjobb. Csak **kis mértékű problémákra** alkalmas, ahol az állapot- és akciótér nem túl nagy (pl. hálózat max. 10 csomópont).

**Reinforcement Learning (DRL, Q-learning)**,

A **Reinforcement Learning** egy gépi tanulási paradigma, amelyben egy **ügynök (agent)** tanul interakciók során, hogy maximális jutalmat (reward) szerezzen. Az ügynök nem rendelkezik előre meghatározott címkékkel vagy adatokkal, hanem **próbálgatásos alapú tanulással** javítja döntéseit. [11]

**Állapotok:**

- **Állapot (State, S)**: Az ügynök aktuális helyzete a környezetében. Minden környezet egy állapotot reprezentál (pl. egy robot helyzete egy szobában).
- **Cselekvés (Action, A)**: Az ügynök által választott döntés vagy művelet az adott állapotban.
- **Jutalom (Reward, R)**: A cselekvés eredményeként kapott visszajelzés. Az ügynök a cselekvését úgy választja meg, hogy a jutalmat maximalizálja.**Politika (Policy, π)**: Egy függvény, amely meghatározza, hogy egy adott állapotban az ügynök milyen cselekvést végezzen. A politika lehet determinisztikus vagy valószínűségi.

**Q-learning**

Q-learning célja, hogy megtanulja az ügynök számára optimális politikát anélkül, hogy tudnia kellene a környezet dinamikáját.

A Q-learning algoritmus egy **Q-táblát** épít fel, amely az egyes állapot-cselekvés párosokhoz rendelt **Q-értékeket** tartalmaz. Ezek a Q-értékek azt mérik, hogy az adott állapotban végrehajtott cselekvés milyen várható jutalmat eredményez a jövőben.

A **Q-érték** (Q(s, a)) az alábbi képlettel frissíthető:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left( R_{t+1} + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t) \right)$$

- **s_t**: Az aktuális állapot.
- **a_t**: Az aktuális cselekvés.
- **R_{t+1}**: A cselekvés által kapott jutalom.
- **α\alphaα**: A tanulási sebesség, amely meghatározza, hogy mennyire veszi figyelembe az új információkat.

- **γ\gammaγ**: A diszkontálási tényező, amely az **új jutalmak** és a **jövőbeli jutalmak** közötti súlyt szabályozza [19]

**LSTM(**Long Short-Term Memory) [17]

Az LTMS egy idősor alapú algoritmus, ami alkalmas arra, hogy a hálózati forgalmat előre jelezze. Segítségével a hálózati forgalmi mintázatokat alapján előrejelzést kaphatunk a várható forgalomról, sávszélesség, és késleltetésről. Vizsgálva az algoritmust az időbeli összefüggéseket jól fel lehet ismerni, és jó teljesítményt mutat nemlineáris mintázatok esetében és hatékonyan alkalmazható a hálózati forgalom torlódás előrejelzés, és csomagkésés jóslására. [12]

**Előnyök:**

- Stabil tanulási folyamatot képvisel
- Képesség a hosszú mintázatok felismerésére.
- Időbeli adatok kezelése

**Hátrány**

- Számítási erőforrás
- Skálázási nehézségek
- Nagy adatmennyiség szükséges a tanuláshoz.

## KÉPESSÉG A HÁLÓZATI ESZKÖZÖK ÖNÁLLÓ KONFIGURÁLÁSÁRA

Az AI képes önállóan beállítani a hálózati eszközöket, figyelembe véve a legfrissebb biztonsági szabványokat és az iparági legjobb gyakorlatokat, ezzel csökkentve az emberi hiba lehetőségét. A hálózati eszközöket kézzel előre megtervezett informatikai struktúra alapján konfiguráluk. Használhatunk hozzá különböző hálózat tervező programokat amelyek segítségével lemodellezhetjük a hálózat működését is. Azonban azt a lehetőség t vizsgálom hogyan lehetne gépi tanulási módszerekkel vizsgálni a hálózati biztonságot, felderíteni a behatolást és gépi tanulási módszerekkel védelmet is adni a hálózatnak.

## OPTIMALIZÁLT ERŐFORRÁS KEZELÉS

A modern számítógépes hálózatok, a felhőalapú rendszerek, mobilhálózatok, növekvő kihívás elé állnak a hatékonyság terén is. Az informatikai infrastruktúrában a felhasználók száma dinamikusan nőhet, és a hagyományos hálózati menedzsmentben lehet olyan eset amikor nem képes kielégíteni az elvárt teljesítményt, rugalmasságot és legfőbbképpen a minőséget. A kor vívmányait követve, alkalmazhatjuk az AI technológiát, azon belül a gépi tanulást, megerősítéses tanulást. Reinforcement Learning – RL) és a tartós memóriával rendelkező LSTM [17] és a neurális hálózatot is. Az optimális erőforráskezelés célja az, hogy jelen esetben egy infrastrukturális és adott hálózati topológiájú hálózatban az erőforrások leghatékonyabb leosztása, amely segíthet a szolgáltatás működésének minőségében. Ha az MI megközelítést nézzük akkor, a forgalmi mintázatok alapján képes előre jelezni a hálózati túlterheltséget, és a döntéseket képes létrehozni majd beavatkozni a hálózat működésében, míg a hagyományos hálózat működésében kézzel manuálisan avatkozunk be és javítjuk ki a hálózati hibát, míg az MI alkalmazása egy előrelátó működést , tanult minták alapján döntést hoz és javít a hálózatban. A másik út a megerősítéses tanulás amely egy

ügynök segítségével tanulja alhálózati forgalomirányítást minimális késleltetés, és veszteség mellett, de figyel a megfelelő sávszélességre, amelyben a lehető legnagyobbat veszi alapul. A hálózatban dinamikus újra leosztását az LSTM hálózatok segítségével tehetjük meg, amely lehetővé teszi a hálózati forgalom előrejelzését, a várható hálózati terhelést, és a késleltetés egy becslésé**t.** [17] A harmadik szempont a gráfalapú neurális hálózatok, amely képes lemodellezni az adott hálózat topológiáját, támogatást adva a hálózatban a döntéshozatalra. A gyakorlati szempontot az AI alapra helyezzük, amely egy hálózati menedzsmentrendszer feltételez, szükség van egy hálózat monitorozó modulra, amely gyűjti az információkat a hálózatról, (pl.: késleltetés, hálózati terheltség. Jump) amit a (LSTM) fog feldolgozni, a megerősítéses tanulási rendszer komponense DQN pedig döntéseket hozhat, és segíthet a hálózati anomáliák csökkentésében a döntések és végrehajtási események alapján pl: új forgalomirányitás, ACL, szabályok javaslata vagy végrehajtása során a hálózatban. [21] Az rendszer képes lehet a teljesítményen javítani, amely hatékonyságot mutathat hosszú távon. Az optimális hálózati kezelés kulcsszerepet játszik az MI által vezérelt hálózatokban, amely képes lehet különböző hálózati állapotok alapján reagálni és javítani és tanulni is, a múltbéli eseményekből. Az AI képes a hálózati erőforrások (például memória, CPU, sávszélesség) automatikus felosztására és optimalizálására annak érdekében, hogy a hálózat minden egyes eleme a legjobb teljesítményt nyújtsa. [17]

## KONKLÚZIÓ

A gépi tanulás alkalmazása a hálózati forgalomelemzésben ígéretes megoldás a dinamikusan változó támadások és anomáliák felismerésére, amelynek segítségével hatékonyabban beazonosítható az informatikai hálózati korábbról ismert vagy még nem ismert de érzékelhető hálózati fenyegetettség. Az algoritmusok segítségével és az MI is alkalmazva kiberbiztonsági szempontból védettebb informatikai rendszerhez juthatunk. A fenti táblázatokban felsorolt algoritmusok figyelembe véve az egyes előnyöket és hátrányokat is, egy jól összehangolt, és hatékony teljesítményű hálózatot is létre tudunk hozni. Attól függően, hogy mi a specifikáció, mi az, amit szeretnék megvalósítani kombinálhatjuk az algoritmusokat. Az osztályzás jól mutatja, hogy az előnyök és hátrányok alapján kimondható, hogy hatékonyságot érhetünk el a statikus algoritmusokhoz képest és figyelembe véve az emberi reakcióidőt is. A hálózati anomáliák jogosulatlan behatolások vagy hibás konfigurációk jelentős kockázatot jelentenek a szolgáltatások folyamatosságára és az adatok biztonságára nézve. Ha az emberi konfigurációt nézzük, a hálózat védelmét tűzfal konfigurációk, acl szabályok segítségével védik, itt azonban a kutatás arra irányul, hogy milyen módszerek és lehetőségeket lehetne használni a modern kor vívmányai alkalmazásával.

## ÖSSZEFOGLALÁS

A digitalizáció és a hálózati technológiák rohamos fejlődése új kihívásokat állít a kiberbiztonság elé. A hagyományos, szabályalapú védelmi rendszerek nem képesek hatékonyan reagálni a dinamikusan változó, előre nem ismert fenyegetésekre. A tanulmány célja annak bemutatása, hogy a mesterséges intelligencia, különösen a gépi tanulási algoritmusok miként alkalmazhatók hatékonyan a hálózati anomáliák észlelésére, előrejelzésére és megelőzésére. A kutatás során különböző gépi tanulási modelleket, köztük autoencodereket, döntési fákat, megerősítéses tanulást és gráfalapú neurális hálózatokat vizsgáltunk, azok

előnyeivel, hátrányaival és alkalmazhatóságukkal együtt. A tanulmány részletesen bemutatja az egyes algoritmusok diagnosztikai képességeit, skálázhatóságát, valamint azt, hogy mennyire képesek támogatni az automatizált hibajavítást. A dolgozatban bemutatásra kerültek nyílt forráskódú adatbázisok (NSL-KDD, CICIDS2017, UNSW-NB15) alapján végzett elemzések, amelyek igazolják, hogy az AI-alapú rendszerek jelentősen javíthatják a hálózati biztonságot. Emellett kiemelésre került az AI szerepe a forgalom optimalizálásában, az önálló eszközkonfigurációban és az erőforrások hatékony kezelésében is. A kutatás megállapításai szerint a gépi tanulási technikák alkalmazása nemcsak a biztonsági fenyegetések pontosabb azonosítását teszi lehetővé, hanem a hálózatok proaktív, önjavító működésének alapját is képezheti. Ezáltal hozzájárulnak a megbízhatóbb, rugalmasabb és jövőállóbb informatikai rendszerek kialakításához.

## FELHASZNÁLT IRODALOM

[1] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 108–116. https://doi.org/10.5220/0006639801080116

[2] Ring, M., Wunderlich, S., Scheel, C., Landes, D., & Hotho, A. (2019). A Survey of Network-based Intrusion Detection Data Sets. *Computers & Security*, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.008

[3] Canadian Institute for Cybersecurity. (2021). CSE-CIC-IDS2021 Dataset. *University of New Brunswick*. https://www.unb.ca/cic/datasets/ids-2021.html

[4] Moustafa, N., Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). *Military Communications and Information Systems Conference (MilCIS)*. https://doi.org/10.1109/MilCIS.2015.7348942

[5] Ferrag, M. A., Maglaras, L., Derhab, A., Mukherjee, M., & Janicke, H. (2020). Security for 5G and Beyond. *IEEE Communications Surveys & Tutorials*, 22(1), 196–248. https://doi.org/10.1109/COMST.2019.2951818

[6] Umer, M. F., Sher, M., Bi, Y., & Debar, H. (2022). Evaluating Deep Learning for Network Intrusion Detection: Benchmarks, Datasets, and Metrics. *Applied Sciences*, 12(3), 1458.

[7] Diro, A. A., & Chilamkurti, N. (2018). Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.

[8] Krasznay Csaba, Bencsáth Boldizsár, Kiberbiztonság alapjai, Hálózati támadások, megelőzés, behatolás-észlelés, incidenskezelés, Nemzeti Közszolgálati Egyetem, 2021

[9] Gál Zsolt, Kriptográfia, hálózati biztonság, kockázatelemzés, Typotex, 2017

[10] Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning MIT Press 2016

[11] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, MIT Press (2018)

[12] François Chollet , Deep Learning with Python, Manning Publications 2017 Using LSTMs to Predict the Next Word 6. chapter 185.
[13] William Stallings, Network Security Essentials, Pearson, 2009
[14] Aiko Pras, Paul C. van Oorschot , DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Mitigation 2014
[15] Ivan Nikolaev, Hands-On Network Security with Python: Implementing Real-Time Network Traffic Analysis and Intrusion Detection, Packt Publishing, 2020
[16] Stefan A. W. S. V. G. Gattaca, Machine Learning and Data Science in Cybersecurity: A Practical Guide to Real-World Solutions, Wiley, 2023
[17] Ian Goodfellow, Yoshua Bengio, Aaron Courville , Deep Learning, MIT Press, 2016
[18] S. Chakrabarti, S. N. Balakrishnan, R. Krishna , Deep Learning for Graphs, Springer, 2020
[19] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, MIT Press, 2018 second press
[20] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley(2011)
[21] Maxim Lapan , Deep Reinforcement Learning Hands-On, Packt Publishing 2018

DOI: https://doi.org/10.12700/btsz.2025.7.3.179

# ARTIFICIAL INTELLIGENCE IN EVERYDAY LIFE: APPLICATION AREAS AND GENERATIONAL CHARACTERISTICS BASED ON THE RESULTS OF A PRIMARY RESEARCH

# MESTERSÉGES INTELLIGENCIA A MINDENNAPOKBAN: ALKALMAZÁSI TERÜLETEK ÉS GENERÁCIÓS SAJÁTOSSÁGOK EGY PRIMER KUTATÁS EREDMÉNYEI ALAPJÁN

BERÉNYI Csaba[1] – CSISZÁRIK-KOCSIR Ágnes[2]

**Abstract**

Artificial intelligence is playing an increasingly important role in education, research, information processing, and digital interactions. This study examines the use of AI-based solutions across generational differences. The research covers ten areas of application, including language learning, data collection, information summarization, source searching, translation, essay writing, and role-playing. We measured the intensity of AI use on a five-point Likert scale, allowing for statistical analysis of differences between generations. AI is most commonly used for language learning, research, and resource search, while role-playing and essay writing are less common. Generational differences are clearly observable: while Generation Z uses AI more intensively in all areas examined, Generations X and Y primarily use these technologies for professional and research purposes. Our results highlight that the prevalence and functional diversity of AI use is closely related to generational characteristics.

**Keywords**

artificial intelligence, AI usage, education, learning, generational differences

**Absztrakt**

A mesterséges intelligencia egyre jelentősebb szerepet tölt be az oktatásban, kutatásban, információfeldolgozásban és digitális interakciókban. Jelen tanulmány az MI-alapú megoldások generációs különbségek mentén történő használatát vizsgálja. A kutatás tíz alkalmazási területet ölel fel, többek között nyelvtanulás, adatgyűjtés, információk összegzése, forráskeresés, fordítás, esszéírás és szerepjáték. Ötfokozatú Likert-skálával mértük az MI-használat intenzitását, lehetőséget adva a generációk közötti eltérések statisztikai vizsgálatára. Az MI-t leggyakrabban nyelvtanulás, kutatás és forráskeresés céljából alkalmazzák, míg a szerepjáték és esszéírás ritkább. A generációs különbségek egyértelműen megfigyelhetők: míg a Z generáció az összes vizsgált területen intenzívebben alkalmazza az MI-t, addig az X és Y generációk elsősorban szakmai és kutatási célokra használják ezeket a technológiákat. Eredményeink rávilágítanak arra, hogy az MI-használat elterjedtsége és funkcionális sokfélesége szorosan összefügg a generációs sajátosságokkal.

**Kulcsszavak**

mesterséges intelligencia, MI használat, oktatás, tanulás, generációs különbségek

[1] berenyi.csaba@kgk.uni-obuda.hu | ORCID: 0009-0008-9461-9889 | Assistant Lecturer, Óbuda University Keleti Károly Faculty of Business and Management | Egyetemi tanársegéd, Óbudai Egyetem, Keleti Károly Gazdasági Kar

[2] kocsir.agnes@kgk.uni-obuda.hu | ORCID: 0000-0001-5454-7843 | Professor, Óbuda University Keleti Károly Faculty of Business and Management | Egyetemi tanár, Óbudai Egyetem, Keleti Károly Gazdasági Kar

## BEVEZETÉS

Az elmúlt évtizedek technológiai fejlődése nemcsak az ipari és gazdasági szektorokat alakította át gyökeresen, hanem az egyének hétköznapi életét is jelentősen befolyásolta. A digitális eszközök, a globális hálózatok és az automatizált rendszerek mind hozzájárultak egy új, információalapú társadalom kialakulásához. E folyamat egyik legújabb és legmeghatározóbb eleme a mesterséges intelligencia (MI), amelynek hatása már nem csupán a technológiai szakértők világában érezhető, hanem a laikus felhasználók körében is mindennapossá vált. Míg az ipari forradalom gépesítette a fizikai munkát, a mesterséges intelligencia napjainkban a szellemi és kreatív tevékenységek digitalizálásának és automatizálásának élharcosa.

Az MI rendszerek képesek tanulni, alkalmazkodni, és egyre összetettebb feladatokat végezni emberi beavatkozás nélkül – legyen szó szövegek generálásáról, képelemzésről, vagy akár személyre szabott tanácsadásról. E jelenség azonban nem minden társadalmi csoportot érint egyformán. A technológiához való hozzáférés, a használat módja, illetve az MI-vel kapcsolatos elvárások és félelmek jelentős eltéréseket mutathatnak generációs szinten. Különösen érdekes kérdés, hogy miként viszonyulnak az egyes korcsoportok az MI kínálta lehetőségekhez, és mely élethelyzetekben hajlandóak azt ténylegesen használni. A jelen tanulmány nem csupán az MI alkalmazási területeinek feltérképezésére törekszik, hanem arra is, hogy feltárja a generációs különbségeket ezen technológia mindennapi használatában. Az ilyen jellegű kutatások nemcsak a társadalmi tendenciák jobb megértését segítik elő, hanem alapot adhatnak az oktatás, a technológiai fejlesztés és a közpolitika számára is, hogy hatékonyabban reagáljanak a digitális korszak kihívásaira.

## SZAKIRODALMI ÁTTEKINTÉS

A mesterséges intelligencia (MI) az a képesség, amely lehetővé teszi a számítógépes rendszerek számára, hogy olyan feladatokat hajtsanak végre, amelyek normál esetben emberi intelligenciát igényelnének, mint például a tanulás, érvelés, problémamegoldás és nyelvi megértés [1]. Haenlein és Kaplan [2] szerint az MI történeti gyökerei az 1950-es évekre vezethetők vissza, amikor Alan Turing felvetette, hogy vajon a gépek képesek lehetnek-e gondolkodni. A mesterséges intelligencia kifejezés eredetét John McCarthy 1956-os munkájához kötik, aki az MI-t a számítástechnika olyan ágaként határozta meg, amely az emberi viselkedés szimulálására képes rendszerek létrehozását vizsgálja [2] [3]. A mesterséges intelligencia az 1950-es évektől számít önálló tudományos területnek, ám hosszú időn keresztül csak szűk körben keltett érdeklődést, és gyakorlati felhasználása is csekély volt. Azonban a Big Data elterjedése, valamint a számítási teljesítmény jelentős növekedése következtében napjainkra az MI meghatározó szereplővé vált mind az üzleti szektorban, mind a társadalmi diskurzusban. A mesterséges intelligencia fogalma dinamikusan alakul, mivel a technológiai fejlődés során az egykor intelligensnek tartott megoldások hétköznapivá válnak – ezt a jelenséget AI-hatásként tartják számon [2].

Bár az MI rokon terület a pszichológiával – amely az emberi gondolkodás természetét tanulmányozza –, az MI elsősorban a számítási folyamatokra fókuszál, különös tekintettel az érzékelés, a logikai következtetés és a döntéshozatal gépi modelljeire. Ezen túlmenően az MI megkülönböztethető a klasszikus számítástechnikától is, amely többnyire

determinisztikus feladatok végrehajtására irányul, míg az MI célja az adaptív, „intelligens" viselkedés megvalósítása [1] [2].

