ISSN 2676-9042

Vol 7, No 4, 2025.

2025, VII. évf. 4. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

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

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
Composition (detail) | **Kompozíció (részlet)**
painting | című festménye látható

© Bors Györgyi, 2022

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

epa.oszk.hu

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

MATARKA

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

Óbudai Egyetem Digitális Archívum

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

dk Országos Széchényi Könyvtár - Digitális Könyvtár

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

ULRICHSWEB™ GLOBAL SERIALS DIRECTORY

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

doi Foundation

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

Edited by Editorial Board | Szerkeszti a Szerkesztőbizottság

Chairman of the Editorial Board | A Szerkesztőbizottság elnöke
Prof. Dr. RAJNAI Zoltán
rajnai.zoltan@bgk.uni-obuda.hu

Scientific Secretary of the Editorial Board, person responsible for editing | A szerkesztőbizottság tudományos titkára, a szerkesztésért felelős személy
Dr. Dr. habil. KOLLÁR Csaba PhD
kollar.csaba@uni-obuda.hu

Members of the Editorial Board | A szerkesztőbizottság tagjai
Prof. Dr. BÁNÁTI Diána banati@mk.u-szeged.hu
Dr. BEREK László PhD berek.laszlo@uni-obuda.hu
Prof. Dr. BEREK Tamás PhD berek.tamas@uni-nke.hu
Prof. Dr. BESENYŐ János besenyo.janos@uni-obuda.hu
Prof. Dr. CVETITYANIN Lívia akadémikus cpinter.livia@bgk.uni-obuda.hu
Prof. Dr. Dragan JOVANOVIĆ draganj@uns.ac.rs
Prof. Dr. Jeffrey KAPLAN kaplan@uwosh.edu
Prof. Dr. KOVÁCS Tünde PhD kovacs.tunde@bgk.uni-obuda.hu
Dr. Cyprian Aleksander KOZERA PhD c.kozera@akademia.mil.pl
Prof. Dr. Maashutha Samuel TSHEHLA samuel@sun.ac.za
Prof. Dr. Manuela TVARONAVIČIENĖ manuela.tvaronaviciene@vgtu.lt
Dr. habil. NAGY Rudolf PhD nagy.rudolf@bgk.uni-obuda.hu

Staff of the Editorial Board | A szerkesztőbizottság munkatársai
BELÁZ Annamária, SZALÁNCZI-ORBÁN Virág

English language lecturer | Angol nyelvi lektor
Dr. BEKE Éva PhD

Technical editor | Technikai szerkesztő
HARTMANN László

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

The Journal's Professional-Scientific Advisory Board | **A Folyóirat Szakmai-Tudományos Tanácsadó Testülete**

Chairman of the Advisory Board | A Tanácsadó Testület elnöke

Prof. Dr. GODA Tibor DSc.
Az Óbudai Egyetem Biztonságtudományi Doktori Iskola vezetője

Members of the Advisory Board in alphabetical order | A Tanácsadó Testület tagjai ABC sorrendben

Prof. Dr. HAIG Zsolt mk. ezredes
A Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola vezető helyettese
A Védelmi elektronika, informatika és kommunikáció kutatási terület vezetője

Prof. Dr. KÓNYA Zoltán DSc.
A Szegedi Tudományegyetem Környezettudományi Doktori Iskola vezetője

Prof. Dr. KORINEK László akadémikus
A Magyar Rendészettudományi Társaság elnöke

LONTAI Márton
A Nemzeti Szakértői és Kutató Központ főigazgatója

Prof. Dr. PADÁNYI József DSc. mk. vezérőrnagy
A Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola vezetője
A Magyar Hadtudományi Társaság elnöke

Prof. Dr. RÉGER Mihály DSc.
Az Óbudai Egyetem Anyagtudományok és Technológiák Doktori Iskola vezetője

TIKOS Anita
Women In IT Security (WITSEC) Egyesület elnökségi tagja

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 4, 2025. | **2025. VII. évf. 4. szám**

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

ANTAL Tímea

timea.antal0@gmail.com

Dr. Tímea ANTAL is a compliance lawyer with thirteen years of management experience. She spent eighteen years working in European Union and domestic development policy, both in public administration and in the public sector using resource support. As a department head, she managed the implementation of public administration development programs in an organization performing official tasks. From 2018, she was the operational director of Új Világ Nonprofit Szolgáltató Kft. for three years, where she was responsible for operating IT system of development policy that ensured the use of many billions of forints. Since 2021, she has been working as a legal advisor at KBKB Kék Bolygó Klímavédelmi Befektetési Alapkezelő Zártkörűen Működő Részvénytársaság (KBKB Blue Planet Climate Protection Investment Fund Management Private Limited Company), and from 2024, she will also be working as a legal advisor at MÁV Zrt. In addition to gaining practical experience, the lessons learned from academic study also play a significant role in her professional life. She has presented her research findings on various aspects of compliance and artificial intelligence at academic conferences in Hungarian and English, and has published articles on these topics, with others currently being reviewed and awaiting publication.

Dr. ANTAL Tímea tizenhárom évnyi vezetői tapasztalattal rendelkező compliance szakjogász. Tizennyolc évet töltött az európai uniós és a hazai fejlesztéspolitikában, közigazgatási és forrástámogatást felhasználó állami közegben egyaránt. Főosztályvezetőként hatósági feladatokat ellátó szervezetben irányította a közigazgatás-fejlesztési programok megvalósítását. 2018-tól három éven át operatív igazgató az Új Világ Nonprofit Szolgáltató Kft.-ben, ahol sok ezermilliárd forint felhasználását biztosító fejlesztéspolitikai-informatikai rendszer működtetésért felelt. 2021 óta a KBKB Kék Bolygó Klímavédelmi Befektetési Alapkezelő Zártkörűen Működő Részvénytársaságnál, 2024-től pedig a MÁV Zrt.-nél is jogtanácsosként tevékenykedik. A gyakorlati tapasztalatszerzés mellett a tudományos elmélyülés tanulságai is jelentős szerepet játszanak szakmai életében. A compliance és a mesterséges intelligencia különböző aspektusait vizsgáló kutatási eredményeiről tudományos konferenciákon tartott magyar és angol nyelvű előadásokon számolt be, valamint cikkei jelentek meg, illetve lektorálás és megjelenés alatt vannak e tárgykörben.