Az intelligenciát gyakran úgy értelmezik, mint azt a készséget, amely lehetővé teszi az ismeretek elsajátítását, azok feldolgozását és gyakorlati felhasználását bonyolult feladatok megoldása érdekében. Az MI célja olyan algoritmusok és modellek fejlesztése, amelyek lehetővé teszik a számítógépek számára, hogy érzékeljenek, gondolkodjanak és reagáljanak a környezetükre – azaz képesek legyenek döntéseket hozni és tanulni tapasztalataikból [4]. Az MI folyamatosan fejlődik és több fejlődési hullámon ment keresztül, napjainkban a gépi tanulás és a mélytanulás áll a kutatások középpontjában [5] [6].

Az MI gyors elterjedése számos társadalmi és etikai kérdést vet fel. Dignum [7] kiemeli, hogy az MI rendszerek fejlesztésének felelősségteljes módon kell történnie, figyelembe véve az átláthatóság, a méltányosság és az adatvédelem és biztonság számos kérdését és szempontjait [8]. Mittelstadt et al. [9] szerint a „fekete doboz" rendszerek problémája, vagyis az algoritmusok működésének átláthatatlansága, különösen komoly kockázatokat jelent a társadalmi bizalom szempontjából. Rai [10] hangsúlyozza az úgynevezett „magyarázható MI" jelentőségét, amely elősegítheti, hogy a felhasználók jobban megértsék és elfogadják az MI által hozott döntéseket. Jordan és Mitchell hangsúlyozzák, hogy a gépi tanulás, mint a mesterséges intelligencia egyik központi eleme, nemcsak technológiai fejlődést jelent, hanem mélyreható gazdasági és társadalmi hatásokkal is jár, mivel egyre több ágazatban válik kulcsfontosságúvá az adatalapú döntéshozatal és az automatizáció támogatásában [11].

A mesterséges intelligencia meghatározó technológiai tényezővé vált a 21. században, jelentős hatást gyakorolva az oktatásra, az egészségügyre, az üzleti szférára és a társadalmi kapcsolatokra, nem beszélve az innovációk lehetőségeiről az élet minden területén [12] [13] [14]. Az oktatás területén lehetőséget biztosít személyre szabott tanulási élmények megvalósítására, prediktív analitikára és adminisztratív folyamatok automatizálására [15] [16]. A mesterséges intelligencia jelentős támogatást nyújthat a hallgatók, oktatók, intézményi adminisztrátorok és kutatók számára, ezért elengedhetetlen, hogy a felsőoktatási rendszer szerves részévé váljon [17]. Chatterjee és Bhattacharjee [18] kutatásukban kimutatták, hogy az MI-alapú oktatási rendszerek pozitív hatással vannak a tanulási hatékonyságra, különösen a felsőoktatásban. A mesterséges intelligencia képes nagy mennyiségű orvosi adat elemzésére, döntéshozatalra és tanulásra, ezáltal javítva a diagnosztika, a kezelés, valamint az egészségügyi ellátás hatékonyságát és pontosságát, különösen a modern orvoslásban és az egészségügyi hiányosságok pótlásában, valamint a személyre szabott orvosi kezelések kialakítását teszi lehetővé [19]. Üzleti környezetben az MI automatizálja a döntéshozatali folyamatokat, növeli a termelékenységet és elősegíti az ügyfélkapcsolatok hatékonyabb kezelését [20] [21]. A kis- és középvállalkozások gazdasági jelentősége szorosan összefügg innovációs képességükkel [22], amely napjainkban a digitalizáció és a mesterséges intelligencia alkalmazása révén válhat még hangsúlyosabbá [23], különösen azon generációk esetében, amelyek nyitottabbak az új technológiák bevezetésére.

A technológia elfogadásának és használatának mintázatai jelentős eltéréseket mutatnak generációs szinten. A digitális bennszülöttek (Z és Y generáció) természetesebben mozognak az MI által kínált környezetekben, míg a digitális bevándorlók (X generáció és idősebbek) óvatosabban közelítenek ezen technológiákhoz [24]. A demográfiai tényezők,

mint az életkor, jelentős szerepet játszanak az MI-technológiák elfogadásában, mivel a fiatalabb fogyasztók nyitottabbak az ilyen innovációkra, míg az idősebbek körében nagyobb fokú óvatosság figyelhető meg [25]. A digitális technológiák elfogadásának jelentős lökést adott a koronavírus válság miatti digitális kényszer is, mint külső kényszerítő erő [26]. Az információs technológia elfogadását olyan tényezők befolyásolják, mint a teljesítményvárakozás, az erőfeszítés elvárása, a társas hatás, valamint az egyéni tapasztalat [27]. A fiatalabb korosztályok kedvezőbben viszonyulnak a mesterséges intelligenciához, és nagyobb bizalommal tekintenek annak jövőbeli előnyeire, mint az idősebbek [28]. A generációk közötti különbségek nemcsak a technológiai jártasságban, hanem a technológiai újításokkal szembeni attitűdökben is jelentkeznek, ami jelentős hatással van a technológia elfogadására [29]. A különböző generációk eltérő mértékben és módon használják az MI-t, ami kihívásokat és lehetőségeket egyaránt jelent a fejlesztők és a döntéshozók számára. A technológia felelős alkalmazása, valamint a társadalmi különbségek figyelembevétele elengedhetetlen az MI fenntartható integrációjához [30].

Gazdasági és társadalmi szinten azok az országok élvezhetnek előnyt, amelyek időben felismerik az MI-ben rejlő lehetőségeket, és integrálják azt különböző ágazataikba, mint például az ipar, a szolgáltatások, az egészségügy vagy az oktatás, mivel ez növelheti termelékenységüket, ösztönözheti az innovációt, és hosszú távon hozzájárulhat a jóléti szintek emelkedéséhez. A mesterséges intelligencia hatása a munkaerőpiacra szintén jelentős, különösen a rutinjellegű, ismétlődő munkakörök automatizálása révén [31]. Az MI technológiák adaptálása nem csupán a gazdasági növekedés motorjaként szolgálhat, hanem átalakíthatja a munkaerőpiacot, új foglalkozások létrejöttét eredményezve, miközben egyes rutinszerű feladatok automatizálása kihívásokat jelenthet a munkavállalók számára, különösen azokban a szektorokban, ahol az emberi munka könnyen kiváltható [32].

A mesterséges intelligencia technológiák használata generációk szerint jelentős eltéréseket mutat, amelyeket a technológiai jártasság, a hozzáférés, valamint az attitűdök és az önhatékonyság érzete egyaránt befolyásol. A fiatalabb generációk – különösen a Z és Y generáció – nagyobb gyakorisággal és magabiztossággal alkalmazzák az MI-t, köszönhetően a digitális környezetben szerzett tapasztalataiknak és az új technológiák iránti nyitottságuknak [33]. Ezzel szemben az idősebb generációk, mint az X generáció és a baby boomerek, jellemzően visszafogottabban használják ezeket a rendszereket, és főként praktikus, munkához vagy egészségügyhöz kötődő célokra alkalmazzák őket [34].

A generációs különbségek megértéséhez fontos figyelembe venni az észlelt önhatékonyság és az újdonságokkal szembeni bizalom szerepét is. Az idősebb felnőttek esetében az új technológiák iránti bizalom alacsonyabb, ami korlátozhatja az MI elfogadását, míg a fiatalabbak körében az adaptáció gyorsabb és pozitívabb. Ezek az eltérések alapvető fontosságúak az MI-alapú rendszerek fejlesztése szempontjából, különösen akkor, ha cél az egyenlő hozzáférés biztosítása minden korcsoport számára [35].

## ANYAG ÉS MÓDSZER

Jelen tanulmányunkban azt vizsgáljuk, hogy a különböző generációk hogyan viszonyulnak az AI eszközökhöz, mire használják azokat a mindennapi életük során. Ehhez egy összetett, több témakört érintő kérdőívet alkalmaztunk, amelyet online formában, Google Űrlapok segítségével töltöttek ki a válaszadók. A kutatás során hólabda módszert alkalmaztunk magvakkal. A hólabda módszer magvakkal egy speciális mintavételi technika, amelyet

főként nehezen elérhető vagy rejtett populációk vizsgálatára alkalmaznak. A módszer lényege, hogy a kutatás kiindulópontjaként néhány, előre kiválasztott résztvevőt vonunk be a mintába. Ezek a magok olyan személyek voltak a kutatás során, akik releváns ismeretekkel, kapcsolatokkal vagy tapasztalatokkal rendelkeznek a vizsgált közösségen belül. A kiválasztott módszernek köszönhetően a kutatásba minden generációt sikerült bevonnunk, a minél szélesebb körű képalkotás érdekében. A kutatás 2024 év végén zajlott, és összesen 6574 értékelhető kérdőív alapján vontuk le következtetéseinket. Jelen tanulmányban vizsgált felmérés egy ötfokozatú skála segítségével történt, ahol az AI eszközök alkalmazásának területeit mérte fel. A skála legalsó vége a „soha" válasznak felelt meg (0-s érték), a teteje pedig a „mindig" választ jelentette (75-100%-os érték mentén). A jelen munkánk során elsőként megvizsgáltuk az adatokat a Cronbach-Alfa együttható alapján. A Cronbach-Alfa egy statisztikai mutató, amelyet arra használnak, hogy felmérjék egy kérdőív vagy teszt belső megbízhatóságát. Az együttható értéke 0,906 volt, ami azt mutatja, hogy az adatok kiválóan alkalmasak az elemzésre. A minta összetételét az alábbi ábra szemlélteti.

| Generációk | Megoszlás |
|---|---|
| BB generáció (1940 - 1964) | 5,0 |
| X generáció (1965-1979) | 21,4 |
| Y generáció (1980-1994) | 19,5 |
| Z generáció (1995 - 2007) | 50,7 |
| Alfa generáció (2008-) | 3,4 |

*1. Táblázat: A minta összetétele, Saját kutatás, 2024, N = 6574*

## EREDMÉNYEK

Első lépésként az alkalmazás gyakoriságának átlagértékeit vettük górcső alá. Érdekes tény, hogy az ötfokozatú skálán egyetlen kiugró értékkel bíró területet sem tudtunk azonosítani, így elmondható, hogy egyelőre, a 2024-es adatok alapján a válaszadóink még nem hagyatkoznak erősen az AI tanácsaira, megoldásaira.

A kapott eredmények alapján látható, hogy a kutatás és adatgyűjtés területe mutatja a legmagasabb alkalmazási gyakoriságot 2,763-as átlagértékkel. Ez nem meglepő eredmény, hiszen az AI eszközök kiválóan alkalmasak a nagy mennyiségű információ gyors feldolgozására, releváns források azonosítására és adatok strukturált összegyűjtésére. A magas átlagérték arra utal, hogy a válaszadók felismerték az AI hatékonyságát a kutatási folyamatokban, remélve, hogy emellé kritikus gondolkodás és szemlélet is társul az adatok megfelelő értelmezése érdekében. A második legmagasabb értéket az adott anyag összefoglalása kategória érte el 2,711-es átlaggal. Ez szintén elvárható eredménynek mondható, mivel az AI kiválóan alkalmas hosszabb szövegek lényegi elemeinek kiemelésére és tömör összefoglalók készítésére. A harmadik helyen a fordítási feladatok állnak 2,548-as átlagértékkel. Az AI-alapú fordítóeszközök jelentős fejlődésen mentek keresztül az elmúlt években, és ma már sokkal pontosabb és természetesebb fordításokat képesek produkálni, mint korábbi változataik. Ez magyarázza a viszonylag magas alkalmazási gyakoriságot, amelyet a kutatási eredményeink is hoztak.

A legalacsonyabb értékek szempontjából azt tapasztaltuk, hogy a szerepjáték kategória mutatja a legalacsonyabb alkalmazási gyakoriságot mindössze 1,965-os átlagértékkel.

Az eredmény itt sem meglepő, hiszen a szerepjátékok specifikus, kreatív és személyes interakciót igénylő tevékenységek, amelyben a válaszadók nem igazán látják az AI szerepét és fontosságát. Az egészség és fitnesz tanácsok területe a második legalacsonyabb értéket mutatja 2,212-es átlaggal. Itt valószínűleg az óvatosság és a bizalmatlanság játszik szerepet, mivel az egészségügyi tanácsok komoly következményekkel járhatnak, ha azok nem megfelelő forrásból származnak, és sok felhasználó inkább szakértőket keresi hasonló esetekben. Az utazás szervezés 2,259-es átlagértékkel a harmadik legalacsonyabb kategória. Bár az AI hasznos lehet útvonaltervezésben és helyszínkeresésben, azonban az utazás szervezése gyakran személyes preferenciák mentén történik, saját gondolatok és döntések mentén.

A középmezőnyben található kategóriák - mint a házi feladat megírása (2,467), irodalmi források keresése (2,402), dolgozat és esszé írás (2,434), valamint a nyelvtanulás (2,342) - mind az oktatási szférához kötődnek, ami az AI elterjedtségére és térhódítására enged következtetni az tanulmányok során.

A szórásértékek viszonylag homogénnek tekinthetők, 1,225 és 1,365 között mozognak. A legalacsonyabb szórást a szerepjáték (1,225) és az egészség és fitnesz tanácsok (1,240) mutatják, ami arra utal, hogy ezekben a kategóriákban a válaszadók véleménye viszonylag egységes volt. A legmagasabb szórás az adott anyag összefoglalása kategóriánál figyelhető meg (1,365), ami nagyobb véleményszóródást jelez a felhasználók között. Összességében azonban a szórásértékek nem mutatnak extrém eltéréseket, ami a minta konzisztenciájára utal.

| | Átlag | Szórás |
|---|---|---|
| Nyelvtanulás | 2,342 | 1,284 |
| Kutatás és adatgyűjtés | 2,763 | 1,305 |
| Egészség és fitnesz tanácsok | 2,212 | 1,240 |
| Utazás szervezés | 2,259 | 1,280 |
| Adott anyag összefoglalása | 2,711 | 1,365 |
| Házi feladat megírása | 2,467 | 1,333 |
| Irodalmi források keresése | 2,402 | 1,305 |
| Fordítási feladatok | 2,548 | 1,334 |
| Szerepjáték | 1,965 | 1,225 |
| Dolgozat, esszé írás | 2,434 | 1,339 |

*2. táblázat: Az AI alkalmazási területei és az alkalmazási gyakoriság átlaga és szórása a válaszadók véleménye alapján, Forrás: saját kutatás, 2024, N = 6574*

A továbbiakban a kapott eredményeket kívánjuk bemutatni generációnkénti bontásban. A vizsgált adatok generációk szerinti elemzése számos érdekes mintát tárt fel az alapkompetenciák és a digitális magatartás területén. A következőkben részletesen megvizsgáljuk az egyes generációk átlagértékeit, kiemelve azokat a kategóriákat, ahol az egyes csoportok a mintaátlag felett teljesítettek (pirossal jelölve).

A Baby Boomer (BB) generáció adatai alapján az AI alkalmazásának gyakorisága minden területen a legalacsonyabb vagy az egyik legalacsonyabb értéket mutatja a többi generációhoz képest. Kiemelkedően alacsony az AI használata nyelvtanulásban (2,064), egészség- és fitnesz tanácsokban (2,268), valamint dolgozat, esszé írásban (2,171). Ez arra utal, hogy a BB generáció tagjai – életkoruknál fogva – kevésbé integrálják az AI-t a mindennapi életükbe. Az adatok alapján a legmagasabb értékeket kutatás és adatgyűjtés (2,338), valamint utazás szervezés (2,329) területén mutatják, de ezek is elmaradnak a fiatalabb generációk átlagától. Az alacsony értékek mögött feltételezhetően technológiai szkepticizmus, digitális készségek hiánya, illetve az AI-alkalmazások iránti bizalmatlanság állhat. A BB generáció tehát inkább hagyományos módszereket preferál, és az AI-t csak korlátozottan vonja be a mindennapi tevékenységeibe.

Az X generáció tagjai már valamivel nyitottabbak az AI alkalmazására, de továbbra is mérsékelt értékeket mutatnak. A legmagasabb átlagot kutatás és adatgyűjtés (2,339), valamint nyelvtanulás (2,108) területén érik el, de ezek az értékek még mindig elmaradnak a fiatalabb generációkétól. Az egészség- és fitnesz tanácsok (2,011), utazás szervezés (2,150) és dolgozatírás (1,954) terén különösen alacsony az AI használatának gyakorisága. Ez azt mutatja, hogy az X generáció ugyan már ismeri és használja az AI-t, de inkább információgyűjtésre, kevésbé kreatív vagy komplex feladatokra alkalmazza. Az AI-tól való távolságtartás esetükben is érzékelhető, bár a digitális eszközök használata már természetesebb számukra, mint a BB generáció esetében.

A Y generáció (más néven millenniumi generáció) már jóval aktívabban használja az AI-t, különösen a kutatás és adatgyűjtés (2,635), nyelvtanulás (2,422), valamint irodalmi források keresése (2,473) területén. Ezek az értékek jelentősen magasabbak, mint az idősebb generációknál tapasztaltak. Az AI alkalmazása házi feladat megírásában (2,447) és dolgozatírásban (2,261) is erőteljesebb, ami arra utal, hogy a Y generáció tagjai már bátrabban támaszkodnak az AI-ra tanulmányaik és munkájuk során, magabiztosabbak és elfogadóbbak iránta. Az egészség- és fitnesz tanácsok (2,226) és utazás szervezés (2,311) területén is aktívabbak, de ezekben a kategóriákban még nem érik el a legfiatalabb generációk szintjét.

A Z generáció adatai alapján az AI alkalmazásának gyakorisága szinte minden területen magasabb, mint az idősebb generációknál. Kiemelkedően magas értékeket mutatnak nyelvtanulásban (2,413), kutatás és adatgyűjtésben (3,013), egészség- és fitnesz tanácsokban (2,261), valamint dolgozatírásban (2,698). Ez azt jelzi, hogy a Z generáció tagjai már teljes mértékben integrálják az AI-t a tanulási folyamataikba és a mindennapi életükbe. Az AI-t nemcsak információgyűjtésre, hanem kreatív, szervezési és problémamegoldó feladatokra is használják. Az adatok alapján a legmagasabb értékeket kutatás és adatgyűjtés, illetve dolgozatírás területén érik el, ami arra utal, hogy az AI-t a tanulmányi teljesítményük javítására is aktívan alkalmazzák. A Z generáció tehát digitális bennszülöttként magabiztosan és sokoldalúan használja az AI-t. Ez a tény azonban veszélyeket is jelent, hiszen nem biztos, hogy fiatal koruknál fogva rendelkeznek azokkal a képességekkel, melyeknek köszönhetően kritikusan, fenntartásokkal tudják kezelni az általa mondottakat. Mindezt az is bizonyítja, hogy itt jelenik meg elsőként a 3-as feletti átlagérték, ami a használat magasabb gyakoriságára utal.

Az Alfa generáció, vagyis a legfiatalabbak körében a legmagasabb az AI alkalmazásának gyakorisága szinte minden vizsgált területen. Kiemelkedő értékeket látunk nyelvtanulásban (2,728), kutatás és adatgyűjtésben (3,054), egészség- és fitnesz tanácsokban (2,594), utazás szervezésben (2,585), valamint dolgozatírásban (2,983). Ezek az értékek messze meghaladják az összes többi generáció átlagát. Az Alfa generáció tagjai már magától értetődő módon használják az AI-t a tanulás, szervezés, kreatív és mindennapi problémák megoldására. Az AI alkalmazása náluk nemcsak gyakori, hanem sokszínű is: a nyelvtanulástól kezdve a házi feladat megírásán át a szerepjátékokig szinte minden területen jelen van. Ez a generáció már digitális környezetben szocializálódott, így az AI-t természetes eszközként használja, amely szervesen beépült a mindennapjaikba.

| | Nyelvtanulás | Kutatás és adatgyűjtés | Egészség és fitnesz tanácsok | Utazás szervezés | Adott anyag összefoglalása | Házi feladat megírása | Irodalmi források keresése | Fordítási feladatok | Szerepjáték | Dolgozat, esszé írás |
|---|---|---|---|---|---|---|---|---|---|---|
| BB generáció (1940 - 1964) | 2,064 | 2,338 | 2,268 | 2,329 | 2,317 | 2,223 | 2,284 | 2,448 | 2,049 | 2,171 |
| X generáció (1965-1979) | 2,108 | 2,339 | 2,011 | 2,150 | 2,266 | 1,945 | 2,138 | 2,403 | 1,766 | 1,954 |
| Y generáció (1980-1994) | 2,422 | 2,635 | 2,226 | 2,311 | 2,516 | 2,225 | 2,279 | 2,573 | 1,988 | 2,261 |
| Z generáció (1995 - 2007) | 2,413 | 3,013 | 2,261 | 2,256 | 2,997 | 2,779 | 2,554 | 2,598 | 1,997 | 2,698 |
| Alfa generáció (2008-) | 2,728 | 3,054 | 2,594 | 2,585 | 2,951 | 2,871 | 2,683 | 2,701 | 2,478 | 2,897 |
| Total | 2,342 | 2,763 | 2,212 | 2,259 | 2,711 | 2,467 | 2,402 | 2,548 | 1,965 | 2,434 |

*3. táblázat: Az AI alkalmazási területei és az alkalmazási gyakoriságának átlaga generációs bontásban*
*Forrás: saját kutatás, 2024, N = 6574*

A fenti összefüggések mentén kíváncsiak voltunk arra is, hogy az egyes használati területek statisztikailag összefüggésbe hozhatók-e a válaszadók életkorával. A szignifikancia értéke alapján egyértelműen bizonyítást nyert, hogy a generációs hovatartozás mérhető szignifikáns hatással van az AI használatára.

| | | Négyzetek összege | df | Négyzet középérték | F | Sig. |
|---|---|---|---|---|---|---|
| Nyelvtanulás | Csoportok között | 160,480 | 4 | 40,120 | 24,673 | 0,000 |
| | Csoportokon belül | 10681,756 | 6569 | 1,626 | | |
| | Total | 10842,236 | 6573 | | | |
| Kutatás és adatgyűjtés | Csoportok között | 559,330 | 4 | 139,833 | 86,339 | 0,000 |
| | Csoportokon belül | 10639,009 | 6569 | 1,620 | | |

| | | Négyzetek összege | df | Négyzet középérték | F | Sig. |
|---|---|---|---|---|---|---|
| | Total | 11198,340 | 6573 | | | |
| Egészség és fitnesz tanácsok | Csoportok között | 98,915 | 4 | 24,729 | 16,239 | 0,000 |
| | Csoportokon belül | 10003,491 | 6569 | 1,523 | | |
| | Total | 10102,406 | 6573 | | | |
| Utazás szervezés | Csoportok között | 45,724 | 4 | 11,431 | 6,999 | 0,000 |
| | Csoportokon belül | 10728,112 | 6569 | 1,633 | | |
| | Total | 10773,836 | 6573 | | | |
| Adott anyag összefoglalása | Csoportok között | 664,094 | 4 | 166,023 | 94,217 | 0,000 |
| | Csoportokon belül | 11575,506 | 6569 | 1,762 | | |
| | Total | 12239,600 | 6573 | | | |
| Házi feladat megírása | Csoportok között | 839,015 | 4 | 209,754 | 127,022 | 0,000 |
| | Csoportokon belül | 10847,519 | 6569 | 1,651 | | |
| | Total | 11686,534 | 6573 | | | |
| Irodalmi források keresése | Csoportok között | 216,094 | 4 | 54,023 | 32,320 | 0,000 |
| | Csoportokon belül | 10980,319 | 6569 | 1,672 | | |
| | Total | 11196,413 | 6573 | | | |
| Fordítási feladatok | Csoportok között | 47,160 | 4 | 11,790 | 6,644 | 0,000 |
| | Csoportokon belül | 11657,438 | 6569 | 1,775 | | |
| | Total | 11704,598 | 6573 | | | |
| Szerepjáték | Csoportok között | 120,875 | 4 | 30,219 | 20,385 | 0,000 |
| | Csoportokon belül | 9738,008 | 6569 | 1,482 | | |
| | Total | 9858,883 | 6573 | | | |
| Dolgozat, esszé írás | Csoportok között | 667,026 | 4 | 166,757 | 98,545 | 0,000 |
| | Csoportokon belül | 11115,954 | 6569 | 1,692 | | |
| | Total | 11782,980 | 6573 | | | |

*4. táblázat: A generációs csoportok és az alkalmazási gyakoriság átlaga közötti kapcsolat varianciaanalízise (ANOVA), Forrás: saját kutatás, 2024, N = 6574*

A 3. táblázat korrelációs mátrixa részletes képet nyújt arról, hogyan kapcsolódnak egymáshoz a különböző használati módok. A 6574 fős minta alapján számított korrelációs együtthatók számos érdekes mintázatot tárnak fel, amelyek segítenek megérteni a felhasználói viselkedés struktúráját. A házi feladat megírása és a dolgozat/esszé írás közötti korreláció mutatja a legmagasabb értéket (0,721), ami logikus összefüggést tükröz. Mindkét tevékenység az iskolai, tanulmányi feladatok megíráshoz kapcsolódik, és hasonló készsége-

ket, valamint AI-funkciók használatát igényli. A felhasználók, akik az egyik területen aktívak, nagy valószínűséggel a másikban is alkalmazzák az AI eszközöket. Az utazás szervezés és az egészség/fitnesz tanácsok területek közötti erős korreláció (0,683) első ránézésre meglepő lehet, azonban mélyebb elemzés után érthető. Mindkét kategória életstílus-orientált alkalmazásokat takar, amelyek személyes jóllétre és életminőségre fókuszálnak. Azok a felhasználók, akik nyitottak az AI-alapú tanácsokra, valószínűleg más személyes területeken is használnak hasonló eszközöket. A kutatás/adatgyűjtés és az anyag összefoglalása közötti magas korreláció (0,666) szintén természetes kapcsolatot mutat. Ezek a funkciók gyakran egymást kiegészítő lépések egy nagyobb munkafolyamatban: a kutatás után következik az információk strukturálása és összefoglalása.

| | Nyelvtanulás | Kutatás és adatgyűjtés | Egészség és fitnesz tanácsok | Utazás szervezés | Adott anyag összefoglalása | Házi feladat megírása | Irodalmi források keresése | Fordítási feladatok | Szerepjáték | Dolgozat, esszé írás |
|---|---|---|---|---|---|---|---|---|---|---|
| Nyelvtanulás | 1,000 | | | | | | | | | |
| Kutatás és adatgyűjtés | 0,538 | *1,000* | | | | | | | | |
| Egészség és fitnesz tanácsok | 0,570 | *0,484* | *1,000* | | | | | | | |
| Utazás szervezés | 0,539 | *0,454* | *0,683* | *1,000* | | | | | | |
| Adott anyag összefoglalása | 0,462 | *0,666* | *0,479* | *0,485* | *1,000* | | | | | |
| Házi feladat megírása | 0,441 | *0,560* | *0,471* | *0,441* | *0,635* | *1,000* | | | | |
| Irodalmi források keresése | 0,497 | *0,572* | *0,544* | *0,550* | *0,605* | *0,604* | *1,000* | | | |
| Fordítási feladatok | 0,583 | *0,503* | *0,507* | *0,520* | *0,508* | *0,467* | *0,551* | *1,000* | | |
| Szerepjáték | 0,509 | *0,351* | *0,603* | *0,582* | *0,396* | *0,464* | *0,538* | *0,488* | *1,000* | |
| Dolgozat, esszé írás | 0,448 | *0,542* | *0,472* | *0,459* | *0,597* | *0,721* | *0,585* | *0,485* | *0,519* | *1,000* |

*5. táblázat: A területek közötti korrelációs mátrix (Inter-Item korrelációs mátrix), Forrás: saját kutatás, 2024, N = 6574*

## KÖVETKEZTETÉSEK

Vitathatatlan tény, hogy a mesterséges intelligencia soha nem látott népszerűségre tett szert napjainkban. Az AI megoldások gyorsasága és emberi munkát kiváltó mivolta miatt szinte mindenkinek a figyelmét magára vonta, és használja a mindennapi munkája

során, ami azonban jelentős eltérést mutat generációnként. A fent bemutatott kutatás alapján megállapítható, hogy az AI alkalmazásának gyakorisága generációs bontásban egyértelmű növekedést mutat: míg az idősebb generációk (Baby Boomer és X) inkább óvatosak, és főként információgyűjtésre, illetve szervezési feladatokra használják az AI-t, addig a fiatalabb generációk (Z és Alfa) már magabiztosan, sokoldalúan és rutinszerűen integrálják azt a tanulás, kreatív feladatok, sőt a mindennapi élet számos területén. Az AI leggyakrabban a kutatás, az információk összefoglalása és fordítás területén jelenik meg, míg a legkevésbé a szerepjátékokban, egészségügyi tanácsadásban és utazás szervezésben van jelen a mintába bevont válaszadóink mindennapjaiban. A kutatás alapján nagyon fontos lenne a jövőbeli digitális kompetenciafejlesztés, ami minden generáció számára célzott AI- és digitális írástudást fejlesztő programokat jelenthetne, hogy az idősebbek is magabiztosabban, a fiatalabbak pedig tudatosabban használják az AI-t. A fiatalabb generációknál kiemelten szükséges a kritikus gondolkodás fejlesztése, hogy az AI által nyújtott információkat megfelelően értékeljék. Fontos és lényeges kihívás a bizalomépítés és a tájékoztatás is, hiszen az AI-alkalmazások előnyeiről és korlátairól szóló hiteles tájékoztatás segítheti az elfogadottság növelését, főként az idősebbek körében. Mindezek a feladatok gyors megoldásokért kiáltanak, hiszen a mesterséges intelligencia előretörése sohasem látott mértékű. Azon rendszerek, melyek ezen kihívásokra választ tudnak adni, jelen állapotukban merevek, szabályozottak, ami újabb kihívásokat jelent. A kihívásoknak való megfelelés igényli a civil kezdeményezéseket, az egymástól való tanulás fontosságát azért, hogy minden generáció egyenlő arányban tudja élvezni az AI hozta előnyöket a mindennapi élete során.

## FELHASZNÁLT IRODALOM

[1] Russell, S. J., & Norvig, P. (2016). Artificial intelligence: a modern approach. pearson.
[2] Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. California management review, 61(4), 5-14.
[3] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955. AI Magazine, 27(4), 12–14.
[4] Pannu, A. (2015). Artificial intelligence and its application in different areas. Artificial Intelligence, 4(10), 79-84.
[5] Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., ... & Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2(4).
[6] Sterczl, G., & Csiszárik-Kocsir, Á. (2025). Comparative analysis of AI models – Using AI-supported qualitative data analysis for interview analysis. *Acta Polytechnica Hungarica, 22*(7). 223-243
[7] Dignum, V. (2019). Responsible artificial intelligence: how to develop and use AI in a responsible way (Vol. 2156). Cham: Springer.
[8] Kollár, Cs. (2023). A mesterséges intelligencia megjelenése a biztonságtudományban. In J. K. Tibor (Szerk.), What will our Future be Like? : 2 essays in German, 7 in English, 30 in Hungarian language (Német, angol és magyar nyelvű esszék), 242–256
[9] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

[10] Rai, A. (2020). Explainable AI: From black box to glass box. Journal of the academy of marketing science, 48, 137-141.
[11] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.
[12] Balogh, A., & Varga, J. (2025). A hallgatók álláspontja a mesterséges intelligencia használatáról a gazdasági felsőoktatásban. Controller Info, 13(1), 40–45.
[13] Kozhanov, M., Mosavi, A., Amirov, A., Kaibassova, D., Póser, V., Shakhatova, A., La Lira, & Eigner, Gy. (2024). Syllabus design and planning with artificial intelligence and the potential of generative AI. In A. Szakál (Ed.), IEEE 24th International Symposium on Computational Intelligence and Informatics (CINTI 2024): Proceedings, 257–264
[14] Garai-Fodor, M., & Huszák, N. (2025). The potential of integrating conscious living into education for generation Z in the light of primary data. Frontiers in Education, 9, Article 1477879, 1–10.
[15] Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education–where are the educators?. International journal of educational technology in higher education, 16(1), 1-27.
[16] Luckin, R., & Holmes, W. (2016). Intelligence unleashed: An argument for AI in education.
[17] Menon, R., Tiwari, A., Chhabra, A., & Singh, D. (2014). Study on the higher education in India and the need for a paradigm shift. Procedia Economics and Finance, II, 1, 886–871.
[18] Chatterjee, S., & Bhattacharjee, K. K. (2020). Adoption of artificial intelligence in higher education: A quantitative analysis using structural equation modelling. Education and Information Technologies, 25, 3443-3463.
[19] Haleem, A., Javaid, M., & Khan, I. H. (2019). Current status and applications of Artificial Intelligence (AI) in medical field: An overview. Current Medicine Research and Practice, 9(6), 231-237.
[20] Davenport, T. H., & Ronanki, R. (2018). Artificial Intelligence for the Real World. Harvard Business Review, 96(1), 108–116.
[21] Brynjolfsson, E., & McAfee, A. (2017). The Business of Artificial Intelligence. Harvard Business Review. https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence (letöltve: 2025.04.12.)
[22] Varga, J. (2021). Defining the economic role and benefits of micro, small and medium-sized enterprises in the 21st century with a systematic review of the literature. Acta Polytechnica Hungarica, 18(11), 209-228.
[23] Kovács, E.-Zs., & Horváth, I. (2025). Trust, transparency, and AI adoption in business. Acta Polytechnica Hungarica, 22(6), 81-100
[24] Prensky, M (2001): "Digital Natives, Digital Immigrants", in On the Horizon, Vol. 9, No. 5.
[25] Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R. (2019). Consumers acceptance of artificially intelligent (AI) device use in service delivery. International Journal of Information Management, 49, 157-169.

[26] Garai-Fodor, M. (2022). The Impact of the Coronavirus on Competence, from a Generation-Specific Perspective. Acta Polytechnica Hungarica. 19(8) pp. 111-125.
[27] Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly, 157-178.
[28] Zhang, B., & Dafoe, A. (2019). Artificial intelligence: American attitudes and trends. Available at SSRN 3312874 (letöltve: 2025.02.11.)
[29] Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. Personnel psychology, 53(2), 375-403.
[30] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds and machines, 28, 689-707.
[31] Bessen, J. (2018). AI and jobs: The role of demand (No. w24235). National Bureau of Economic Research.
[32] Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & company.
[33] Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). Psychology and aging, 21(2), 333.
[34] Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., Dijkstra, K., Fisk, A. D., Rogers, W. A., & Sharit, J. (2010). Older adults talk technology: Technology usage and attitudes. Computers in human behavior, 26(6), 1710-1721.
[35] Charness, N., & Boot, W. R. (2009). Aging and information technology use: Potential and barriers. Current directions in psychological science, 18(5), 253-258.

DOI: https://doi.org/10.12700/btsz.2025.7.3.193

# NEW OPPORTUNITIES IN OCCUPATIONAL ACCIDENT DATA PROCESSING: INVESTIGATING THE PREREQUISITES FOR AI-BASED SUPPORT (PART ONE)

# A MUNKABALESETI ADATFELDOLGOZÁS ÚJ LEHETŐSÉGEI: AI TÁMOGATÁS ELŐFELTÉTELEINEK VIZSGÁLATA (ELSŐ RÉSZ)

HERÉNYI Zoltán[1]

**Abstract**

In the aftermath of a serious or fatal workplace accident, legal proceedings critically depend on the conclusions of official investigations. These essential insights must often be established within hours, directly at the accident site and under psychologically demanding condi-tions. The advancement of artificial intel-ligence enables the development of decision-support systems that may reduce the likelihood of human error. This, however, requires that regulatory knowledge be transformed into a reliable, machine-readable data structure. The present study investigates how, based on the official Methodological Guide, a su-itable framework can be designed to sup-port AI-based accident investigations. While the study does not cover all sta-tistical outcomes of practical implementa-tion, it provides a foundation for a more detailed, data-driven analysis to be presented in a subsequent article.

**Keywords**

artificial intelligence, augmented intelligence, decision support, regulatory occupational safety inspection, work accident

**Absztrakt**

Egy súlyos vagy halálos munkabaleset utáni jogi eljárásban a hatósági vizsgálatok megállapításai kulcsszerepet játszanak. Az alapvető megállapításoknak, lényegi felismeréseknek már a balesetet követő órákban meg kell történni a bal-eset helyszínén, feszült, pszichésen terhelt környezetben. A mesterséges intelligencia fejlettsége lehetővé teszi olyan döntéstámogató rendszerek létrehozását, amelyek csökkenthetik a hibázás esélyét. Ennek feltétele, hogy a hatósági tudás megbízható, a gépi feldolgozás számára is kezelhető adatstruktúrává legyen átalakítható. A jelen tanulmány azt vizsgálja, hogy a Módszertani útmutató alapján milyen formában alakítható ki olyan keretrendszer, amely az MI-alapú vizsgálati támogatás alapjául szolgálhat. A tanulmány nem tér ki a gyakorlati megvalósítás minden statisztikai eredményére, de megalapozza azt a részletesebb és adatalapú elemzést, amely egy következő cikkben kerül bemutatásra.

**Kulcsszavak**

mesterséges intelligencia, kiterjesztett intelligencia, döntéstámogatás, munkavédelmi hatósági ellenőrzés, munkabaleset

[1] zoltan.herenyi@gmail.com | ORCID: 0009-0000-2583-7104| PhD student, Doctoral School of Safety and Security Sciences, Óbuda University | doktorandusz, Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Az európai uniós országoknak keretirányelvek [1], [2] írják elő, hogy milyen alapvető munkavédelmi normáknak kell megfelelniük. A keretirányelvek, ahogy a nevük is mutatja, csak alapvető munkavédelmi normákat fektetnek le, de azokon belül az egyes nemzetállamok saját munkavédelmi stratégiákat dolgoznak ki a foglalkozási megbetegedések és munkabalesetek visszaszorítására. Ezek a stratégiák időről időre változhatnak a munkavédelmi ellenőrzéseket végző hatósági szervek visszajelzései alapján. Ahhoz azonban, hogy a jogalkotók hatékony intézkedéseket dolgozhassanak ki, a visszajelzéseknek konzisztensnek, szubjektív torzításoktól minél inkább mentesnek kell lenniük. Ennek elérésére a hatósági működés, azon belül is konkrétan az ellenőrzések menetének, részletes szabályozása eszközként kínálkozik.

Magyarországon már korábban is történtek kísérletek az egységes ellenőrzési gyakorlat megvalósítására különböző módszertani dokumentumok formájában. 2016-ban azonban új lendületet vett a folyamat: a Nemzetgazdasági Minisztérium, az Országos Munkavédelmi és Munkaügyi Főfelügyelőség, valamint a Munkavédelmi Kutatóintézet közösen kidolgozta a Módszertani útmutató a munkabalesetek hatósági vizsgálatához című dokumentumot, amely az egységes értelmezési és eljárási keretek biztosítását tűzte ki célul. Bár maga a dokumentum a munkavállalók számára is elérhető formában készült el, hatálybalépésének egyértelmű dátuma és a benne foglalt részletes előírások jelzik, hogy a munkavédelmi ellenőrzéseket végző hatóságok számára irányadóvá vált. Az útmutató megalkotásának egyik legfontosabb háttérfolyamata a GINOP-5.3.4-16-2016-00001 projekt keretében zajlott, amelynek célja kifejezetten a munkabalesetek vizsgálati módszertanának megújítása és korszerűsítése volt [3]. A „Módszertani útmutató a munkabalesetek hatósági vizsgálatához" című dokumentum teljes részletességgel rögzíti, hogy egy munkavédelmi hatósági ellenőrzés során milyen protokollt kell követni, illetve milyen vizsgálati szempontokra kell kitérni. A kihívás azonban nem pusztán a szabályozási keret meglétében rejlik, hanem abban, hogy képes-e minden munkavédelmi felügyelő készségszinten alkalmazni az előírtakat, gyorsan, precízen, és nehéz körülmények között is. A hatósági ellenőrzések időkerete ugyanis nem lehet indokolatlanul hosszú, a súlyos vagy halálos munkabalesetek kivizsgálásakor pedig a helyzet extrémitása érzelmi és pszichés terhelést is ró az eljáró szakemberre.