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 kutatás-fejlesztési projekt szakmai irányítója és résztvevője, aki a mérnöki tudományok elméleti alapjait a fenntartható energetikai megoldások gyakorlati alkalmazásával ötvözi.

BEDNÁRIK Boldizsár

bednarik.boldizsar@uni-obuda.hu

Boldizsár BEDNÁRIK is a software architect and researcher, a PhD student at the Doctoral School on Safety and Security Sciences of Óbuda University

BEDNÁRIK Boldizsár szoftverarchitekt és kutató, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusza 2024 óta. Egyetemi diplomával

since 2024. He holds a bachelor's degree in Electronics and Telecommunication and a master's degree in Information Technology. He has more than fifteen years of professional experience in full-stack software development, DevOps, system design, hardware-level development, and AI-based systems. His scientific work focuses on the application of large language models (LLMs) in safety- and security-critical environments, the related cybersecurity risks, and the predictive use of this technology.

rendelkezik Elektronika és Telekommunikáció, valamint mester diplomával Információs Technológiák szakon, és több mint tizenöt éves szakmai tapasztalata van full-stack szoftverfejlesztés, DevOps, rendszertervezés, hardverközeli fejlesztés és mesterséges intelligencia-alapú rendszerek területén. Tudományos munkája a nagy nyelvi modellek (LLM-ek) biztonságkritikus környezetekben való alkalmazására, az ezekhez kapcsolódó kiberbiztonsági kockázatokra, valamint a technológia prediktív alkalmazására fókuszál.

BEREK László

berek.laszlo@uni-obuda.hu

László BEREK graduated as an information specialist–librarian from Eötvös Loránd University, after which he obtained qualifications as a system informatics specialist and library expert. He defended his doctoral dissertation at the Doctoral School of Safety and Security Sciences of Óbuda University in 2024. Over the past twenty years, he has gained extensive professional experience in scientific and academic libraries, and since 2015 he has served as Director of the University Library of Obuda University. His research interests include the security of online scholarly communication, research ethics, plagiarism detection and the identification of AI-generated texts, as well as university rankings and related scientometric issues. He is the author of four university textbooks used in the doctoral programmes of two doctoral schools at Óbuda University, and he teaches the course "Research Publication Skills" at the Doctoral School of Innovation Management. In recent years, he has developed several e-learning materials. He is a member of five committees at Obuda University, including the Scientific Council, the Ranking Committee, the Greenmetric Committee, the IT Committee, and the Artificial Intelligence Transition Committee. He also serves as a board member of the Technical Librarians' Section of the Association of Hungarian Librarians.

BEREK László az Eötvös Loránd Tudományegyetemen végzett informatikus könyvtárosként, ezt követően rendszerinformatikusi és könyvtári szakértői képesítést szerzett. Doktori értekezését az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában védte meg 2024-ben. Az elmúlt húsz évben tudományos és egyetemi könyvtárakban szerzett szakmai tapasztalatot, 2015 óta az Óbudai Egyetem Egyetemi Könyvtárának igazgatója. Kutatási területei közé tartozik az online tudományos kommunikáció biztonsága, a tudományetika, a plágiumellenőrzés és a mesterséges intelligencia által generált szövegek detektálása, továbbá az egyetemi rangsorok és a kapcsolódó tudománymetriai kérdések. Négy egyetemi tankönyv szerzője, amelyeket az Óbudai Egyetem két doktori iskolájának programjaiban használnak, emellett az Innovációmenedzsment Doktori Iskola „Kutatási publikációs ismeretek" című kurzusának oktatója. Az elmúlt években több e-learning tananyagot is kidolgozott. Az Óbudai Egyetem öt bizottságának tagja, köztük a Tudományos Tanácsé, a Ranking Bizottságé, a Greenmetric Bizottságé, az Informatikai Bizottságé és a Mesterséges Intelligencia Átállási Bizottságé. Emellett a Magyar Könyvtárosok Egyesülete Műszaki Könyvtáros Szekciójának elnökségi tagja.

GOGOLÁK László

gogolak@mk.u-szeged.hu

Dr. László GOGOLÁK was born in 1984 in Topolya and earned his degree in mechatronic engineering at the University of Novi Sad, Faculty of Technical Sciences, where he also completed his PhD in technical sciences. He is currently an associate professor at the University of Szeged, Faculty of Engineering, in the Institute of Mechatronics and Automation. His teaching activities cover BSc courses in control engineering, sensors, actuators, process control, and mechatronic case studies, as well as MSc-

Dr. Gogolák László 1984-ben született Topolyán, okleveles mechatronikai mérnöki diplomát szerzett az Újvidéki Egyetem Műszaki Tudományok Karán, majd ott fejezte be PhD-ját is műszaki tudományokból. Jelenleg a Szegedi Tudományegyetem Mérnöki Kar Mechatronikai és Automatizálási Intézetének főiskolai docense. Oktatói tevékenysége kiterjed BSc-n az irányítástechnikára, szenzorokra, aktuátorokra, folyamatirányításra és mechatronikai esettanulmányokra, valamint MSc-n az

level control engineering. His research focuses on modern technologies such as indoor localization methods, measurement and testing equipment, industrial camera-based machine vision, EtherCAT-based servo drives, and IO-Link sensor systems. He has also published works on topics such as the design and application of EtherCAT and serial communication-based servo control systems.He is a member of the Higher Education Control Engineering Methodological Association and contributes as a program coordinator to the MSc in mechanical engineering. Through CEEPUS and Erasmus programs, he has completed study visits in Slovakia, Romania, Croatia and Slovenia. His scientific work is supported by an active publication record, available on major academic platforms such as Google Scholar and Scopus.

irányítástechnikára. Kutatásai fókuszában olyan modern technológiák állnak, mint beltéri lokalizációs eljárások, mérő- és tesztelő berendezések, ipari kamerás gépi látás, valamint EtherCAT-alapú servo-hajtások és IO-Link alapú szenzorrendszerek fejlesztése. Emellett publikált olyan tanulmányokat, mint az EtherCAT és soros kommunikáció alapú szervovezérlő rendszer tervezése és alkalmazása. Tagja a Felsőoktatási Irányítástechnikai Oktatásmódszertani Egyesületnek, és szakfelelősként is részt vesz a gépészmérnök MSc képzésben. Tanulmányútjai során CEEPUS és Erasmus ösztöndíjakkal járt Szlovákiában, Romániában, Horvátországban, Szlovéniában. Tudományos tevékenységének eredményességét mutatja az aktív publikációs munka, amely megtalálható több tudományos portálon.

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.

KERTAI-KISS Ildikó

kertai.kiss.ildiko@gmail.com

She has been working in organization and management science since 2008, including in the consulting industry (organizational development, organizational diagnostics, leadership development, mentoring) and in higher education for more than 10 years as an applied psychologist, university lecturer and supervisor. As a PhD student at the PhD School of Safety and Security Science, University of Óbuda, since 2014, he has been working on functional issues of safety in socio-technical systems (management and organization science), safety culture, organizational behaviour, risk analysis of organizational processes and the organizational background of human error. In addition to teaching and re-

Szervezés-és vezetés tudománnyal 2008. óta foglakozik, ezen belül a tanácsadó iparban (szervezetfejlesztés, szervezeti diagnosztika, vezető fejlesztés, mentoring) és a felsőoktatásban több, mint 10 éve dolgozik, mint alkalmazott pszichológus, egyetemi oktató és szakfelelős. Mint az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD-hallgatója, 2014-től, a szocio-technikai rendszerek biztonságának funkcionális kérdéseivel (vezetés - és szervezés tudomány), biztonsági kultúrával, szervezeti magatartással, a szervezeti folyamatok kockázatainak elemzésével és az emberi hibázás szervezeti hátterével foglalkozik. Az oktató és kutató munka mel-

search, he is a member of the research group of the Society of Informatics Economy at Óbuda University and a member of the board of the Culture-Economy Section of the Hungarian Economic Society. In her free time he sings in the Budapest Academic Choir and performs in orchestral productions.

lett, tagja az Óbudai Egyetem Társadalom Informatika Gazdaság, kutató csoportjának, valamint a Magyar Közgazdasági Társaság Kultúra-gazdaság szakosztályának elnökségi tagjaként végez társadalmi munkát. Szabadidejében a Budapesti Akadémiai Kórusban énekel, zenekari produkciókban lép fel.

KISS Gábor

kiss.gabor@bgk.uni-obuda.hu

Dr. habil. Gabor KISS is 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 tanár, 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.

LŐCSEI Anikó

locsei.aniko@bparchiv.hu

Aniko LŐCSEI obtained her MA degree in History (EKF-BTK) through an accredited university program and later received her appointment as an archivist. She participated in several professional conferences in the archival field (2012, 2014, 2016, 2019). Her research primarily focused on the processing and analysis of judicial records and statistics of defendants from various historical periods. In 2017, she was appointed Senior Archivist, later advancing to the position of Advisor. In her professional work, she is involved in developing and maintaining record management systems, databases, and reference tools, as well as supporting academic research groups. Her research direction centers on digital data protection,

Lőcsei Anikó a történettudományi MA diploma (EKF-BTK), akkreditált egyetemi képzését és levéltárosi kinevezését követően, több szakmai konferencián is vett részt levéltári területen (2012, 2014, 2016, 2019). Kutatásai elsősorban a különböző korszakok jogszolgáltatási iratainak és perbe vont személyek statisztikáinak feldolgozására, elemzésére összpontosítottak. 2017-ben főlevéltárosi, később tanácsosi kinevezésben részesült. Munkája során nyilvántartási rendszerek, adatbázisok és segédletek készítésével, valamint tudományos kutatói csoportok támogatásával foglalkozik. Kutatási irányvonala a digitális adatvédelemre összpontosít, különös figyelemmel jelen tanulmányban szereplő témák alapján a digitális doku-

particularly on solutions related to the data security of digital documents discussed in this study, considering both digital and existing records from data protection and data security perspectives. She also explores the application of blockchain technology to enhance data integrity and ensure the authenticity of digital documents.

mentumok adatbiztonságára vonatkozó megoldások alkalmazásával, a digitális és meglévő iratok adatvédelmi, adatbiztonsági szempontjait figyelembe véve. Ezen kívül a blokklánc technológia alkalmazásának vizsgálatával is foglalkozik, amely hozzájárulhat az adatintegritás növeléséhez és a digitális dokumentumok hitelességének biztosításához.

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 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.

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 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.

MÓROCZ Máté

morocz.mate@stud.uni-obuda.hu

I am Máté MÓROCZ, a first-year doctoral student at the Doctoral School of Security Sciences at Óbuda University. I obtained both my bachelor's and master's degrees as a power electrical engineer at the Kandó Kálmán Faculty of Electrical Engineering of Óbuda University. My scientific interests focus on the feasibility, cyber-physical vulnerabilities, and security challenges of digital substations. The aim of my research is to explore how high operational security and cyber-resilience can be ensured in IEC 61850-based automated substation environments, with particular emphasis on the protection of critical infrastructures.

MÓROCZ Máté vagyok, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának elsőéves doktorandusz hallgatója. Alap és mestervégzettségemet erősáramú villamosmérnökként szereztem az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karán. Tudományos érdeklődésem középpontjában a digitális alállomások megvalósíthatósága, kiberfizikai sérülékenységei és biztonságtechnikai kihívásai állnak. Kutatásaim célja annak feltárása, hogy az IEC 61850-alapú automatizált alállomási környezetekben miként biztosítható a villamosenergiarendszerek magas fokú üzembiztonsága és kiberellenálló képessége, különös tekintettel a kritikus infrastruktúrák védelmére.

NAGY Rudolf

nagy.rudolf@bgk.uni-obuda.hu

Dr. habil. Rudolf NAGY, retaired firefighter Colonel, is currently associate professor at Óbuda University. He studied in foreign educational institutions. He served as a CBRN defence officer, and took part in industrial safety tasks. He gained experience as an operations officer in the NATO SFOR mission. After that he became Deputy Head of the Emergency Management Department of Hungarian Nation al Directorate General for Disaster Management. Summa cum laude earned a PhD degree in field of Critical Infrastructure Protection. Later he was appointed Deputy Head of the Disaster Management Training Centre. In civilian life, he worked as an EHS manager. He has been teaching subjects of safety and security sciences since 2015, and is responsible for the fire protection engineering specialization. He obtained a habilitated doctorate in the scientific study of self-ignition.