A jelen kutatás célja annak feltárása, hogy a Nemzetgazdasági Minisztérium által kiadott „Módszertani útmutató a munkabalesetek hatósági vizsgálatához" dokumentum alapján kialakítható-e egy mesterséges intelligenciával támogatott vizsgálati keretrendszer. A vizsgálat során az útmutatóban rögzített vizsgálati szempontok olyan módon kerültek átalakításra, hogy azok segítségével a kutatásban feldolgozott 29 esettanulmány érdemi megállapításai számszerűsíthető adatokként legyenek megjeleníthetők.

A kutatás főbb kérdései:

1. K1. Létrehozható-e egy olyan vizsgálati keretrendszer a módszertani útmutató alapján, amely lehetővé teszi az esettanulmányokban foglalt érdemi információk hiteles, számszerűsített reprezentációját?
2. K2. Ha az új vizsgálati keretrendszerrel pontosan leképezhetők az esettanulmányok lényegi elemei, alkalmas lehet-e az új keretrendszer olyan mintázatok, szabályszerűségek azonosítására, amelyek hagyományos vizsgálati módszerekkel nem lennének felismerhetők?

## SZAKIRODALMI ÁTTEKINTÉS

A munkabalesetek és foglalkozási megbetegedések megelőzése mindig is kiemelt kérdés volt a nemzetállamok számára. Az Európai Unió tagállamai 1989. június 12-én fogadták el a 89/391/EGK számú keretirányelvet, melynek célja a munkabalesetek visszaszorítása volt az uniós országokban [4]. A tagállamok, köztük Magyarország ennek szellemében dolgozzák ki saját munkavédelmi stratégiáikat, szem előtt tartva az irányelvben foglaltak teljesülését. Mindezek ellenére napjainkig sem sikerült radikális javulást elérni sem a munkabalesetek, sem a foglalkozási megbetegedések területén.

Számos kimutatás és tanulmány foglalkozik a témával hazai [5],[6],[7]és nemzetközi [8], [9], szinten egyaránt. Ezek közé sorolható Szabó munkája is, aki a kockázatértékelési módszerek sajátosságait elemzi külön tanulmányban [10]Az Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség (EU-OSHA) oldalán elérhető becslés szerint a munkavégzéssel összefüggő balesetek és megbetegedések évente legalább 476 milliárd eurónyi kárt okoznak az Európai Uniónak, ami a GDP 3,3%-ának felel meg [11]. A Makronóm Intézet 2023-as tanulmánya alapján ez a költség Magyarország esetében 2022-ben 382,1 milliárd forintra rúgott [12]. Ehhez még hozzájönnek azok az anyagi veszteségek is, amelyeket a munkáltatók és munkavállalók a munkából való kiesés miatt szenvednek el. Az európai uniós keretirányelvek szándékosan hagynak mozgásteret a tagállamok számára, hogy azok saját gazdasági, társadalmi és munkakultúrájuk figyelembevételével alakíthassák ki a legmegfelelőbb szabályozásokat a foglalkozási megbetegedések és a munkabalesetek megelőzése érdekében. Ez nemcsak az adott ország, hanem az Európai Unió közös érdeke is, hiszen a hatékony megelőzés gazdasági, társadalmi és egészségügyi szinten egyaránt érezhető pozitív hatást gyakorol.

Magyarországon a munkavédelem részletesen szabályozott a meglehetősen sok jogszabálynak és a szabványoknak köszönhetően. A Napo-filmek 1998 óta ingyenesen elérhető, szórakoztató formában segítenek az alapvető munkavédelmi ismeretek elsajátításában és a jogszabályok gyakorlati alkalmazásában [13]. Az OSHwiki platform 2014-től biztosít naprakész, hiteles munkavédelmi információkat a szakemberek és vállalkozások számára [14], a 2011-ben indított OiRA platform pedig lehetővé teszi az ingyenes és szakszerű kockázatértékelések elvégzését [15].

A Magyar Szabványügyi Testület és az illetékes minisztériumok folyamatosan nyomon követik a munkavédelem aktuális helyzetét, és szükség esetén módosítják a vonatkozó jogszabályokat és szabványokat. Ezek változásairól a Magyar Közlönyben [16], az MSZT hivatalos honlapján [17], valamint az online szabványkönyvtárban lehet tájékozódni [18]. Emellett nemzetközi szintű jogszabályok és szabványok is elérhetők [19], [20].

A munkavédelmi normák teljesülésének ellenőrzése a Nemzetgazdasági Minisztérium hatáskörébe tartozó munkavédelmi hatóságok feladata. A felügyelők rendszeres ellenőrzéseket tartanak, és hiányosság esetén intézkednek a megszüntetés érdekében. Az ő munkájuk alapvetően hozzájárul a nemzeti munkavédelmi politika megvalósításához [21].

A munkavédelmi hatóságok által végzett ellenőrzések jegyzőkönyvei alapján megyei szintű jelentések készülnek, amelyekből később országos, nemzetgazdasági szintű jelentések is születnek [22]. Ezek a jelentések közvetlen hatást gyakorolnak a jogalkotásra, ezért különösen fontos, hogy az ellenőrzések egységes szempontok szerint, magas szakmai színvonalon történjenek. Ezt a célt szolgálja a Nemzetgazdasági Minisztérium által 2016-

ban kiadott Módszertani útmutató a munkabalesetek hatósági vizsgálatához is, amely részletesen szabályozza a munkavédelmi hatósági ellenőrzések és balesetkivizsgálások lefolytatásának módját, és elősegíti az egységes elvek mentén történő munkavégzést. Az útmutató a baleseti kivizsgálások során vizsgálandó szempontokat is meghatározza. A dokumentum 8. fejezetétől a 12. fejezetéig öt kulcsterületre bontva tárgyi, személyi, szervezési, környezeti tényező, valamint a dokumentációk vizsgálatán belül mintegy 70 vizsgálati szempontot jelöl meg a hozzájuk tartozó különböző tényezőkkel mely így több mint 100 tényező mérlegelését követeli meg egyetlen eljárás során. A módszertani útmutatóban szereplő, mintegy hetven vizsgálati szempont készségszintű alkalmazása különösen kihívást jelent pszichésen megterhelő munkakörnyezetben, például súlyos vagy halálos kimenetelű balesetek helyszínén. Ilyen körülmények között a felügyelő döntéseit érzelmi nyomás, időkorlát és információhiány is torzíthatja, ami jelentősen növeli a hibázás valószínűségét [23],[24]. Az egységes, magas szakmai színvonalú hatósági ellenőrzések irányába tett következő logikus lépés a módszertani útmutatók olyan döntéstámogató rendszerré való átalakítása lehet, amely képes objektíven, valós időben segíteni az eljáró felügyelőt. Hasonló rendszerek sikeres alkalmazására már számos példa létezik: a Semmelweis Egyetem hivatalos beszámolója szerint a mesterséges intelligenciát több száz bőrbetegség hatékony felismerésére használták sikeresen [25]. Ezen rendszerek hatékonysága döntően azon múlik, hogy a releváns tényezőket milyen mértékben sikerül az algoritmusok számára is feldolgozható, strukturált adattá alakítani [26]. Erre vonatkozóan Szabó az informatikai rendszerek üzemeltetésének minőségbiztosítási szempontjait tárgyalja tanulmányában, különös tekintettel az adatmegbízhatóság szerepére a döntéstámogató rendszerekben [27]

A hatósági tapasztalatok és a munkavédelmi ellenőrzések során rögzített jegyzőkönyvek tartalmazhatnak olyan ismétlődő mintázatokat, amelyek alkalmasak lehetnek egy strukturált tudásbázis kialakítására. Ennek érdekében kulcsfontosságú, hogy az ellenőrzési szempontok és azokhoz kapcsolódó megállapítások olyan módon kerüljenek rögzítésre, amely lehetővé teszi azok matematikai, logikai vagy szabályalapú reprezentációjukat. A különböző vizsgálati elemek, például a személyi, tárgyi vagy szervezeti tényezők, tipikusan logikai összefüggéseken, állapotokon, eseményláncolatokon keresztül értelmezhetők, amelyeket döntési mátrixok és súlyozott relációs modellek segítségével lehet a gépi intelligencia számára értelmezhető formában feldolgozni [28].

## KUTATÁSMÓDSZERTAN

### A kutatás jellege

A kutatás kvalitatív módszertannal dolgozik, amely hatékonynak bizonyult 29 halálos munkabaleset hivatalos kivizsgálási összefoglalójának elemzésében. A kvalitatív kutatási módszerek célja az összetett jelenségek, szubjektív tapasztalatok és társadalmi interakciók feltárása és megértése. Ezek a módszerek mélyreható betekintést nyújtanak az emberi viselkedés, attitűdök és társadalmi interakciók összetettségébe és árnyalataiba [29],[30]

A vizsgálati folyamatot a grounded theory megközelítés támogatta, lehetőséget biztosítva az elemzési keretrendszer folyamatos fejlesztésére. A grounded theory olyan kutatási módszer, ahol az elmélet az empirikus adatokból fejlődik ki és abban gyökerezik [31], [32]

**Az adatok forrása**

Az elemzés a Munkavédelem Foglalkoztatás-felügyelet hivatalos oldalán publikált esettanulmányokra épül. [33]Ezek az összefoglalók a legtanulságosabb halálos munkabalesetek hivatalos kivizsgálásainak eredményeit tartalmazzák, közérthető módon bemutatva a történteket, miközben megőrzik a hivatalos dokumentáció struktúráját.

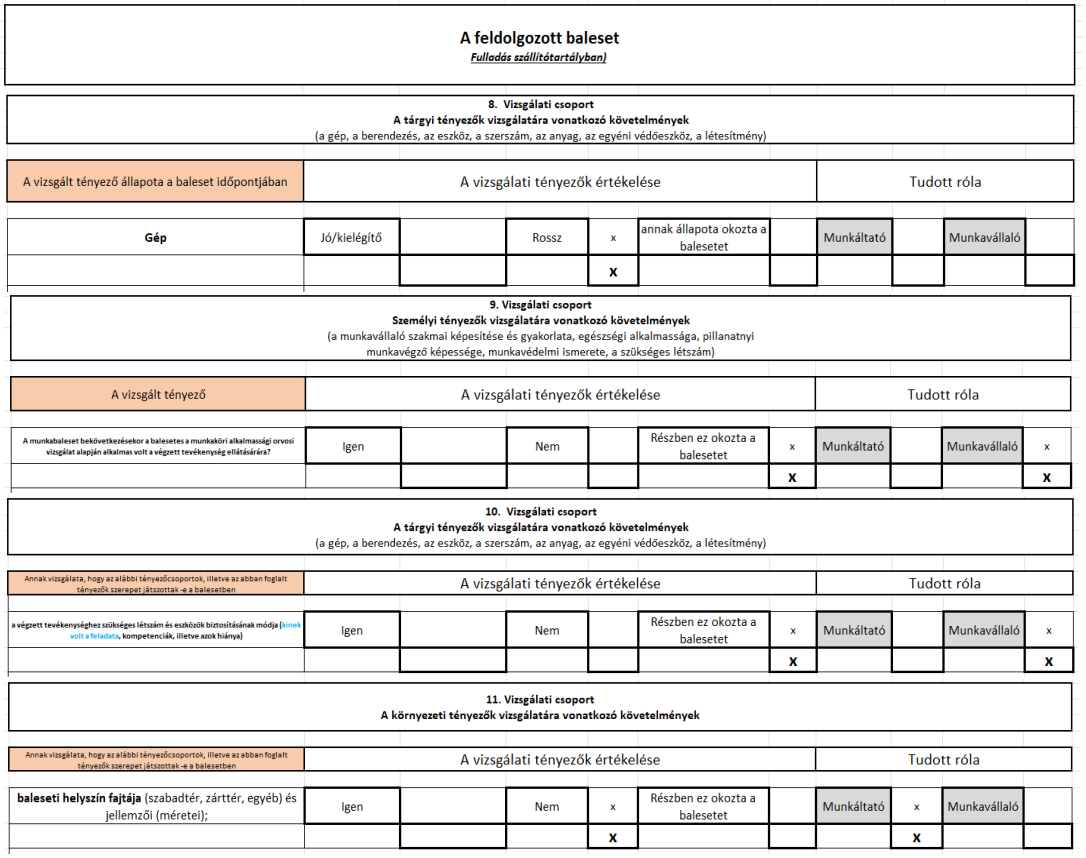
**Az esettanulmányok feldolgozása**

Az esettanulmányok tartalomelemzése strukturált táblázatok segítségével történt. A vizsgálati rendszer alapját a Nemzetgazdasági Minisztérium által kiadott „Módszertani útmutató a munkabalesetek hatósági vizsgálatához" című dokumentum képezte, amely a munkavédelmi felügyelők számára rögzíti a kivizsgálás szabályait és szempontjait. Bár a dokumentum hivatalosan nem nyilvános kiadványként került forgalomba, a kutatás során a szerző személyes archívumából származó, hiteles példány alapján történt a vizsgálati szempontok strukturálása és értelmezése.

**A táblázatok strukturálása**

A vizsgálati rendszer táblázatos formája az útmutató 8., 9., 10., 11. és 12. fejezetei alapján, öt vizsgálati csoportra bontva készült el. A táblázatok felépítése követi a hivatalos dokumentum fejezetszámozását, elősegítve az átláthatóságot. Összesen 70 vizsgálati szempont szerepel a rendszerben, amelyekhez alszempontok is tartoznak, így a ténylegesen vizsgált tényezők száma 152-re bővül. A szempontok megjelölése az értéknégyzetekbe helyezett „X" karakterrel történt.

Az 1. ábra célja, hogy átfogó képet adjon a vizsgálati szempontstruktúra felépítéséről és a szempontcsoportokhoz tartozó adatok jellegéről. Az itt bemutatott sorok minden szempontcsoportból egy-egy reprezentatív példát tartalmaznak, amely lehetővé teszi az olvasó számára a teljes rendszer logikájának és az összegzett válaszok eloszlásának gyors áttekintését. A teljes adattábla mellékletként elérhető a kutatásban, így a teljes részletesség iránt érdeklődők számára is hozzáférhető.



**A feldolgozott baleset**
***Fulladás szállítótartályban)***

**8. Vizsgálati csoport**
**A tárgyi tényezők vizsgálatára vonatkozó követelmények**
(a gép, a berendezés, az eszköz, a szerszám, az anyag, az egyéni védőeszköz, a létesítmény)

| A vizsgált tényező állapota a baleset időpontjában | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Gép** | Jó/kielégítő | | Rossz | x | annak állapota okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | | | | X | | | | | | |

**9. Vizsgálati csoport**
**Személyi tényezők vizsgálatára vonatkozó követelmények**
(a munkavállaló szakmai képesítése és gyakorlata, egészségi alkalmassága, pillanatnyi munkavégző képessége, munkavédelmi ismerete, a szükséges létszám)

| A vizsgált tényező | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| A munkabaleset bekövetkezésekor a balesetes a munkaköri alkalmassági orvosi vizsgálat alapján alkalmas volt a végzett tevékenység ellátására? | Igen | | Nem | | Részben ez okozta a balesetet | x | Munkáltató | | Munkavállaló | x |
| | | | | | | X | | | | X |

**10. Vizsgálati csoport**
**A tárgyi tényezők vizsgálatára vonatkozó követelmények**
(a gép, a berendezés, az eszköz, a szerszám, az anyag, az egyéni védőeszköz, a létesítmény)

| Annak vizsgálata, hogy az alábbi tényezőcsoportok, illetve az abban foglalt tényezők szerepet játszottak-e a balesetben | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| a végzett tevékenységhez szükséges létszám és eszközök biztosításának módja (kinek volt a feladata, kompetenciák, illetve azok hiánya) | Igen | | Nem | | Részben ez okozta a balesetet | x | Munkáltató | | Munkavállaló | x |
| | | | | | | X | | | | X |

**11. Vizsgálati csoport**
**A környezeti tényezők vizsgálatára vonatkozó követelmények**

| Annak vizsgálata, hogy az alábbi tényezőcsoportok, illetve az abban foglalt tényezők szerepet játszottak-e a balesetben | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **baleseti helyszín fajtája** (szabadtér, zárttér, egyéb) és jellemzői (méretei); | Igen | | Nem | x | Részben ez okozta a balesetet | | Munkáltató | x | Munkavállaló | |
| | | | | X | | | | X | | |

*1. Ábra: Mintatáblázat a vizsgálati szempontok jelölésére Forrás: Saját szerkesztés.*

A példaként bemutatott részlet a táblázatok gyakorlati alkalmazását és a válaszformák értelmezhetőségét hivatott illusztrálni.

## A jelölések és válaszformák alkalmazása

A feldolgozás során nemcsak azt kellett rögzíteni, hogy egy tényező jelen volt-e az esettanulmányban, hanem azt is, hogy milyen szerepet töltött be a balesetben. A válaszformák három kategóriában jelentek meg: „Igen”, „Nem”, és „Annak állapota okozta a balesetet”. Ezzel biztosíthatóvá vált, hogy a vizsgálati szempontok ne csak egyszerűen megjelenjenek, hanem a tényleges jelentőségük is rögzítésre kerüljön. A választási lehetőségek a vizsgálati csoport logikájához igazodtak, de funkciójuk egységes maradt: lehetőséget adni a felügyelői megállapítások értékelésére.

A jelölések minden esetben a felügyelői megállapításokon alapultak. A könnyebb áttekinthetőség érdekében a vizsgálati szempont melletti cellákba is bekerült az „X” karakter, amely segítette az értékelés gyors áttekintését és a lehetséges hibák kiszűrését.

## A „Tudott róla” kiegészítő vizsgálati szempont bevezetése

A feldolgozási rendszer kiegészült a „Tudott róla” vizsgálati szemponttal, amely minden alapszempont mellett megjelent. Célja annak jelzése volt, ha a felügyelői megállapítás szerint a munkáltató vagy a munkavállaló tudott az adott hiányosságról. Ez a szempont

elsősorban a munkavédelmi tudatosság becslésére szolgált, és csak akkor került rögzítésre, ha a tudatosság ténye az esettanulmányból egyértelműen kiolvasható volt. A „Tudott róla" szempont minden esetben elkülönülten, szürke színnel szerepelt.

**A szempontrendszer alkalmazhatósága és bővítése**

A vizsgálati rendszer sikeresen strukturálhatóvá teheti az esettanulmányok tartalmát, lehetővé téve a vizsgálati szempontok rögzítését, azok szerepének értelmezését és a vizsgálat során feltárt szabálytalanságok szisztematikus rögzítését. A rendszer így nem csupán az esetek feldolgozását, hanem azok összehasonlíthatóságát és a mintázatok azonosítását is elősegítheti. A szempontok ilyen szintű strukturálása nemcsak a feldolgozhatóságot, hanem a gépi tudásreprezentáció lehetőségét is megalapozza. A mesterséges intelligencia számára a logikai struktúrák, ontológiák, súlyozott gráfok vagy döntési fák formájában megjelenített tudásbázisok biztosítják a releváns információk értelmezését és alkalmazását. A jelen vizsgálatban kialakított szempontrendszer ennek előszobája lehet, hiszen lehetővé teszi, hogy a munkabalesetekre vonatkozó emberi tudás az MI számára is értelmezhető formában legyen reprezentálva [34]

**Bizonytalanság csökkentése a jelölések redundáns alkalmazásával**

Az esettanulmányok alapján összeállított táblázat egy nagyméretű, komplex struktúrát eredményezett, amelyben a kitöltés során előfordulhattak elírások vagy hibás jelölések. Ennek kiszűrésére a releváns szempontokat nem csak kizárólag az értéknégyzetekben, hanem azok közvetlen szomszédos celláiban is jelölésre kerültek. Ez a megközelítés ugyan a valódi jelölések duplikációját eredményezte, azonban az összegzések értékeinek kettővel történő osztása révén a torzítások kiküszöbölhetők voltak.