Dr. habil. NAGY Rudolf nyugalmazott tűzoltó ezredes, jelenleg az Óbudai Egyetem egyetemi docense. Külföldi oktatási intézményekben tanult. Vegyivédelmi tisztként szolgált, és részt vett iparbiztonsági feladatokban. A NATO SFOR misszióban műveleti tisztként szerzett tapasztalatokat. Ezt követően az Országos Katasztrófavédelmi Főigazgatóság Veszélyhelyzetkezelési Főosztályának helyettes vezetője lett. Summa cum laude minősítéssel szerzett PhD fokozatot a kritikus infrastruktúrák védelme területén. Később a Katasztrófavédelmi Oktatási Központ vezetőjének helyettesévé nevezték ki. A polgári életben EHS vezetőként dolgozott. 2015 óta oktatja a biztonságtudományok tantárgyakat, a tűzvédelmi mérnöki specializáció felelőse. Habilitált doktori címet szerzett az öngyulladások tudományos vizsgálatából.

OLÁH Róbert

olah.robert@eotvostechnikum.hu

Robert OLÁH completed his studies as an IT engineer (GDE), a software engineer at ELTE -IK, and an engineering teacher (OE-KVK). He began his career in public education, starting with professional training as a computer programmer at Weis Manfréd Technikum in a school environment. He then continued his professional journey in higher education, where he gained further experience, all of which contributed to his current professional expertise. During his higher education studies, he conducted individual research, which he continued throughout his academic career, focusing on areas such as computer networks, artificial intelligence, machine learning, model creation, and training. He completed his studies in these fields but also gained professional experience independently in the areas of artificial intelligence and networks, which could be the key to his success. One of his main goals is to write publications to showcase his professional work. In the near future, he envisions pursuing studies in PHP systems, particularly in relation to the areas mentioned above.

OLÁH Róbert, mint mérnök informatikus (GDE), programtervező informatikus ELTE -IK, és mérnök tanár (OE-KVK) végezte tanulmányait. Karrierjét a közoktatásban egy szakmai képzés keretében kezdte meg számítástechnikai programozóként (Weis Manfréd Technikum) iskolai környezetben, ezután szakmai útját a felsőoktatásban folytatta, ahol további szakmai tapasztalatokat szerzett, mindez hozzájárultak jelenlegi szakami tapasztalataihoz is. A felsőoktatásban a tanulmányai alatt egyéni kutatásokat végzett, melyet felsőoktatás tanulmányai idején is folytatott (számítógép hálózat, mesterséges intelligencia, gépi tanulás, modellalkotás és betanítás) területén. Tanulmányait ezeken a területen végezte, de otthoni szakmai tapasztalatokat is szerzett mesterséges intelligencia, hálózat témakörében, ami a siker kulcsa lehet. Egyik fő célja publikációk írása, amelyel szakmai munkásságát tudja megismertetni. A közeljövőben PHP rendszereket illető tanulmányait a fenti területen képzeli el.

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

Egyetemi tanár, Az Óbudai Egyetem – Kandó Kálmán Villamosmérnöki Karon működő Elektrofizikai Intézet igazgatója. Szakmai felügyelete alatt zajlik a matematika és fizika tantárgyak oktatása. Kutatási területei közé tartozik a lézerfizika, a napelemes

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

energiarendszerek, a speciális napelemek, atomerőművek és az elosztott paraméterű hálózatok, valamint a fizikaoktatás módszertani fejlesztése. Témavezetőként aktívan részt vesz az 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

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); 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 (MHTT) and its Geoinformation Section. Founder and editor-in-chief of the planetary science portal Planetology.hu.

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) 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 (MHTT) és Geoinformációs Szakosztályának tagja. A Planetology.hu bolygótudományi portál alapító-főszerkesztője.

SEPRÉNYI Patrik

patrik.seprenyi@gmail.com

Patrik SEPRÉNYI, PhD student at the University of Public Service, Doctoral School of Military Sciences. He obtained his bachelor's and master's degrees in International Security and Defence Policy at the same university in 2021 and 2023, respectively. He spent the academic year 2019/2020 at the Beijing International Studies University (BISU). His current doctoral research focuses on analyzing technology related security policy trends in the 21st century from a NATO perspective. He is a member of the Hungarian Association of Military Science and the NATO Youth Atlantic Council. He has worked at the Ministry of Defense and is currently working at the Permanent Delegation of Hungary to NATO as part of the Hungarian Public Affairs Scholarship Program.

SEPRÉNYI Patrik, a Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskolájának doktorandusza. Alap- és mesterszakos oklevelét ugyanezen egyetemen, nemzetközi biztonság- és védelempolitika szakon szerezte 2021-ben, illetve 2023-ban. A 2019/2020-as tanévet a Pekingi Nemzetközi Tanulmányok Egyetemén (BISU) töltötte. Jelenlegi doktori kutatása a 21. századi technológiai verseny biztonságpolitika vonatkozású trendjeinek NATO-szemszögből történő elemzésére fókuszál. A Magyar Hadtudományi Társaság és a NATO Ifjúsági Atlanti Tanács tagja. A Honvédelmi Minisztériumnál dolgozott, valamint Magyarország NATO melletti Állandó Képviseletén dolgozik a Magyar Közigazgatási Ösztöndíjprogram keretében.

SOMOGYI Tamás

somogyit588@gmail.com

Holds a Master's degree in IT engineering and a complementary degree in Legal Studies. He is currently a PhD student at the Doctoral School on Safety and Security Sciences, Óbuda University. His research area is the security issues of the financial sector's infrastructure, with a special focus on natural hazards. He has more than 15 years of experience in the banking industry.

Mérnök-informatikus, mérnök-szakjogász. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának hallgatója. Kutatási területe a bankszektor létesítményi infrastruktúrájának védelme és ellenállóképességének fokozása, elsősorban a természeti veszélyek jelentette fenyegetettséggel szemben. Több, mint 15 év banki munkatapasztalattal bír.

SZÁMADÓ Róza

szamado.roza@bgk.uni-obuda.hu

Dr. SZÁMADÓ Róza is the head of the Adult Education Center at the Bánki Faculty of Óbuda University and an assistant professor. With decades of experience as an organizational development and change management consultant, her professional focus is on human factors. Her work and research focus on what helps organizations to be effective, flexible, and responsive to change. What frameworks, methodologies, and tools can help in this, and what obstacles might there be.