A módszer lehetővé tette, hogy az összesítés során tört értékek is megjelenhessenek, amelyek potenciálisan hibás jelölésekre utalhattak. A jelölések helyességének ellenőrzését cellaszűrések alkalmazása is támogatta.

**Bizonytalanság csökkentése a részeredmények döntéseinek ellenőrizhetőségével**

A vizsgálat során kizárólag olyan szempontok kerültek be a rendszerbe, amelyek relevanciáját az esettanulmányokban a felügyelők kifejezett megállapításai is alátámasztották. A későbbi validálási folyamatok során azonban érdemes lehet megfontolni az újraértékelést független szakértői bevonással, amely során az egyes tényezőkre vonatkozó értékelések szintén rögzítésre kerülhetnének a vizsgálati rendszerben. A szakértői vélemények szubjektív jelölései abban az esetben is hasznos kiegészítő információt nyújthatnak, ha jól elkülöníthetők maradnak a hivatalos megállapításoktól, ezáltal lehetőséget biztosítva a későbbi összevetésre és kritikai értékelésre is. A vizsgálati keretrendszer kialakításakor kiemelt cél volt a rugalmas jelölési lehetőségek biztosítása. Ennek megfelelően a rendszer nem korlátozódik kizárólag az „x" karakter használatára: a jelölések bármilyen, előzetesen egyeztetett karakterrel történhetnek, figyelembe véve a szakértői megállapodások tartalmát. A választott karakterek nem befolyásolják a kiértékelési folyamat értelmezhetőségét vagy eredményességét, így a rendszer könnyen alkalmazkodik az eltérő értelmezési és gyakorlati igényekhez.

**Bizonytalanságok csökkentése hiteles adatbázis és módszer alkalmazása által**

Bár a szubjektív torzítások teljes mértékű kizárása a balesetvizsgálatok során nem lehetséges, a kutatás során alkalmazott módszertani elemek megbízhatóságát több tényező

is erősíti. Az eljárási keretrendszert képező útmutató többéves szakértői tapasztalatra épül, és hatóságilag elfogadott irányelveken alapul. Az esettanulmányokon alapuló adatbázis hitelességét pedig azok a munkavédelmi felügyelők biztosítják, akik a kivizsgálásokat végezték, a szakmai protokollok és szabályozások keretein belül. A vizsgálatok rendszerszintű jellege és a kivizsgálók gyakorlati tapasztalata hozzájárul ahhoz, hogy a kutatás során felhasznált adatok és megállapítások megfelelő alapot nyújtsanak a további elemzésekhez.

### Az eljárás finomítási lehetőségei

A kutatási eredmények mögötti bizonytalanság jelenleg abból fakad, hogy a kialakított vizsgálati eljárás még nem esett át teljes körű validáláson. Ennek ellenére a kutatás célja nem az eljárás véglegesítése, hanem annak vizsgálata volt, hogy a hivatalos módszertani útmutató alapján létrehozható-e egy olyan strukturált vizsgálati rendszer, amely alkalmas a munkabalesetek általános jellemzőinek feltárására.

A módszer megbízhatósága és alkalmazhatósága a gyakorlati alkalmazás során szerzett tapasztalatok alapján ítélhető meg. A kutatás során felhasznált esettanulmányok jellemzően rövidített formában álltak rendelkezésre, amelyekben a felügyelők elsősorban a baleset közvetlen kiváltó okaira koncentráltak. Ennek következtében nem minden esetben kerültek rögzítésre az összes feltárt hiányosságok, így a háttérben meghúzódó tényezők megítélése torzulhatott.

Továbbá a vizsgálati módszertan egyik gyakorlati nehézsége, hogy bizonyos hiányosságok több szempont alá is besorolhatók, ami értelmezési átfedésekhez vezethet. Ennek kezelésére célszerű lehet a szempontrendszer olyan irányú módosítása, amely lehetővé teszi az átfedések pontosabb azonosítását, valamint a másodlagos tényezők egyértelműbb elkülönítését

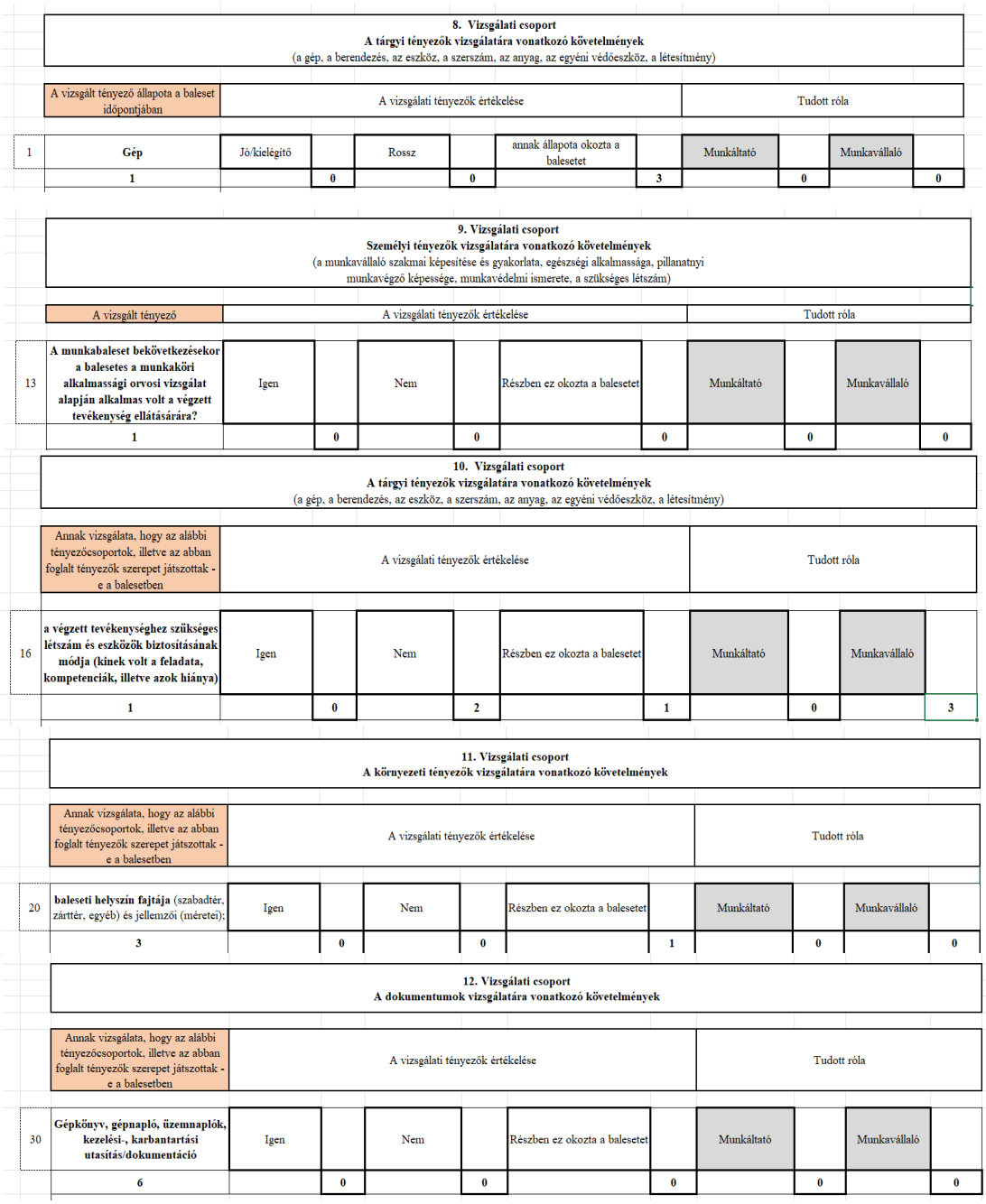
## KUTATÁSI EREDMÉNYEK

A következőkben bemutatott eredmények a 29 halálos munkabaleset esettanulmányainak feldolgozásából származnak. Az elemzések alapját a strukturált táblázatok képezték, amelyek a munkavédelmi hatóság módszertani útmutatója alapján kialakított szempontcsoportok szerint rendszerezték az egyes esetekben feltárt tényezőket.

A táblázatok nemcsak a balesetek közvetlen kiváltó okait, hanem a munkáltatók és munkavállalók tudatosságát is vizsgálták. A fejezetben először egy összefoglaló adatbázis kerül bemutatásra, majd az adatok részletes kiértékelése következik, többek között a szempontrendszer kihasználtságának, a gyakorisági eloszlásoknak és a közvetett tényezők jelenlétének vizsgálatával.

### A balesetek vizsgálatából származó összesített adatok

A 2. ábra célja, hogy átfogó képet adjon a vizsgálati szempontstruktúra felépítéséről és a szempontcsoportokhoz tartozó adatok jellegéről. Az itt bemutatott sorok minden szempontcsoportból egy-egy reprezentatív példát tartalmaznak, amely lehetővé teszi az olvasó számára a teljes rendszer logikájának és az összegzett válaszok eloszlásának gyors áttekintését. A teljes adattábla mellékletként elérhető a kutatásban, így a teljes részletesség iránt érdeklődők számára is hozzáférhető.



**8. Vizsgálati csoport**
**A tárgyi tényezők vizsgálatára vonatkozó követelmények**
(a gép, a berendezés, az eszköz, a szerszám, az anyag, az egyéni védőeszköz, a létesítmény)

| | A vizsgált tényező állapota a baleset időpontjában | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Gép** | Jó/kielégítő | | Rossz | | annak állapota okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | **1** | | **0** | | **0** | | **3** | | **0** | | **0** |

**9. Vizsgálati csoport**
**Személyi tényezők vizsgálatára vonatkozó követelmények**
(a munkavállaló szakmai képesítése és gyakorlata, egészségi alkalmassága, pillanatnyi munkavégző képessége, munkavédelmi ismerete, a szükséges létszám)

| | A vizsgált tényező | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | **A munkabaleset bekövetkezésekor a balesetes a munkaköri alkalmassági orvosi vizsgálat alapján alkalmas volt a végzett tevékenység ellátására?** | Igen | | Nem | | Részben ez okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | **1** | | **0** | | **0** | | **0** | | **0** | | **0** |

**10. Vizsgálati csoport**
**A tárgyi tényezők vizsgálatára vonatkozó követelmények**
(a gép, a berendezés, az eszköz, a szerszám, az anyag, az egyéni védőeszköz, a létesítmény)

| | Annak vizsgálata, hogy az alábbi tényezőcsoportok, illetve az abban foglalt tényezők szerepet játszottak - e a balesetben | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | **a végzett tevékenységhez szükséges létszám és eszközök biztosításának módja (kinek volt a feladata, kompetenciák, illetve azok hiánya)** | Igen | | Nem | | Részben ez okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | **1** | | **0** | | **2** | | **1** | | **0** | | **3** |

**11. Vizsgálati csoport**
**A környezeti tényezők vizsgálatára vonatkozó követelmények**

| | Annak vizsgálata, hogy az alábbi tényezőcsoportok, illetve az abban foglalt tényezők szerepet játszottak - e a balesetben | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | **baleseti helyszín fajtája** (szabadtér, zárttér, egyéb) és jellemzői (méretei); | Igen | | Nem | | Részben ez okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | **3** | | **0** | | **0** | | **1** | | **0** | | **0** |

**12. Vizsgálati csoport**
**A dokumentumok vizsgálatára vonatkozó követelmények**

| | Annak vizsgálata, hogy az alábbi tényezőcsoportok, illetve az abban foglalt tényezők szerepet játszottak - e a balesetben | A vizsgálati tényezők értékelése | | | | | | Tudott róla | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 30 | **Gépkönyv, gépnapló, üzemnaplók, kezelési-, karbantartási utasítás/dokumentáció** | Igen | | Nem | | Részben ez okozta a balesetet | | Munkáltató | | Munkavállaló | |
| | **6** | | **0** | | **0** | | **0** | | **0** | | **0** |

*2. Ábra: A vizsgálati szempontstruktúra áttekintő kivonata Forrás: Saját szerkesztésű*

Az ábra minden vizsgálati szempontcsoportból tartalmaz egy-egy jellemző sort, a hozzájuk tartozó "Igen", "Nem", "Annak állapota okozta a balesetet", valamint "Tudott

róla" válaszok összesített előfordulásával. A kiválasztott sorok célja, hogy strukturált áttekintést nyújtsanak a vizsgálati mátrix felépítéséről, a részletes adatokat tartalmazó teljes táblázat a mellékletben található.

**A vizsgálati szempontrendszer struktúrája és feldolgozottsági aránya**

A 3. Ábra a vizsgálati szempontrendszer általános jellemzőit és annak feldolgozottsági szintjét mutatja be. A szerkezeti adatok mellett megjelennek azok az arányszámok is, amelyek a tanulmány során ténylegesen felhasznált szempontok arányát tükrözik. A táblázat külön sorokban tartalmazza azokat a szempontokat is, amelyek egyszerű értékadással nem voltak értelmezhetők, ezáltal nem vettek részt a feldolgozásban.

| | A vizsgálati szempontrendszer struktúrájára és feldolgozottságára vonatkozó összesített adatok | Kiértékelés darabszám alapján | A teljes esetszámhoz viszonyított százalékos érték |
|---|---|---|---|
| 1 | A vizsgálati csoportok száma | 5 | |
| 2 | A vizsgálati szempontok száma | 70 | |
| 3 | A szempontrendszerben szereplő valamennyi szempont és azokhoz kapcsolódó alszempontok összessége | 152 | |
| 4 | A legalacsonyabb tényezőszám egy vizsgálati szemponton belül | 1 | |
| 5 | A legmagasabb tényezőszám egy vizsgálati szemponton belül | 9 | |
| 6 | A szempontrendszer feldolgozottsága a főszempontok alapjána | 65/70 | 92% |
| 7 | A szempontrendszer feldolgozottsága (főszempontokat és alszempontokat is figyelembe véve) | 131/152 | 86% |
| 8 | A szempontrendszer kihasználtsága a benne szereplő összes vizsgálati szempont és a tanulmány során ténylegesen felhasznált szempontok arányának vizsgálatával | 38/70 | 54% |
| 9 | Egyszerű értékadással nem értelmezhető szempontok száma | 5 | 7% |
| 10 | Egyszerű értékadással nem értelmezhető (al)szempontok száma | 21 | 13% |

*3. Ábra: A szempontrendszer szerkezeti jellemzői és feldolgozottsága Forrás: Saját szerkesztésű*

A bemutatott adatok így nem csupán a vizsgálati szempontrendszer méretéről és szerkezetéről adnak képet, hanem arról is, hogy a kiválasztott módszertan milyen mértékben

volt alkalmas ezek tényleges vizsgálatára. Az értelmezhetetlen szempontok külön rögzítése pedig hozzájárul a feldolgozás határait kijelölő keret tisztázásához.

**A vizsgálati szempontok megjelenése és összefüggései az esettanulmányokban**

A 4. táblázat a vizsgálati szempontok előfordulási gyakoriságát, valamint a munkabalesetekhez vezető tényezők számát és típusait mutatja be. Kiemelten szerepelnek benne azok a szempontok, amelyek a leggyakrabban vagy legritkábban fordultak elő az esettanulmányokban, valamint azok is, amelyek egyáltalán nem lettek felhasználva a vizsgálatok során. A táblázat kitér a szabálytalanságok tudatosulására, valamint arra is, hogy a munkáltatóknál a közvetlen kiváltó okokon túl feltártak-e további munkavédelmi hiányosságokat.

| | A vizsgálati szempontok gyakoriságára és munkavédelmi tudatosságot vizsgáló kérdések | Vizsgálati tényezők száma | Előfordulás | Százalékos érték |
|---|---|---|---|---|
| 1 | A legtöbbször előforduló vizsgálati szempontok sorszámai, valamint ezek előfordulási gyakorisága | 10 | 8 | |
| 2 | A második leggyakrabban előforduló vizsgálati szempontok sorszámai, valamint ezek előfordulási gyakorisága | 12 | 6 | |
| 3 | A harmadik leggyakrabban előforduló vizsgálati szempontok sorszámai, valamint ezek előfordulási gyakorisága | 4,11,14,17,65 | 5 | |
| 4 | A legkevesebb alkalommal előforduló vizsgálati szempontok, sorszámai, valamint ezek előfordulási gyakorisága | 3,7,34,38,40,41,43, 46,47,49,52,57,67, 68 | 1 | |
| 5 | Nem használt vizsgálati szempontok, sorszámai, valamint darabszáma | 5,6,8,9,13,15, 22,25,26,27,28,29, 30,35,36,37,39,42, 44,45,48,50,51,55, 56,58,60,61,62,63, 69,70 | 32 | |
| 6 | A balesetek kiváltó okaként megjelölt vizsgálati szempontok sorszámai, valamint ezek előfordulási gyakorisága | 4,7,14,16,17,18,19, 20,21,23,24,32,47, 49,53,63,65,66 | 5,1,1,1,4,1,1,1,11,1, 4,4,1,1,1,2,5,1 | |
| 7 | Azon szabálytalanságok száma melyről tudott a munkáltató | | 19 | |
| 8 | Azon szabálytalanságok száma melyről tudott a munkavállaló | | 27 | |
| 9 | Azon munkáltatók száma melyeknél a felügyelők más munkavédelmi hiányosságot is feltártak azon kívül ami közvetlenül a balesetet okozta | | 16 | 55% |

*4. Ábra: A vizsgálati szempontok előfordulási gyakorisága és a szabálytalanságok megoszlása*
*Forrás: Saját szerkesztés*

### A kutatási eredmények összegzése és értelmezése

A kutatás során alkalmazott vizsgálati szempontrendszer és annak gyakorlati alkalmazhatósága több dimenzióban is vizsgálatra került. A 3. táblázat adatai alapján a szempontrendszer összesen 70 főszempontot tartalmaz, melyekhez további alszempontok kapcsolódnak. Ezek összesen 152 vizsgálati tényezőt foglalnak magukba. A feldolgozhatóság szempontjából a szempontrendszer 92%-os lefedettséget mutatott a főszempontok, és 86%-os feldolgozottságot a teljes tényezőszám viszonylatában, amint az a 3. ábra sorai közül egyértelműen kiolvasható.

A 3. ábrában szintén szereplő információ, hogy 21 olyan (al)szempont volt, amely nem volt egyértelműen kódolható és ezáltal nem kerülhetett be a vizsgálati rendszerbe. Ezek leggyakrabban olyan elemek, amelyek egyéni adat megadását (pl. felelős személy nevét) várták el, és nem voltak alkalmasak az egyszerű értékadással történő feldolgozásra. Ennek figyelembevétele különösen fontos a szempontrendszer jövőbeli finomhangolása során.

A 4. ábra értelmezése rávilágít arra, hogy a vizsgálati szempontrendszer mely elemei fordultak elő leggyakrabban és melyek maradtak teljesen kihasználatlanok. A gyakorisági eloszlás bemutatása nemcsak a munkavédelmi gyakorlatban leginkább jellemző tényezők azonosítását teszi lehetővé, hanem utal arra is, mely területeken lenne szükséges a jövőben átgondoltabb adatgyűjtés vagy következetesebb vizsgálati metodika. A táblázat sorai közül kiderül, hogy vannak olyan szempontok, amelyek minden esetben előkerültek, míg mások egyszer sem kerültek megjelölésre a feldolgozott 29 eset egyikében sem. Fontos kiemelni, hogy egy szempont alacsony előfordulása nem jelenti annak irrelevanciáját, csupán az adott mintában nem volt domináns, de más környezetben vagy jövőbeli esetek során lényegessé válhat.