Dr. SZÁMADÓ Róza az Óbudai Egyetem Bánki Kara Felnőttképzési Központjának vezetője és egyetemi adjunktusa. Több évtizedes szervezetfejlesztési és változásmenedzsment tanácsadóként szakmai fókusza az emberi tényezőkre összpontosul. Munkája, kutatása arra irányul, hogy mi segíti a szervezetek hatékonyságát, rugalmasságát és a változásokra adott reagálási képességét. Milyen keretrendszerek, módszertanok és eszközök segíthetnek ebben, és milyen akadályai lehetnek ezeknek.

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.

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

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.

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.

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.

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 4, 2025. | **2025. VII. évf. 4. 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

DOI: https://doi.org/10.12700/btsz.2025.7.4.1

The Role of University Libraries in Protecting Scholarly Output and Improving Institutional Reputation

Az egyetemi könyvtárak szerepe a tudományos kibocsátás biztonságában és az intézményi reputáció erősítésében

BEREK László[1]

Abstract

The quality and credibility of higher education institutions' scientific performance play a key role in strengthening international competitiveness, university ranking positions, and institutional reputation. The aim of this research was to develop a library-based operational model that reviews and supports manuscripts associated with university affiliations before submission, as well as the publication activities of academic staff and researchers. The framework includes journal recommendations, plagiarism and AI-generated text detection, and the optimization of titles, abstracts, and keywords. The system takes into account institutional indicators, ranking expectations (THE, QS), and science communication objectives. By implementing the framework, the institution can reduce research ethics risks, enhance publication security, ensure the efficient use of resources, and strengthen both its reputation and ranking performance.

Keywords

research support; bibliometrics; publication ethics; research integrity; predatory journals; open science; university rankings; institutional reputation

Absztrakt

A felsőoktatási intézmények tudományos teljesítményének minősége és hitelessége kulcsszerepet játszik a nemzetközi versenyképesség, az egyetemi rangsorokban elfoglalt hely és az intézményi reputáció erősítésében. A kutatás célja egy olyan könyvtári alapú működési modell kidolgozása volt, amely a kéziratok benyújtása előtt ellenőrzi és támogatja az egyetemi affiliációval megjelenő publikációkat, illetve az oktatók és kutatók publikációs tevékenységét. A keretrendszer elemei közé tartozik a célfolyóirat ajánlás, a plágium- és mesterséges intelligencia által generált szöveg ellenőrzése, valamint a cím, absztrakt és kulcsszavak optimalizálása. A rendszer figyelembe veszi az intézményi indikátorokat, a rangsorok (THE, QS) elvárásait és a tudománykommunikációs célokat. A keretrendszer bevezetésével az intézmény képes csökkenteni a kutatásetikai kockázatokat, elősegíti a publikációs biztonságot, a források hatékony felhasználását és a reputáció, valamint a rangsorpozíciók erősítését.

Kulcsszavak

tudománymetria; publikációs etika; kutatási integritás; predátor folyóiratok; open science; egyetemi rangsorok; intézményi reputáció

[1] berek.laszlo@uni-obuda.hu | ORCID: 0000-0002-4126-1528 | könyvtárigazgató, Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola| Library director Obuda University University Library ; Obuda University Doctoral School of Innovation Management

BEVEZETÉS

A felsőoktatási intézmények tudományos teljesítményének láthatósága és hitelessége ma nagymértékben meghatározza az egyetemi reputációt és a nemzetközi rangsorokban elért pozíciót. A publikációk mennyisége önmagában már nem elegendő: a minőség, a kutatási integritás és a publikációs etika iránti elvárások felerősödtek. Az egyetemi könyvtárak a 2010-es évektől a dokumentumszolgáltatói szerepből fokozatosan a kutatásmenedzsment stratégiai partnereivé váltak: adat- és publikációs munkafolyamatokat terveznek, kutatási adatokat kezelnek, tudománymetriai elemzéseket nyújtanak, és aktívan részt vesznek a publikációs kockázatok (plágium, predátor kiadványok, etikai vétségek) megelőzésében. [1-4]

Az egyetemi könyvtárak ma már olyan kutatástámogató szolgáltatásokat kínálnak, amelyek közvetlenül reagálnak az egyetemi rangsorolási rendszerekre és a hiteles tudományos teljesítmény iránti igényre. A kutatások egyértelműen kimutatják az elmozdulást a hagyományos könyvtári szerepköröktől – például a tájékoztató és gyűjteménykezelési feladatoktól – a specializált funkciók irányába, mint a tudománymetriai, a kutatási adatkezelés, az open access kezdeményezések és a tudományos kommunikációs képzések és tréningek. [2]

Ausztrál kutatások például kimutatták, hogy a tudománymetriai és digitális repozitóriumi szolgáltatások térnyerése összefüggésbe hozható a nemzeti értékelési rendszerekkel, mint az Excellence in Research for Australia (ERA) és a Research Excellence Framework (REF). Ezzel párhuzamosan Észak-Amerikában és Európában végzett vizsgálatok hasonló fejleményeket kötnek össze az olyan rangsorokban való javuló láthatósággal, mint a Times Higher Education (THE) és a Quacquarelli Symonds (QS).

Egy felsőoktatási intézmény számára alapvető fontosságú, hogy a könyvtár olyan kutatástámogató keretrendszert működtessen, amely biztosítja a tudományos kommunikáció átláthatóságát, hitelességét és etikai megfelelőségét. A könyvtár ebben a szerepben nem pusztán információszolgáltató, hanem a publikációs folyamat szakmai és etikai minőségbiztosítója, amely a kéziratok benyújtása előtt szűri, elemzi és támogatja a kutatói munkát. Egy ilyen rendszer működtetése révén az intézmény képes megelőzni a tudományetikai vétségeket, elkerülni a predátor folyóiratokban való megjelenést, javítani a nemzetközi láthatóságot és teljesítménymutatókat, valamint hosszú távon erősíteni az egyetem tudományos reputációját és versenyképességét.

SZAKIRODALMI HÁTTÉR

A szakirodalom, a kutatási eredmények feltérképezése a könyvtárak kutatástámogató tevékenységével összefüggő publikációkat azonosította a Scopus adatbázisban 1996 és 2025 között. A keresés több releváns kulcsszót tartalmazott *(„research support”, „research assist”, „academic support”, „librar*”, „data managem*”, „publish*”, „plagiaris*”, „generated text*”, „ethic*”*), amelyek együtt lefedik a könyvtári kutatástámogatás különböző dimenzióit: adatok kezelése, etikai kérdések, publikációs gyakorlat, valamint a tudományos integritás támogatása.

A Scopus adatbázisban alkalmazott keresőkifejezés a következő volt:

(TITLE-ABS-KEY ("research support") OR TITLE-ABS-KEY ("research assist*") OR TITLE-ABS-KEY ("scholarly support*") OR TITLE-ABS-KEY ("academic support*") AND TITLE-ABS-KEY (librar*) AND TITLE-ABS-KEY (predator*) OR TITLE-ABS-KEY ("data managem*") OR TITLE-ABS-KEY (publish*) OR TITLE-ABS-KEY (plagiaris*) OR TITLE-ABS-KEY ("generatedtext*") OR TITLE-ABS-KEY (ethic*)) AND PUBYEAR > 1994 AND PUBYEAR < 2026*

Az 1. ábrán a publikációk éves számát láthatjuk, amely jól szemlélteti a kapcsolódó kutatási eredmények számának növekedését. Az 1996–2005 közötti időszakban a publikációk száma alacsony volt, évente jellemzően 0–6 közötti értékekkel. Ez a korszak az első, elszórt kezdeményezések időszaka, amikor a könyvtári kutatástámogatás még kevéssé jelent meg a szakirodalomban. Pontosabban a mai értelemben vett kutatástámogatás volt kevésbé jelen a könyvtárakban, természetesen a könyvtárak, történetük során mindig is a tudás rendszerezését, megosztását és a tudományos eredmények létrehozását szolgálták. Az időszakban látható alacsonyabb számok annak is köszönhetők, hogy a mai kutatástámogató szolgáltatások alapja az az információ technológiai fejlődés, amely rohamos tempóban elindult a 2000-es évek közepétől.

1. Ábra. Kapcsolódó publikációk száma. (1996-2025 / Scopus) Saját szerkesztés.

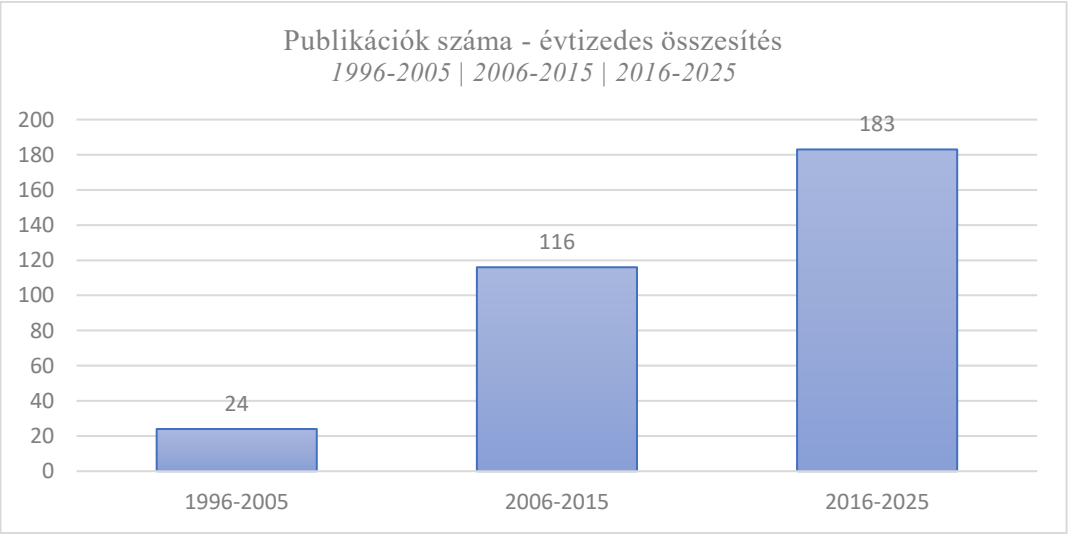
A következő időszakban - 2006–2015 között - már fokozatos növekedés látható: az évtized közepétől egyre több publikáció foglalkozott a témával, ami a digitális szolgáltatások, repozitóriumok, kutatási adatok kezelése és a nyílt hozzáférés (open access) térnyerésének is betudható. A publikációk száma ekkor évi 6–20 között ingadozott.

Ezt követően, 2016-tól jelentős növekedés figyelhető meg: 2016–2025 között évi 10–32 közötti publikációval. A trend különösen 2020 után gyorsul fel, 2025-ben eléri a 32-es csúcsértéket. Ez a robbanásszerű növekedés több tényezőnek tulajdonítható. Az open access folyamathoz kapcsolódó, különböző predátor jelenségek (folyóiratok, kiadók, konferenciák) kapcsán, illetve a félrevezető folyóiratmetrikák megjelenésével az egyetemi és

akadémiai könyvtárak tájékoztató, informáló és edukáló szerepe előtérbe került. Az online tudományos kommunikáció térnyerése következtében a különböző tudományetikai és publikációs etikai kérdések egyre fontosabbá váltak az intézmények, egyetemek számára. Ezen a területen is elsődlegesen a könyvtárak lettek a kulcsszereplők. Az adatmenedzsment és kutatási adatkezelés iránti növekvő érdeklődés és igény kapcsán a – leginkább a – könyvtárak által működtetett intézményi repozitóriumok és adattárak adtak megnyugtató választ.

Az utóbbi pár évben a mesterséges intelligencia által generált szövegek megjelenésével újabb feladatok jelentek meg a könyvtárak kutatástámogató szolgáltatásainak palettáján. A felsőoktatási intézményekben a plágiumellenőrzés – mind a hallgatókra, mind az oktatókra és kutatókra vonatkozóan – leginkább az egyetemi könyvtárakban történt. Az elmúlt években a plágiumellenőrző szoftverek egyre inkább áttértek, illetve bővítik funkcióikat a mesterséges intelligencia által generált szövegek felismerésével.