A fenti értelmezések rávilágítanak arra, hogy a szempontrendszer nemcsak a balesetek azonosítására, hanem azok strukturált és komplex feltárására is alkalmas eszköz lehet. A torzítások, mint például a szöveges esettanulmányok rövidítéséből adódó információvesztés vagy a többszörös besorolások, ugyan jelen vannak, de az alkalmazott módszer és a szempontrendszer jövőbeli fejlesztése e hibák minimalizálására irányulhat. A részletes vizsgálat tehát nemcsak az egyes balesetek okainak feltárásához járulhat hozzá, hanem a teljes munkavédelmi rendszer megbízhatóságának értékeléséhez is.

## KÖVETKEZTETÉSEK, JAVASLATOK

A kutatás során elsődleges célként jelent meg annak vizsgálata, hogy egy hatósági balesetkivizsgálás során készült esettanulmány a megfelelő módszertani átdolgozást követően mennyiben alkalmas strukturált, adatközpontú értelmezésre. A vizsgálat négy fő dimenzió mentén haladt: a szempontok átalakíthatósága, a tényleges relevancia vizsgálata, a szempontok közötti összefüggések feltárása, valamint a matematikai vagy logikai műveletekkel történő következtethetőség lehetősége.

A kutatás első szakaszában a módszertani útmutatóban szereplő szempontok átalakíthatóságának vizsgálata került előtérbe, melynek eredményei a 3. táblázatban kerültek összefoglalásra. Az adatok alapján elmondható, hogy a Nemzetgazdasági Minisztérium Munkavédelmi Irányítási Főosztálya által kiadott „Módszertani útmutató a munkabalesetek hatósági vizsgálatához” című dokumentumban szereplő szempontok 92%-át, a teljes ténye-

zőkészlet 86%-át sikerült úgy átdolgozni, hogy azok teljes mértékben alkalmazhatók legyenek a vizsgálatban. Azokat a tényezőket, amelyek a kutatás során figyelmen kívül maradtak, leginkább olyan konkrét információk alkották – például a munkairányító neve –, amelyek nem relevánsak a kutatás céljai szempontjából. A vizsgálati szempontrendszert tehát sikeresen át lehetett alakítani úgy, hogy az alkalmas legyen az esettanulmányok strukturált, azonosítható és értelmezhető feldolgozására.

A kutatás második szakaszában az egyes vizsgálati szempontok relevanciájának elemzése került előtérbe, melynek eredményeit a 4. ábra tartalmazza. Az ábra első hat sora azokat a szempontokat jeleníti meg, amelyeknél a relevancia mértéke a strukturáltan rögzített válaszok összesítésével kvantitatívan is kinyerhető. Az alkalmazott vizsgálati rendszer lehetőséget biztosított arra, hogy minden vizsgálati pont egységes módon jelölhető legyen az esettanulmányokban, amennyiben az abban megjelent. Ennek köszönhetően egy olyan egységes adatstruktúra jött létre, amelynek értelmezése az alkalmazott szempontrendszer ismeretében válik lehetővé. A rendszer alkalmas arra, hogy képet adjon arról, milyen típusú hiányosságok fordultak elő leggyakrabban a vizsgált esetekben, és megmutassa, mely konkrét szabálytalanságok voltak a legjellemzőbbek.

A 4. ábra 7., 8. és 9. sora azonban már olyan kiegészítő vizsgálati szempontokat is tartalmaz, amelyek nem szerepelnek a hivatalos módszertani útmutatóban, de a kutatás során szükségesnek bizonyult bevezetésük. Kiemelendő ezek közül a „Tudott róla” szempont, mely lehetőséget biztosított annak rögzítésére, ha az esettanulmányban szerepel olyan felügyelői megállapítás, amely szerint a munkáltató vagy a munkavállaló tudatosan követte el a szabálysértést. A szándékos szabálysértés feltárása a hatósági kivizsgálás egyik kulcsfontosságú eleme, és figyelmen kívül hagyása csökkentette volna a kutatás reprezentációs érvényességét, még akkor is, ha e szempont nem szerepel formálisan a hivatalos útmutatóban.

A „Tudott róla” szempont értelmezése egységesebb értelmezési keretrendszert igényel, ami rávilágított arra, hogy a szempontok közötti kapcsolatokat már a vizsgálat kezdeti szakaszában is figyelembe kell venni.

## ÖSSZEFOGLALÁS

A tanulmány célja annak vizsgálata volt, hogy a „Módszertani útmutató a munkabalesetek hatósági vizsgálatához” című dokumentumban foglalt szempontok milyen mértékben strukturálhatók olyan formában, amely lehetővé teszi a munkabaleseti esetek egységesebb, gépi úton is feldolgozható reprezentációját. Az elemzés során a vizsgálati szempontrendszer tartalmi és formai szempontból került átalakításra, melynek eredményeként megállapíthatóvá vált, hogy a rögzített szempontok 92%-a matematikailag is értelmezhető módon újrastrukturálható. Ez megerősíti annak lehetőségét, hogy az útmutatóban szereplő tudás megfelelő adaptációval egy jövőbeni döntéstámogató rendszer alapját képezheti. A kutatás első szakasza így megteremtette az alapjait egy olyan gépi tudásbázis kialakításának, amely az emberi szakértelmet támogatva hozzájárulhat a munkabiztonság hatékonyságának növeléséhez. A további kutatás célja ezen strukturált rendszer tesztelése, valamint a belőle nyerhető mélyebb relációk és összefüggések feltárása lesz. Ennek eredményeit egy következő tanulmány fogja bemutatni.

## FELHASZNÁLT IRODALOM

[1] "Munkahelyi biztonsági és egészségvédelmi stratégiák | Safety and health at work EU-OSHA." Accessed: Apr. 17, 2025. [Online]. Available: https://osha.europa.eu/hu/safety-and-health-legislation/osh-strategies
[2] "Munkahelyi biztonság és egészségvédelem – Európai Bizottság." Accessed: Apr. 17, 2025. [Online]. Available: https://employment-social-affairs.ec.europa.eu/policies-and-activities/rights-work/health-and-safety-work_de
[3] "GINOP-5.3.4-16 A munkahelyi egészség és biztonság fejlesztése (A PÁLYÁZAT LEZÁRULT!) | Széchenyi Terv Plusz." Accessed: Apr. 17, 2025. [Online]. Available: https://archive.palyazat.gov.hu/ginop-534-16-a-munkahelyi-egszsg-s-biztonsg-fejlesztse
[4] "31989L0391 A Tanács irányelve 1989. június 12 a munkavállalók munka..." Accessed: Apr. 17, 2025. [Online]. Available: https://jogkodex.hu/doc/9663062#s78
[5] "Munkavédelem, Foglalkoztatás-felügyelet." Accessed: Apr. 17, 2025. [Online]. Available: https://mvff.munka.hu/#/munkabaleseti_statisztika
[6] B. Katalin, "Semmelweis Egyetem Népegészségtani Intézet Foglalkozás-orvostan Szakvizsga-előkészítő tanfolyam Munkavédelem 1".
[7] "MANDRIK ISTVÁN A MUNKAVÉDELEM HELYZETE, FEJLESZTÉSI IRÁNYAI, KÜLÖNÖS TEKINTETTEL A MAGÁNBIZTONSÁGI MUNKAKÖRÖKRE".
[8] "Accidents at work statistics - Statistics Explained." Accessed: Apr. 17, 2025. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Accidents_at_work_statistics
[9] "SZAKPOLITIKAI TÁJÉKOZTATÓ BIZTONSÁGOS ÉS EGÉSZSÉGES MUNKAHELYEK EURÓPÁBAN: HOGY ÁLLUNK 2023-BAN?", Accessed: Apr. 17, 2025. [Online]. Available: https://www.etuc.org/en/pressrelease/huge-fall-labour-inspections-raises-covid-risk
[10] "A munkavédelemi kockázatkezelés sajátosságai megtekintése." Accessed: Apr. 22, 2025. [Online]. Available: https://bk.bgk.uni-obuda.hu/index.php/BK/article/view/100/108
[11] "A munkavégzéssel összefüggő balesetek és megbetegedések költségének nemzetközi összehasonlítása | Safety and health at work EU-OSHA." Accessed: Apr. 17, 2025. [Online]. Available: https://osha.europa.eu/hu/publications/international-comparison-cost-work-related-accidents-and-illnesses
[12] "A munkabalesetek és foglalkozási megbetegedések nemzetgazdasági költségei".
[13] "NAPO." Accessed: Apr. 17, 2025. [Online]. Available: https://www.napofilm.net/en
[14] "OSHwiki | European Agency for Safety and Health at Work." Accessed: Apr. 17, 2025. [Online]. Available: https://oshwiki.osha.europa.eu/en
[15] "Online interactive Risk Assessment |." Accessed: Apr. 17, 2025. [Online]. Available: https://oira.osha.europa.eu/en
[16] "Magyar Közlöny." Accessed: Apr. 17, 2025. [Online]. Available: https://magyarkozlony.hu/
[17] "Nyitólap." Accessed: Apr. 17, 2025. [Online]. Available: https://www.mszt.hu/hu-hu/
[18] "Szabványkönyvtár." Accessed: Apr. 17, 2025. [Online]. Available: https://www.szabvanykonyvtar.hu/

[19] "ISO – Nemzetközi Szabványügyi Szervezet." Accessed: Apr. 17, 2025. [Online]. Available: https://www.iso.org/home.html
[20] "CEN-CENELEC - CEN-CENELEC." Accessed: Apr. 17, 2025. [Online]. Available: https://www.cencenelec.eu/
[21] "A MUNKAVÉDELEM NEMZETI POLITIKÁJA 2024-2027", Accessed: Apr. 19, 2025. [Online]. Available: https://www.mindbank.info/item/1489
[22] "Munkavédelem, Foglalkoztatás-felügyelet." Accessed: Apr. 19, 2025. [Online]. Available: https://mvff.munka.hu/#/nemzetgazdasagi_jelentesek
[23] A. J. Porcelli, M. R. Delgado, C. Opin, and B. S. Author, "Stress and Decision Making: Effects on Valuation, Learning, and Risk-taking," *Curr Opin Behav Sci*, vol. 14, p. 33, Apr. 2017, doi: 10.1016/J.COBEHA.2016.11.015.
[24] "How Stress Impacts Decision Making | Walden University." Accessed: Apr. 19, 2025. [Online]. Available: https://www.waldenu.edu/online-masters-programs/ms-in-clinical-mental-health-counseling/resource/how-stress-impacts-decision-making
[25] "Mesterséges intelligencia segíti a bőrbetegségek felismerését a Semmelweis Egyetemen (Frissítve) – Semmelweis Hírek." Accessed: Apr. 19, 2025. [Online]. Available: https://semmelweis.hu/hirek/2022/03/24/mesterseges-intelligencia-segiti-a-borbetegsegek-felismereset-a-semmelweis-egyetemen/?utm_source=chatgpt.com
[26] J. ŻYWIOŁEK, "EMPIRICAL EXAMINATION OF AI-POWERED DECISION SUPPORT SYSTEMS: ENSURING TRUST AND TRANSPARENCY IN INFORMATION AND KNOWLEDGE SECURITY," *Scientific Papers of Silesian University of Technology. Organization and Management Series*, vol. 2024, no. 197, pp. 679–695, 2024, doi: 10.29119/1641-3466.2024.197.37.
[27] "MTMT2: Szabó G. Informatikai rendszerüzemeltetés minőségbiztosítása. (2010) HADMÉRNÖK 1788-1919 5 1 323-324." Accessed: Apr. 22, 2025. [Online]. Available: https://m2.mtmt.hu/api/publication/2001575
[28] B. Silva, F. Hak, T. Guimaraes, M. Manuel, and M. F. Santos, "Rule-based System for Effective Clinical Decision Support," *Procedia Comput Sci*, vol. 220, pp. 880–885, Jan. 2023, doi: 10.1016/J.PROCS.2023.03.119.
[29] "Az elmélettől a gyakorlatig: Mind the Graph Blog." Accessed: Apr. 19, 2025. [Online]. Available: https://mindthegraph.com/blog/hu/kutatasi-modszerek/?utm_source=chatgpt.com
[30] "Numerikus problémák a kvalitatív megbízhatósági mutatók meghatározásánál." Accessed: Apr. 19, 2025. [Online]. Available: https://9dok.org/document/y6e083p4-numerikus-probl%C3%A9m%C3%A1k-a-kvalitat%C3%ADv-megb%C3%ADzhat%C3%B3s%C3%A1gi-mutat%C3%B3k-meghat%C3%A1roz%C3%A1s%C3%A1n%C3%A1l.html
[31] A. Z. Mitev, "Grounded theory, a kvalitatív kutatás klasszikus mérföldköve (Grounded theory, the classic milestone of qualitative research)," *Vezetéstudomány / Budapest Management Review*, pp. 17–30, Jan. 2012, doi: 10.14267/VEZTUD.2012.01.02.
[32] V. Sallay and T. Martos, "A Grounded Theory (GT) módszertana," *Magyar Pszichológiai Szemle*, vol. 73, no. 1, pp. 11–28, Mar. 2018, doi: 10.1556/0016.2018.73.1.2.
[33] "Munkavédelem, Foglalkoztatás-felügyelet." Accessed: Apr. 19, 2025. [Online]. Available: https://mvff.munka.hu/#/esettanulmanyok

[34] “Knowledge Representation in AI | GeeksforGeeks.” Accessed: Apr. 19, 2025. [Online]. Available: https://www.geeksforgeeks.org/knowledge-representation-in-ai/?utm_source=chatgpt.com

DOI: https://doi.org/10.12700/btsz.2025.7.3.209

# PANDEMICS FROM AN OCCUPATIONAL SAFETY PERSPECTIVE – REVIEW HISTORY OF WORLD EPIDEMICS FROM THE POINT OF VIEW OF OCCUPATIONAL

# VILÁGJÁRVÁNYOK MUNKAVÉDELMI SZEMPONTBÓL – ÁTTEKINTÉS VILÁGJÁRVÁNYOK TÖRTÉNELME MUNKAVÉDELEM SZEMSZÖGÉBŐL

SIMON Mátyás[1]

**Abstract**

Analyzing the history of pandemics and the procedures used to create safe working conditions and mapping the connection points. Throughout human history, the study of epidemics shows that defenses against epidemics have constantly changed and evolved. Many pandemics have put humanity and healthcare to the test, where in addition to the use of personal protective equipment, collective defenses were also of prime importance in order to reduce biological risks. Epidemics also pose serious challenges to today's advanced health care worldwide, where occupational health and safety has played a prominent role. The regulations defined in the laws, standards, and documents related to health and safety at work help to a great extent to create appropriate and safe working conditions and to choose appropriate and effective personal protective equipment.

**Keywords**

epidemic, biological risk, hospital safety, personal protective equipment, collective protection, vaccination

**Absztrakt**

A világjárványok történelmének és a biztonságos munkavégzés feltételeinek megteremtéséhez alkalmazott eljárás rendek elemzése és a kapcsolódási pontok feltérképezése. Az emberi történelem során a járványok tanulmányozása azt mutatja, hogy a járványok elleni védekezése folyamatosan változott és fejlődött. Számos világjárvány próbára tette az emberiséget és az egészségügyet, ahol az egyéni védőeszközök használatán felül a kollektív védelmek is kiemelt fontossággal bírtak a biológiai kockázatok csökkentése érdekében. A járványok a mai fejlett egészségügyet is komoly kihívások elé állítja világszerte, ahol kiemelt szerepet kapott a munkavédelem. Az egészséges és biztonságos munkavégzésre vonatkozó jogszabályokban, szabványokban, munka-védelemmel kapcsolatos dokumentumok-ban meghatározott előírások nagymérték-ben segítik a megfelelő és biztonságos munkakörülmények kialakítását, a megfelelő, hatékony egyéni védőeszközök kiválasztását.

**Kulcsszavak**

járvány, biológiai kockázat, kórházbiztonság, egyéni védőeszköz, kollektív védelem, védőoltás

[1] matyas.simon86@gmail.com | 0000-0002-2714-857X | PhD Student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

## INTRODUCTION

The study of epidemics throughout human history shows that epidemics started in specific geographical areas and spread relatively quickly because the optimal conditions for spread were in place. The optimal conditions for transmission are the source of infection, the vector organism and the susceptible organism.

The emergence and spread of epidemics can be linked to the development of trade, geographical discoveries, the outbreak of wars, poverty and famine. The rapid spread and high infectiousness of pandemics was fuelled by overpopulation, poor sanitation, poor medicine and a lack of knowledge about pathogens and transmission.

In the 15th century, for example, geographical exploration brought measles, smallpox, influenza and plague to the New World, but the indigenous peoples' immune systems were immune to these infections. It is believed that the infectious diseases introduced by the conquistadors caused more casualties than the wars of conquest. discoveries brought to Europe by the return of the conquistadors include syphilis and typhoid fever.

## HISTORICAL OVERVIEW OF PANDEMICS

Among the epidemics that have affected mankind, I would highlight the following, which have had a major impact on the development of medicine and the treatment of diseases, and thus on the development of occupational safety and personal protective equipment in the health sector.

The first description of the epidemic is attributed to Thucydides, who witnessed the great Athenian plague. Based on his descriptions, it was for a long time unclear to medical science what kind of infection ravaged Athens in 430 BC, because the symptoms described suggested a variety of diseases. However, a paleomicrobiological study carried out in 1995 clearly identified the causative agent of typhoid fever. Rash typhus - typhus exanthematicus - is primarily caused by the cellular parasitic bacterium Rickettsia prowazekii, which lives in the clothes mite (less commonly in the head mite). The louse sheds the pathogen in its faeces, which enters the skin through micro-wounds caused by scratching when bitten by another individual. The louse is only a vector in the infection cycle, while the host pathogen (reservoir function) is the infected individual. It typically shows winter seasonality, because in cold weather, people living in poor sanitary conditions clean less frequently, change and wash clothes less often, and live in more crowded conditions, crowded together in small spaces. Symptoms start 1-2 weeks after infection, followed by high fever, chills, headache, muscle aches. A few days later, small rashes appear on the trunk and body folds, which later spread to the limbs. Some skin lesions may bleed (petechiae) or purpurae may develop as a result of already confluent petechiae. The acute phase lasts about 2 weeks without complications. A long-term consequence of untreated or inadequately treated typhoid fever is that the infection can reactivate, which is known as Brill-Zinsser disease. Rash typhoid fever is a typical epidemic of the army and wars, sometimes referred to as "prison fever". In the 16th century, it was called the dishonourable "morbus hungaricus" or "lues pannonicus" (Hungarian disease) because it was spread throughout Europe by mercenaries who flocked to liberate Buda and then dispersed after the siege. The disease is not to be confused with Hash typhus, which is caused by Salmonella typhi. [2] [3]

The second most deadly of all the epidemics that have ever struck humanity was perhaps the plague. The Black Death has caused several epidemics and pandemics in Europe, with some estimates suggesting that nearly 200 million people have fallen victim to the plague to date. The first pandemic appeared in the mid-14th century, with bubonic plague and pneumonic plague described as spreading in parallel, taking victims in Europe, North Africa, the Middle East and Central Asia. The causative agent of plague is the bacterium Yersina pestis, which is transmitted mainly by the bite of fleas that feed on rodents. The bacterium causes a lesion in the flea's intestinal tract, causing the insect to vomit the blood it has sucked out into a wound, along with the pathogen, thus infecting the host. The bacterium can cause three types of disease. Symptoms include fever, nosebleeds, headaches, limb pain, confusion, and the appearance of painful lumps. Lymph nodes swell, black patches appear on the skin, especially on the fingertips and nose, and then turn bluish-black and fade due to haemorrhages. Septicaemic plague develops when the bacterium enters the bloodstream. Symptoms include high fever, chills, headache, malaise, haemorrhages in the skin and internal organs. Fatal within 36 hours without treatment. Pneumonic plague is spread from person to person by droplet infection - sneezing, coughing. It is faster and more severe than bubonic plague because the bacteria enter the lungs directly, bypassing the lymph nodes. Incubation period is 1-3 days with a 95% mortality rate.