A 2. ábrán az évtizedenkénti összesített publikációszámokat láthatjuk. Az első évtizedhez (1996–2005) képest a 2006–2015 közötti időszakban több mint négyszeres növekedés történt. Ez tükrözi a könyvtárak szerepének átalakulását, a hagyományos információszolgáltatástól az aktív kutatástámogatás felé történő elmozdulást. A 2016–2025 közötti időszakban a növekedés tovább folytatódott, bár mérsékeltebb ütemben (+58%), viszont az abszolút érték így is a legmagasabb. Ez az időszak a kutatási integritás, a nyílt tudomány, az adatkezelés és a kutatásetika intenzív támogatásának korszaka.



2. Ábra. Publikációk száma – évtizedes összesítés. (1996-2025 / Scopus) Saját szerkesztés.

A növekvő publikációs aktivitás egyértelműen jelzi, hogy a könyvtárak szerepe stratégiai jelentőségűvé vált a kutatási folyamat támogatásában, és mindinkább integrálódnak az egyetemi tudományos infrastruktúrába. A könyvtárak ma már nem pusztán információs szolgáltatóként, hanem aktív kutatási partnereként és minőségbiztosítási szereplőként vesznek részt a tudományos ökoszisztémában.

A 2025-ös évben elért publikációszámok alapján várható, hogy a kutatástámogatás témaköre a következő években tovább erősödik, különösen a mesterséges intelligencia, a kutatási integritás és a kutatásetika metszéspontjában. A könyvtárak ebben a folyamatban kulcsszerepet tölthetnek be az etikus, biztonságos és átlátható tudományos kommunikáció biztosításában és felügyeletében.

KUTATÁSTÁMOGATÁS KÖNYVTÁRI SZEMSZÖGBŐL

Az egyetemi könyvtárak kutatástámogató szolgáltatásai két jól meghatározható irány mentén fejlődtek: egyrészt a könyvtári szerepkörök specializációjával (adatkurátor, kutatástámogató könyvtáros, tudománymetriai elemző…) másrészt olyan átfogó szolgáltatási láncok kialakításával, amelyek egy kézirat teljes életciklusát végig kísérik – a tervezéstől a megőrzésig. [2][5–8]

Kanadai, tudományegyetemeken végzett felmérések azt mutatják, hogy a könyvtári munkatársak szakértelmének bővítése olyan területeken, mint az adatkezelés, a licencelés, a metrikák vagy az open access politika, intézményi szinten is versenyelőnyt jelent. [2] Ausztráliában és Új-Zélandon a „evidence-based library practice" megközelítés a szolgáltatásfejlesztést a felhasználói igényfelmérésekre, teljesítménymutatókra és pilotprojektekre alapozza, ami gyorsabb alkalmazkodást és mérhető hatást tesz lehetővé. [5]

A kutatók szemszögéből a legkeresettebb szolgáltatási modulok közé tartoznak a folyóiratválasztási tanácsadás, az open access és szerzői jogi útmutatás, a kutatói profilmenedzsment, valamint a bibliometriai és tudománymetriai jelentések összeállítása. [6][9] Ezek összességében a könyvtárat az intézményi kutatási és publikációs kockázatkezelés fontos szereplőjévé teszik.

A tudománymetria intézményi beágyazottsága messze túlmutat a számszerű teljesítményértékelésen. Az olyan komplex rendszerek, mint az ausztrál UNSW-n működő Research Impact Measurement Service (RIMS), valós idejű vagy közel valós idejű integrációt biztosítanak a WoS/Scopus/Dimensions adatforrások között, lehetővé teszik a szerzők és intézmények azonosítását és elkülönítését, valamint benchmarking adatokat szolgáltatnak a vezetői döntéshozatalhoz. [9]

Ebben a környezetben a könyvtári szakemberek két módon is hozzájárulnak a folyamatokhoz: egyrészt biztosítják az adatok pontosságát az affiliációk egységesítésével, a duplikációk megszüntetésével és a hibás hozzárendelések javításával; másrészt a számadatokat értelmezhető, stratégiai jelentésű narratívákká alakítják az akadémiai vezetés számára – bemutatva az erősségeket, gyengeségeket, együttműködési hálózatokat és láthatósági hiányosságokat. [7][10–11]

Emellett a könyvtári közvetítők segítik az intézményeket abban, hogy megértsék kutatási eredményeik hatását, azonosítsák a fejlesztendő területeket, és ajánlásokat dolgozzanak ki az intézményi kutatási stratégia fejlesztésére. Az adatelemzésben és stratégiai tervezésben szerzett szakértelmük révén kulcsszerepet játszanak abban, hogy az akadémiai intézmények maximalizálni tudják kutatási hatásukat és potenciáljukat, ami hosszú távon nagyobb szakmai elismeréshez és sikerhez vezet.

Továbbá a könyvtári szakemberek és közvetítők támogatják az intézményeket a tudományos kommunikáció és a nyílt hozzáférés folyamatosan változó környezetében való eligazodásban. Segítenek naprakészen követni az új publikációs trendeket és azokat a feltörekvő technológiákat, amelyek elősegítik a kutatási eredmények szélesebb körű terjesztését. Ezen proaktív megközelítés révén az intézmények biztosíthatják, hogy kutatásaik szélesebb közönséghez jussanak el és nagyobb hatást gyakoroljanak az tudományos közösségre. A könyvtári szakemberek ezen túlmenően együttműködnek az oktatókkal és kutatókkal olyan stratégiák kidolgozásában, amelyek célja a tudományos munkák globális láthatóságának növelése, a nemzetközi tudományos kapcsolatok erősítése és ezzel együtt az egyetemi rangsorokban történő pozíciók javítása.

PUBLIKÁCIÓS ETIKA ÉS PREDÁTOR FOLYÓIRATOK

A tudományos tevékenység alapvető értékeit és normatív kereteit a kutatási és publikációs etika határozza meg. Az etikus kutatási gyakorlatok nem csupán a magas színvonalú tudomány ismérvei, hanem a felsőoktatási intézmények társadalmi felelősségvállalásának kulcsfontosságú elemei is. A publikációs etika célja a lektorálási folyamat integritásának megőrzése, a szerzői felelősségvállalás biztosítása, az átláthatóság előmozdítása a tudományos kommunikációban, valamint a megfelelő hivatkozási normák betartása.