The spread of the plague in the Middle Ages was facilitated by economic and demographic changes: food shortages and famine, population migration, urban migration, the arrival of overland caravans and merchants on the sea routes. There were various ways of stopping the spread of the plague: cutting the veins, opening the buboes, smoking aromatic plants, but the most effective was the quarantine and the establishment of quarantine hospitals (Lazzaretto Vecchio). Plague doctors were used to treat the sick and register the dead in the affected municipalities. Figure 1 shows the spread of the bubonic plague in 1347-51.

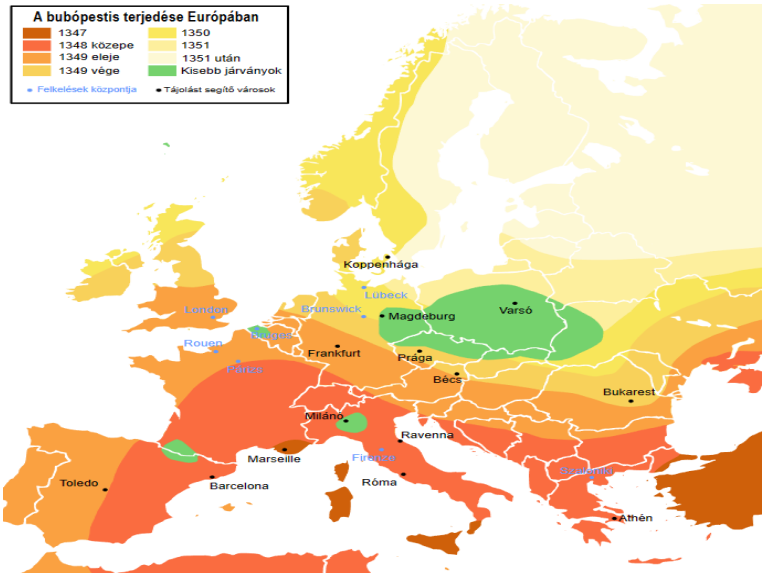



*Figure 1. The spread of the 1347-51 plague in Europe [10]*

The first biological warfare was linked to the plague: in 1346, Mongol troops used catapults to transport carcasses infected with the plague bacterium to the city of Kaffa (now Feodosia), which allowed them to easily occupy the plague-stricken town.

Endemic plague hotspots still occur today, with most cases in East Africa, but outbreaks have also occurred in the United States, New Mexico and Colorado; the most at risk area is the island of Madagascar. [2] [11] [3]

The third is leprosy or Hansen's disease (old Hungarian name: bélpoklosság), a chronic, infectious disease caused by Mycobacterium leprae. The incubation period varies, from a few months to up to 40 years. Several clinical forms are known:

"good-tempered", slow-moving leprosy, which mainly attacks the skin and surrounding nerves, and

the rapid-onset variant, which is highly contagious, forms nodules (leprosy) on the skin, attacks both the nervous system and the viscera. Severe nerve damage results in loss of pain sensation, often leading to loss of limbs and fingers. It is also characterised by dysfunction of the facial muscles, eyebrows falling out, destruction of the nasal cartilage (lion's face).

The origin of the disease is uncertain, with written references to it dating back to ancient Egypt, but in Europe it became a devastating epidemic during the Crusades, especially in the Middle Ages. As the disease proved to be incurable, it was used to prevent the spread of infection.

In the beginning, leprosy patients were expelled from the settlements, they had to walk around with a colomb or a sceptre in their hands, wear a dark hooded coat, gloves and a hat to be recognised and from the 12th to 13th centuries leprosy asylums - leprosariums - were established where the patients were cared for by monks.

Mass outbreaks began to disappear from the 16th century onwards, thanks to the successful isolation of infected people, the population's resistance to bacteria and improved hygiene. The disease is still present today - see Figure 1.4 for an example of new cases worldwide in 2021 - although a combination of antibiotic drugs - the first effective drug only produced in 1946 - can achieve a complete cure. Treatment is expensive and lengthy, which is why leprosy hospitals are still in operation in many countries, mainly in Africa and South America. [2] [12]

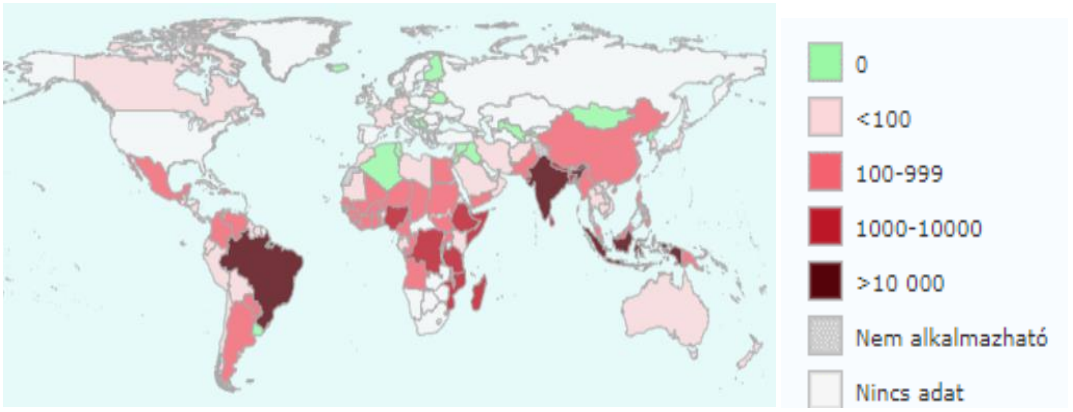



*Figure 2 New leprosy cases in 2021 [13]*

It is important to mention cholera, which appeared in Europe in the 1830s, until then an endemic disease mainly in subtropical India.

The disease is caused by the bacterium Vibrio cholerae. It is mainly transmitted enterally through faeces, vomit and sewage and raw food in contact with them. It usually originates in warm coastal estuaries rich in organic matter and spreads from there.

Two types are distinguished: European cholera (cholera nostras) and Asian cholera (cholera asiatica). Unlike Asian cholera, European cholera is not seen all year round, but only in the second half of summer.

The pathogen can survive for days in aqueous media, preferring alkaline media. It cannot withstand drying and even weak acid (0.1 parts per thousand hydrochloric acid) will kill it. Its mechanism of action is to alter the ionic flux in the cells of the intestinal wall, thus inhibiting the ability of the intestinal wall to absorb water. The course of the disease usually depends on the degree of weight loss suffered by the patient, which can be as much as 8-12% of the infected individual's own body weight lost within a few hours. If the body's mobilisable water reserves are depleted, vomiting and diarrhoea will temporarily cease, but with repeated intake of water these symptoms will reappear. The limbs become characteristically greyish and shrivelled, and the characteristic vox cholerica symptom develops. Death is ultimately due to the salt and water malabsorption associated with dehydration, followed by kidney failure, confusion, fever and other symptoms. Antibiotic treatment and vaccination are not fully effective, and prevention of the disease, proper hygiene and education of the population at risk are necessary.

In 1831, cholera appeared in our country, which was known in medical and popular language as contagious biliary dysentery or biliary ejaculation. According to the available data, major epidemics broke out in 1831-32 and 1872-73, during which nearly 1 000 000 people fell ill and more than 400 000 died. [2] [11]

Cholera is still present today - Figure 1.5 shows the number of cases reported in 2016 - although the last cases occurred in our country in 1916, Peru between 1991-98, Haiti in 2010 and Yemen in 2017.

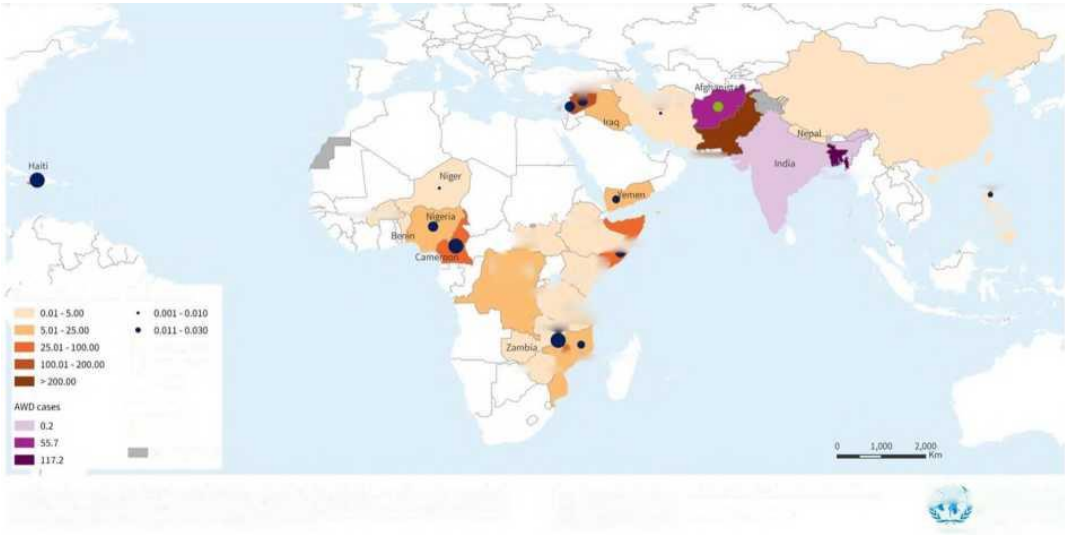



*Figure 3 Case numbers of cholera cases reported in 2016 [14]*

Smallpox was one of the most deadly infectious diseases known until 1977. With the development and use of an appropriate vaccine, 1979 was the first year in which no smallpox cases were recorded.

The most deadly smallpox disease is caused by Poxvirus variolae, which is transmitted from human to human by contact and has no animal vector. The virus enters the lymph nodes via the mucous membranes of the respiratory tract, where it multiplies and damages the small blood vessels of the skin, causing red rashes and spots to form all over the body, which later develop into blisters with purulent, burning pain. The blisters bleed and turn black, hence the name.

Smallpox epidemics in Europe peaked in the 18th century, with some estimates putting the death toll at 60 million. Those who survived often suffered permanent damage, as the infection attacked the nervous system, causing paralysis, convulsions, osteomyelitis, ophthalmia and blindness. The rashes only dried up weeks later, leaving lifelong smallpox scars. [2] [5]

The ancient Chinese realised that those who had been infected with smallpox had acquired immunity to possible re-infection later. This observation is the basis of variolation, a procedure derived from the Latin name for smallpox, in which a sample of the patient's rash was taken and passed through the nasal mucosa or a pointed instrument through the skin into another person's body.

In the late 1700s, vaccination, a newer form of protection against smallpox, appeared. Like variolation, the method was based on observation: in England it was recognised that dairymaids and cows who had contracted cowpox (variola vaccina), a much milder form of cowpox than smallpox, which appeared on the skin and udder of cattle, became immune to smallpox after the disease. In this spirit, the next step in artificial immunisation was vaccination against cowpox. [15]

In the early days, smallpox secretions were passed from "arm to arm", using "smallpox couriers", which meant that the secretions from the body of one vaccinated person were passed on to another. Its effectiveness is debatable, because 'smallpox couriers' often recovered before they could pass on the 'vaccine'. A more effective method has been found to be the placing and transporting of dried smallpox pellets in a bottle and vaccinating with it.

Smallpox is the only infectious disease eradicated worldwide. Today, it is only found at the CDC - Center for Disease Control and Prevention - in Atlanta and the Vektor Virology and Biotechnology Institute in Koltsovo. In our country, vaccination against smallpox was carried out between 1876 and 1980. [2]

In 1918, the world's most devastating epidemic to date was the Spanish flu, caused by the H1N1 influenza A virus, which was neither Spanish nor a flu. Its name is linked to World War I, as the countries at war learned of the epidemic from the press in neutral Spain, hence its name. Its point of origin was Kansas, and the virus arrived in the spring with American troops in southern Europe and spread from there. Initially the pandemic was mild, characterised by weakness, lethargy and fever lasting 3-4 days. The epidemic peaked in October and November 1918, and from December onwards the number of victims declined, with an estimated 3-5% of the world's total population killed, more than in World War I. The Spanish flu was characterised by three waves in one year, was severe and rapid, with high fever and head and limb pain. Most patients got better after a few days, but in some it

rapidly progressed to haemorrhagic pneumonia, often leading to death in just a few hours. Viral pneumonia particularly affected 20-40 year olds, which was explained by the victims' immune systems overreacting to the infection and destroying lung tissue. Deaths in older people and those in risk groups - people with chronic diseases, metabolic disorders, etc. - were more likely to be caused by secondary bacterial pneumonia.

The third wave was not uniform, it was more of a post-epidemic and was much milder than the second wave, with the exception of China. [2] [3] [5]

Of all the pandemics, influenza viruses are the ones that cause the highest number of cases of illness worldwide each year. The reason is that the antigen of the virus is highly variable, with new variants emerging periodically, against which the human body cannot defend itself. It typically evolves very rapidly, and can make someone ill in a matter of hours. It is an infectious respiratory disease with common symptoms (e.g. lethargy, fever, muscle aches), can have serious complications (e.g. lung, myocarditis, meningitis) and can be fatal. It is estimated that around 50 million people died from influenza or complications of influenza in the 20th century.

The flu virus has 3 major groups A, B, C and D:

Pandemics are caused by virus A because the surface antigens of the virus are in a constant state of flux. The change is usually slow and partial (drift), but can also be rapid and complete (shift). The previously acquired immunity of the population is ineffective against the new pathogen with the changed antigenic structure. The A virus occurs in two major variants in nature in human and avian strains.

Type B flu is rarer, mainly affecting humans (seals and ferrets have been shown to be susceptible), and mutates more slowly than type A, making those who have had it immune for a time, thus not causing a pandemic.

"Type C: most commonly spread in children (dogs and pigs are also susceptible to C virus infection), usually causes mild illness, but rarely more severe illness and local outbreaks can occur.

"Type D: spread among pigs and cattle, not yet detected in humans.

Influenza is easily spread from person to person, mainly through direct contact with infectious patient secretions, such as liquid droplets released into the air when coughing or exhaling. It is also spread by secretions on hands, handkerchiefs and surfaces touched by patients. [2] [6]

The seasonal presence of influenza is illustrated in Figure 4, which shows the continuous presence of the virus in temperate and cold climates, typically in winter, and in the tropics almost all year round.

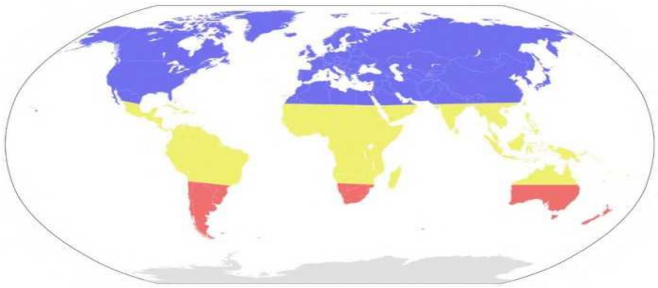


*Figure 4 Influenza season: November-April (in blue), April-November (in red), and rainy season (in yellow) [16]*

Coronaviruses are RNA zoonoses with a lipid envelope. There are (currently) 7 known species of human coronaviruses:

4 species are almost constantly present in the human environment and therefore immune to them, usually causing a mild disease with mild symptoms and a moderate to mild course. The disease, which has symptoms similar to colds and respiratory illnesses, mainly affects the elderly and children, especially in winter.

However, 3 species - SARS (Severe Acute Respiratory Syndrome) CoV; MERS (Middle East Respiratory Syndrome) CoV, and SARS-CoV-2 (Coronavirus Disease-19) - can cause serious and even life-threatening illness, such as SARS, which caused a pandemic in 2003, and MERS-CoV, which emerged in the Middle East in 2012.

The Covid-19 virus can spread intensively in both dry, cold and tropical, high humidity environments, typically through droplet infection, direct or indirect contact with infected secretions. The virus can survive for a few hours on some surfaces (copper, cardboard) and up to several days on others (plastic and stainless steel). However, the amount of viable virus decreases over time and is rarely present on surfaces in sufficient quantities to cause infection. Infection can occur if someone touches their nose, mouth or eyes with their hands and their hands have been contaminated with virus- contaminated fluid or surfaces. The incubation period is usually 5-6 days, but it can be detected in respiratory samples after 1-2 days, and is infectious 48 hours after the onset of symptoms. Patients with mild to moderate COVID-19 remain infectious for up to 10 days after the onset of symptoms, while severe or critical patients may remain infectious for up to 20 days after the onset of symptoms. [17]

The clinical picture can be most often mild to moderate, with symptoms ranging from mild respiratory tract infection to non-severe pneumonia, or severe to critical - 5% incidence - in cases such as respiratory failure, septic shock.

The disease may also be associated with mental and neurological symptoms (e.g. loss/temporary loss of sense of taste, smell, confusion, depression, sleep disturbance) and complications (e.g. acute pulmonary embolism, stroke, delirium).

Their resistance is low, dying within minutes at 50 ºC and within a few days in the outside world, but they can remain infective for 1-2 weeks in cold, winter weather. They are inactivated within minutes by common disinfectants. Both alcohol and hypochlorite-based agents are effective against them. [2] [17] [7]

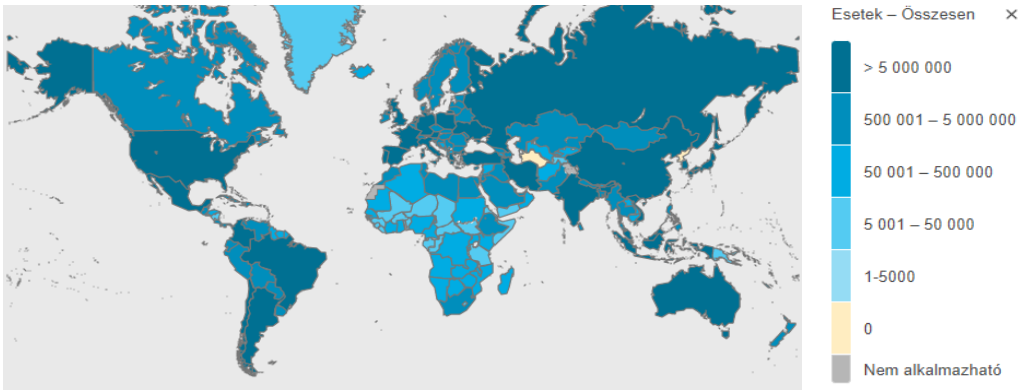



*Figure 5 Registered Covid-19 case numbers [18]*

Although their pathogenic factors are different, parallels can be drawn based on their emergence, spread and epidemiological factors and their prevention and treatment. The epidemics described above are summarised in Figure 6.

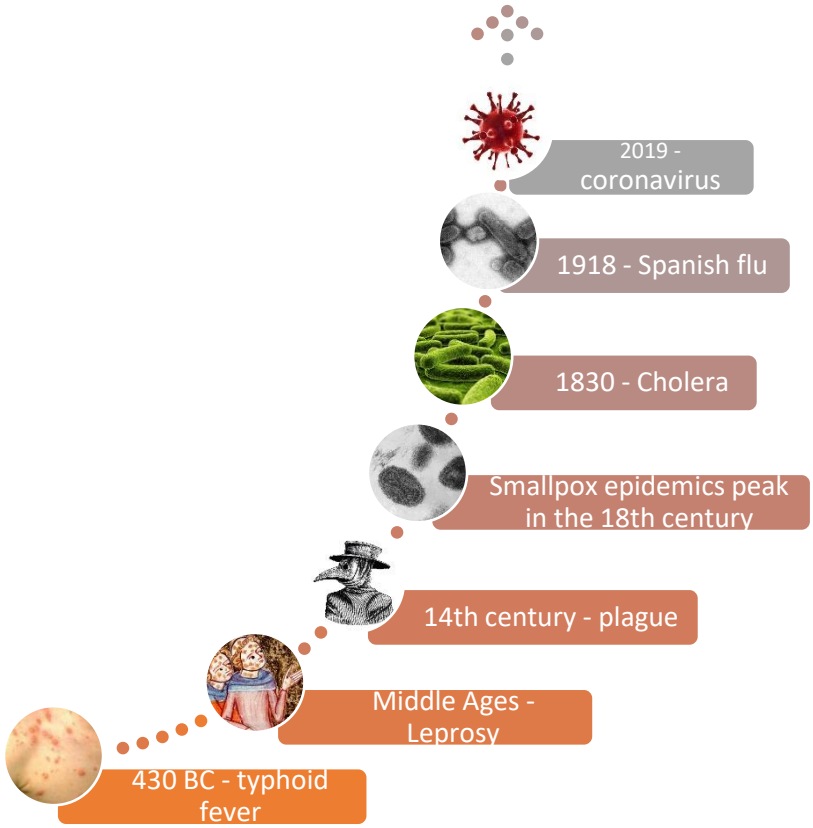



*Figure 6 Time scale of epidemics (author's own editing)*

## PREVENTION OPTIONS PAST AND PRESENT

In antiquity, and later in the Middle Ages, the appearance of infectious diseases was seen as a punishment from the gods for having committed some kind of blasphemy. Prevention was therefore not common at the time. The Greek historian Thucydides (460 BC - 395 BC) made many valuable observations during the Peloponnesian War, which were later useful for medical science. He noted, for example, that crowding plays a role in the spread of disease, that personal contact and encounters cause further infections, and that infected people acquire a certain immunity to disease. However, it was only centuries later that these findings became facts about the incidence and spread of infectious and communicable diseases.

One of the earliest preventive measures was to keep people away from the sick, often in the form of exile or expulsion from settlements. Written records of the isolation of the sick date to the plague epidemic of 549 BC, when the Emperor Justinian ordered the isolation of people from infected areas. The spread of infectious diseases from person to person was recognised as early as the time of Hippocrates. Hippocrates (460 BC - 377 BC), the famous physician of his time, believed that many diseases were caused by polluted and toxic air, and fire was developed to purify the air in line with the thinking of the time. Fragrant grasses such as cypress, juniper and spruce were often burned as firewood. Another effective method was to rub them with essential oils.

According to the medical theory of the time, diseases were caused by changes in the ratio of body fluids - blood, bile and mucus - and were treated by cutting the blood vessels or by spitting [2] [3]

The primary task of prevention today is to prevent an epidemic from developing, which is only successful if one of the primary drivers is eliminated, which it can be:

- identification of an infectious agent
- stopping the spread of
- general prevention procedures:
    - personal hygiene - hand washing, cleaning
    - environmental hygiene - disinfection, rodent control
    - health education
- specific protection - medicines, vaccines

Faragó's study and research found that employers have made significant efforts to protect the health of their employees and prevent the spread of the coronavirus epidemic, which required a significant amount of fundamental change from the way companies operated before the epidemic. [1] As Simon puts it in his study: 'the new procedures, instructions and professional documentation that were created as part of the pandemic response confirmed that the risks to workers in the health sector are complex and that the occupational safety, occupational health and occupational hygiene disciplines need to work together and rely on each other to identify risks effectively and determine the necessary employer actions'. [4]

**Quarantine**

The method of controlling imported epidemics by not only isolating but also monitoring suspected infected persons during the incubation period (quarantine) began during the great plague epidemic of the Middle Ages. It was recognised that it was not only contact with sick persons that posed a threat, but also the clothes and personal belongings of the sick person. During the epidemics of the 14th century, the authorities of the Italian cities ordered the isolation of the cities and areas affected by the epidemics for public health reasons, the control and observation of travellers before they could enter the city; sanitary decrees were issued, doctors were employed and the cleanliness of the cities was regulated. From the 1350s onwards, quarantines began to be established in coastal towns in places far from settlements, in many cases on separate islands or enclosed by moats with drawbridges. When the quarantine appeared, crews of ships arriving in port had to stay on a remote island or small settlement for 30 days before being allowed to enter the city. In 1464, the Venetian Senate decreed that two men of noble birth from each sestieri (town hall) should be selected,

who, on regular income, should transport suspected plague sufferers to the island of Lazzaretto and arrange for the evacuation of the infected person's house. This decree also defined the duties of the epidemiologists: to examine and isolate suspected patients, to search for persons in contact with the infected person (nowadays called contact tracing) and, naturally, to treat them. The island of Lazzaretto was divided into two parts: one part was the quarantine itself and the other part was the "convalescent" area, where citizens released from quarantine had to stay for another 40 days.

The first quarantine decree was made in 1377 in Ragusa (now Dubrovnik), during the plague epidemic, when places declared quarantine were closed to residents for 30 (later 40) days and local residents were not allowed to approach, with only the town physician-in-chief having the right of access to observe the quarantined. The very word quarantine - guarded isolation - refers to this, deriving from the Italian 40 days: 'quaranti giorno'. The buildings were surrounded by high walls and a beach, and guards were often posted to prevent escape attempts by those inside. In the quarantines, medicinal herbs were often smoked, used to make decoctions and to boil the patients' clothes. The curative effect of herbal decoctions is questionable, but 'disinfecting' clothes and fumigation, e.g. against lice, may have been one of the most effective methods.

Written material on quarantine measures in Hungary only survives from the 18th century. A sanitary decree issued by Maria Theresa in 1770 regulates in detail the duration of the quarantine, the order of the guard duty and the location of the "quarantine stations". In the neighbouring countries, 'plague spies' were often sent to watch for the spread of the epidemic, and in the event of an increased risk of epidemic, plague doctors and plague officers were appointed to inspect and supervise the quarantine stations (quarantine house, contumacy house, quarantine).

In London in the late 18th century, a signal was introduced on ships entering port if there was a sick person on board: a yellow rectangular flag with the letter "Q" had to be placed on the mast. During yellow fever, suspicious ships arriving in Philadelphia were fumigated or even burned, which proved effective against the mosquitoes that caused the epidemic.

Quarantine measures can seriously infringe on the freedom of some citizens, so from 1851 onwards, International Public Health Conferences were held to standardise the rules on quarantine - especially to prevent the spread of cholera, plague and yellow fever; to define the principles of control of epidemic diseases; to standardise the operation of quarantines and to establish international cooperation. These conferences were the forerunners of the World Health Organization (WHO), which was established in 1946.

In the second half of the 20th century, the sheer volume of international travel, the huge traffic at airports and ports, the fact that an epidemic from anywhere in the world could appear anywhere in the world in a matter of hours, called into question the use and effectiveness of quarantines.

During the 2019 pandemic COVID-19, the concept of quarantine and "home quarantine", which could be in our country, came to the fore again:

- Epidemiological surveillance: observation of an individual suspected of being infected (e.g. in their home). No contact is allowed.

- Epidemic lockdown: a special form of epidemiological surveillance where patients or suspected infected persons are isolated in a special room or ward and can only enter with appropriate protective equipment. It can be partial or total isolation.
- Epidemiological surveillance: surveillance of an infectious person for the duration of a vector clearance. During this period, the person may be prohibited from certain activities, such as work or school visits, and may be required to undergo laboratory testing. [2]

**Personal protective equipment**

Nowadays, personal protective equipment is defined as any device worn by the worker to reduce the risks arising from the work or technology to a level that does not endanger health.21 The "first personal protective equipment" was the face mask, which was first worn during the plague epidemic of the 1350s,

although the face mask with a long nose ("beak") did not really serve a protective function. According to the 'miasma' theory of the time, the disease was attributed to bad, noxious air, against which the elongated nose, worn by doctors and sanitary workers in the presence of the patient, was the appropriate 'protection'. The beak often contained scented plants (e.g. myrrh, thyme, cloves), which were an adequate protection against 'bad smells'.


*Figure 7 Face mask used during a plague outbreak [19]*

Medical history dates the first appearance and wearing of medical protective clothing to the 16th century. Charles de Lorm, a French doctor, was the first to wear a long goatskin coat, knee breeches, a hat, gloves, boots and a red stick, in addition to a 'beak' mask, to draw attention to the risk of infection. The first surgical gloves, operating caps, gowns and gowns made of sterile materials were first worn in 1896 by Jan Mikulicz-Radecki, a Polish-Austrian doctor. The rubber glove was invented in 1902 by American surgeon William Halstead. The use of masks began to spread in operating theatres in 1905, but their importance and effectiveness was proven during the Spanish flu epidemic of 1918-1919.

*Figure 8 Personal protective equipment used during the Spanish Flu [20]*

The personal protective equipment of the present day is not even comparable to the above mentioned equipment, as protective equipment has undergone a huge evolution and the requirements, testing and marking are laid down in harmonised standards.


*Figure 9 Personal protective equipment used in modern times during a coronavirus epidemic [21]*

## Vaccinations

Artificially-acquired immunity is achieved by vaccination, which involves the introduction of killed or weakened pathogens into the body, triggering the same immunological process as natural infection, but without symptoms or complications.

The first written documentation of the "vaccination" comes from a book on medicine by Li Shizhen, a Beijing physician. This cannot yet be considered an actual vaccination, because at that time inoculation was used in two different images:

- using a piece of cotton to take a sample of nasal secretions from a patient who had already had smallpox, drying and grinding them, or
- the dried stitches on top of the smallpox were ground into a powder and blown into the nostril of the person to be vaccinated.

The procedure following inoculation is scarification, whereby the surface of the skin is broken and the smallpox powder is rubbed into the resulting open wound.

The history of vaccination actually began with the introduction of the smallpox vaccine, which initially caused much controversy. The breakthrough came when Edward Jenner, MD, took a sample from a child who had been cured of smallpox.

The first vaccine to be produced in a laboratory setting was developed by Pasteur in 1897, when he discovered that hens treated with a weakened vaccine did not become ill after an experiment with the poultry cholera pathogen. He then began experiments with the rabies virus - Rabies lyssavirus - and paved the way for the development and production of vaccines. The real preventive vaccine was Pasteur's colleague Gaston Ramón, who in 1923 added formaldehyde to diphtheria toxin, causing it to lose its toxicity. When inoculated into the body, it stimulated the production of antibodies but did not cause serious illness.

In the domestic context, we should mention Endre Hőgyes (1847-1906), a doctor whose merit is the perfection of the vaccination method. Instead of Pasteur's 'dehydration' method, which was used to weaken the virus, he used the 'dilution' method still used today.

In 1905, the paediatricians Clemens Pirquet (1874-1929) and Béla Schick (1877-1967) discovered a symptom called "serum sickness" (allergy), which followed the administration of a vaccine. Pirquet observed that a person who had received the horse serum vaccine a second time would become violently itchy, flushed and have difficulty breathing. In the course of their research, they discovered the role of proteins in triggering allergy and antibody production. [2]

The most effective way to prevent epidemics is immunisation, which can be:

- active: they release killed or killed pathogens into the body, stimulating the body's defences in a process that mimics natural infection. The vaccine, which can be:
  - live, weakened - e.g. measles,
  - inactivated - e.g. influenza,
  - subunit (purified surface antigen) and split (cleaved),
  - containing a weakened toxin,
  - conjugated,
- passive: where immunisation is achieved by the introduction of specific antibodies against a particular pathogen.
- There are different types of vaccinations:
  - age-related, compulsory
  - mandatory in case of disease risk - e.g. rabies
  - recommended to avert the risk of disease - e.g. hepatitis
  - job-related - e.g. for healthcare workers: hepatitis B
  - travel-related - e.g. malaria
  - other - e.g. HPV

In the 18th century, the effectiveness of vaccines was questioned and people distrusted them because of their poor purity and contamination with other pathogens. These factors have now been eliminated by modern medicine, but vaccines administered can still have risks and contraindications:

- dangers:
  - vaccine reactions: local and general symptoms - e.g. itching, fever, scarring
  - complications
  - extinguishing accident:
- the vaccine does not contain a sufficiently attenuated pathogen,

- vaccination administered incorrectly,
- administration of other vaccines
- contra-indications, which are not recommended for vaccination:
  - febrile illness,
  - an immunodeficiency condition,
  - pregnancy,
  - previous vaccine-related complications - e.g. anaphylaxis [8]

**Disinfection and sterilisation**

The use of high temperatures - "sterilisation" - in medicine was already seen in ancient Rome, but in the Middle Ages it was less common. The pioneer of antiseptic surgery was the English surgeon Joseph Lister (1827-1912), who observed that patients who underwent surgery often developed infections and had a high mortality rate. Pasteur's studies led him to conclude that bacteria had to be destroyed before they could enter the surgical wound. To disinfect hands and surgical instruments, he used carbolic acid - nowadays phenol. In a domestic context, we should mention the name of Ignác Semmelweis (1818¬1865), who made it compulsory to wash hands with chlorme lime solution in the obstetrics department of the Szent Rókus Hospital, after he realised that puerperal fever was caused by doctors and medical students, because they examined women in labour with the same hands as the dead without disinfection.

Nowadays, disinfection includes all procedures and methods aimed at destroying pathogens that have escaped from the infectious source into the external environment, or at eliminating (inactivating) their infectiousness.

The disinfectant effect is defined as those chemical, physical, physico-chemical factors which, in direct contact with micro-organisms, at an appropriate intensity and activity, cause their destruction or inactivation during a defined period (exposure time or exposure period). In terms of the magnitude of the effect, it can be:

- physical process - use of thermal and radiant energy
- chemical process - compounds with antimicrobial properties
- combined process - a combination of physical and chemical effects

The procedures are shown in the figure below.

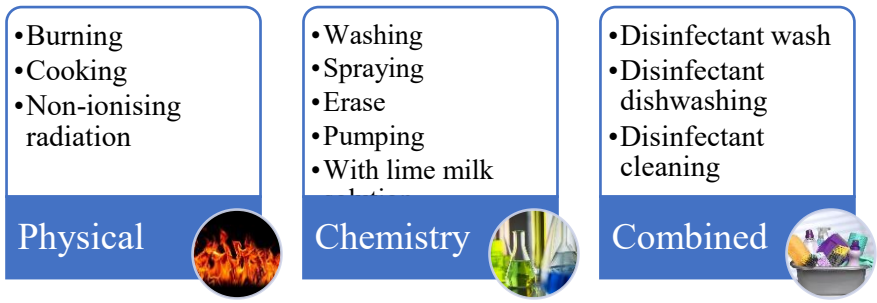



*Figure 10 Types of disinfection procedures (edited by the author)*

Sterilisation is an antimicrobial process that uses physical, chemical or a combination of these to irreversibly inactivate microorganisms and all their dormant forms on the material or substance to be sterilised. Sterilisation can be carried out in many ways: heat, filtration, radiation, chemical agents. The choice of method must be made according to the requirements, taking into account the quality of the materials and equipment used and the effect of the sterilisation process on them. The decisive criteria are to preserve the quality and function of the materials to be sterilised and to ensure sterility. [9] [22]

Sterilisation procedures to be used:

- autoclave
- heat sterilizer
- gas sterilizer with ethylene oxide, formaldehyde
- plasma sterilizer
- in a solution of antimicrobial substances
- filtering

## SUMMARY

In today's advanced, fast-changing world, an infection can cause a pandemic much sooner than in the pre-20th century, one reason being unrestricted travel and free access to countries. The most common pandemic today is caused by viruses of the influenza family.

Epidemics pose serious challenges to today's advanced healthcare systems worldwide, and governments and hospitals must act with similar speed to stop infection and care for seriously ill patients. Fighting the virus is made more difficult by the fact that health workers are frequently infected.

Alongside health, occupational safety and health has been given a prominent role. The requirements laid down in legislation, standards and documents relating to occupational safety and health - risk assessments, the provision of personal protective equipment and the organisation of occupational health examinations - greatly help to ensure that the right working conditions are created and that the right, effective personal protective equipment is selected. Personal protective equipment has evolved enormously over the centuries.

In addition to the use of personal protective equipment, collective protection is also a priority in the health sector and to reduce biological risks. Examples of this are the sterilisation and disinfection procedures described, and the use of vaccines against the various viruses that cause epidemics. Thanks to today's modern medicine and the development of research laboratories, attempts to develop vaccines against viruses can be started quickly and vaccination can be carried out as soon as possible after the virus emerges.

## LITERATURE USED

[1] Faragó F. (2021): COVID-19 and occupational safety: a quantitative survey of the coronavirus control practices of Hungarian companies, SAFETY STUDIES 3 : 4 pp. 113-131. , 19 p.
[2] Felkai P. (2022) The History of Epidemics Budapest.
[3] Czefener D., Fedeles T. (2021): Pécs-Budapest: birding guide - PTKE-Kronosz Kiadó.

[4] Simon, M. (2022) Occupational safety of COVID-19: Occupational safety measures and consequences of the coronavirus pandemic in the health care sector.
[5] Szakály S., Kincses K. M. (2021): From leprosy to the Spanish flu, Scientia et Securitas - Scientific Bulletin, Vol. 2, No. 3, 332-341.
[6] Katalin Meglécz (2012):The history of pandemics and the reasons for their emergence - journal article in Military Engineer Vol.VII No.1: 91-98.
[7] Miklós Kásler (2020):Manual for the prevention and therapy of infections caused by the new coronavirus (SARS-CoV-2) (COVID-19) identified in 2020 - Ministry of Human Resources, Budapest.
[8] Venyingi B., Vitályos Á. G. (2018). Epidemiology for BA students in Infant and Young Child Education – Eötvös Publishing, Budapest
[9] Z. Pechó, M. Milassin (2000):Information on disinfection (Details from the third, revised, expanded edition) - "Johan Béla" National Centre for Epidemiology, Budapest, Hungary
[10] Roger Zenner, Ogodej, https:// commons.wikimedia.org/wiki/File:Pestilence_ spreading_1347- 1351_europe.png, downloaded 23.03.2025.
[11] Epidemics of Everyday Life - Diseases of Historical Times https://ri.abtk.hu/images/letoltes _publ/mende.balazs/jarvanytan.pdf, downloaded 23.03.2025.
[12] THE TRUST, https://semmelweismuseum.blog.hu/2020/04/29/a_belpoklossag, retrieved 23.03.2025.
[13] LEPRA, https://apps.who.int/neglected_diseases/ntddata/leprosy/leprosy.html, downloaded 23.03.2025.
[14] LEPRA,https://cdn.who.int/media/images/default-source/emergencies/disease-outbreak-news/ map_global_cholera_don.jpg?sfvrsn=424d2ed9_5, retrieved 23.03.2025.
[15] THE BLACK SKY'S FIRST ISSUE, https://semmelweismuseum.blog.hu/2020/04/29 /a_belpoklossag, downloaded 23.03.2025.
[16] INFLUENZA, https://commons.wikimedia.org/wiki/File:Influenza_Seasonal_Risk_Areas.svg, retrieved 23.03.2025.
[17] ECDC - European Centre for Disease Prevention and Control, https://www.ecdc.europa.eu/en/covid-19/questions-answers/questions-answers-basic-facts, downloaded 23.03.2025.
[18] WHO Coronavirus (COVID-19) Dashboard, https://covid19.who.int/, retrieved 23.03.2025.
[19] Plague Doctor in the Early Modern Era, https://mnl.gov.hu/mnl/szszbml/a_pestis, retrieved 23.03.2025.
[20] Study on Spanish Flu Debunks Equal Vulnerability Theory, Highlights Environmental, Social, Nutritional Factors, https://weather.com/en-IN/india/health/news/2023-10-11-new-study- contradicts-that-spanish-flu-impacted-healthy-and-frail, retrieved 23.03.2025.
[21] PHOTOREPORT: COVID-ELLATAS AT AITK-N, https://semmelweis.hu/hirek/2021/03/18/ fotoriport-covid-ellatas-az-aitk-n/downloaded 23.03.2025.

[22] Health education materials for all - Disinfection 2023, http://egeszsegugy.hupont.hu/ Viewed 23.03.2025.

**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