A kutatásetikai és publikációs etikai vétségek leggyakoribb formái – mint a plágium, az adathamisítás, a szellemi tulajdon megsértése vagy a duplikált közlés – aláássák a tudományba vetett közbizalmat. Az elmúlt tizenöt évben azonban egyre nagyobb figyelmet kaptak a predátor kiadók és kétes gyakorlatot folytató folyóiratok, amelyek további erkölcsi és reputációs kockázatokat vetnek fel. Ezek a kiadók látszólag tudományos folyóiratként működnek, valójában azonban a publikációs díjak beszedését helyezik előtérbe a tudományos minőség rovására, és nem biztosítanak valódi lektorálási folyamatot. [4][12–15]

A gyors publikálás, a hamis lektorálás és a félrevezető folyóiratmetrikák alkalmazása mind a predátor kiadók üzleti modelljének részei, amelyek közvetlenül veszélyeztetik az intézmények tudományos reputációját. A szakirodalom szerint a könyvtári beavatkozások három szinten lehetnek hatékonyak. A megelőző szinten a könyvtárak tréningek, irányelvek és ellenőrzőlisták segítségével fejlesztik a kutatók kritikai gondolkodását. Az ellenőrzési szinten előzetes konzultációt és folyóirat ellenőrzést biztosítanak (JCR, SJR, DOAJ, kiadói etikai kódex, lektorálási átláthatóság, APC-politika, szerkesztőbizottság követhetősége). A szankcionáló/megelőző szinten a könyvtár szerepe beépül az intézményi előmeneteli és kutatásetikai folyamatokba. Ebben a formában többek közzött a predátor folyóiratokban megjelent közleményeket nem fogadják el érvényes tudományos teljesítményként. [12–13]

Empirikus bizonyítékok támasztják alá ezen intézkedések hatékonyságát. Frandsen és munkatársai kimutatták, hogy Ghánában, ahol egyetemi reform keretében a könyvtári konzultációt beépítették az előmeneteli feltételek közé, rövid idő alatt jelentősen csökkent a predátor folyóiratokban megjelent publikációk aránya. [16] Buitrago Ciro és Bowker összehasonlító elemzése szerint az Egyesült Államokban és Kanadában a könyvtári válaszok

rendszerszintűek, míg Latin-Amerikában gyakran esetlegesek, ami fokozott intézményi kitettséget eredményez. [1] A tematikus kockázat különösen magas a biológiai és műszaki tudományokban, ahol a „gyors publikálás" ígérete csábítóbb, ezért fokozott könyvtári szűrésre van szükség.

Az online tudományos kommunikációban megjelenő predátor jelenség több szinten is veszélyezteti a tudományos közösség résztvevőit, így hatása nem csupán az egyéni kutatókra, hanem az intézményi és társadalmi szintekre is kiterjed. (*Szerző, kutató, oktató | Egyetemi kar, szervezeti egység, intézet, tanszék | Egyetem, kutatóhely, tudományos intézmény | Ország, nemzet, társadalom*) Az online tudományos kommunikáció egyes szereplőire gyakorolt hatást vizsgálva megállapítható, hogy a predátor folyóiratokban történő publikálás negatív hatásai „átöröklődnek" a szintek között. Így a könyvtár ezirányú szolgáltatásai nem csupán a kutató, hanem a köztes szervezeti egységek, illetve az egyetem érdekeit is szolgálják. [17]

3. Ábra. A keretrendszer részei és a folyamat eredményei. Saját szerkesztés. [12]

A predátor kockázatok mellett új veszélyforrásként jelentkeznek az AI-generált publikációk, köztük a gép által előállított szövegek és grafikus tartalmak. A könyvtárak kulcsszerepet játszanak a mesterséges intelligenciával kapcsolatos kutatásetikai érdekek érvényesítésében azáltal, hogy elősegítik az előírások betartását, a generált tartalmak jelölését, az adatok és kódok nyílt és ismételhető megosztását, valamint az ellenőrző eszközök és szakmai protokollok terjesztését. Ez nem felügyeleti tevékenység, hanem kompetenciafejlesztés: a cél a módszertani átláthatóság biztosítása, nem pedig a technológiai korlátozás. [18]

A kutatásetikai megfelelés nem merül ki a plágium megelőzésében; a kutatási adatok megfelelő kezelése ugyanolyan kritikus jelentőségű. A könyvtárak kulcsszerepet játszanak a FAIR-elv (Findable, Accessible, Interoperable, Reusable) gyakorlati megvalósításában: támogatják az adatkezelési tervek kidolgozását, biztosítják az adattárakat és metaadatszabványokat, kezelik a licenceket (CC-BY, ODC-BY), valamint a hosszú távú megőrzést biztosító azonosítókat (DOI, Handle).

EGYETEMI RANGSOROK ÉS REPUTÁCIÓ

A nemzetközi egyetemi rangsorok, mint például a Shanghai (ARWU) rangsor, a Times Higher Education (THE) rangsor és a QS World University Rankings, mára a tudományos teljesítmény és a globális versenyképesség értékelésének fontos viszonyítási pontjaivá váltak. Ezek az értékelések nemcsak a kutatási és oktatási minőséget vizsgálják, hanem az intézményi láthatóságot, a hivatkozási hatásokat, a nemzetközi együttműködéseket és az általános reputációt is. A könyvtár – szolgáltatásaival – ezekre a jellemzőkre közvetlen és közvetett módon is hatással lehet.

A könyvtár hozzáférést biztosít a legfontosabb tudományos adatbázisokhoz (Scopus, Web of Science, InCites, SciVal), valamint képzésekkel és konzultációkkal segíti a kutatókat abban, hogy munkáikat magas presztízsű, Q1–Q2 besorolású folyóiratokban publikálják. Az intézmények szempontjából a *Citations per Faculty* és a *Research Impact* mutatók különösen meghatározóak a THE és QS rangsorokban, hasonlóan ahhoz, ahogy a h-index egyéni kutatói szinten jelzi a tudományos teljesítményt. [19–20] A könyvtár e mutatókat közvetlenül is javítja azáltal, hogy támogatja a kutatókat tudományos eredményeik láthatóságának és minőségének növelésében.

A könyvtár emellett scientometriai elemzésekkel, adatellenőrzéssel és publikációs statisztikák készítésével segíti az intézményi vezetést és az adatszolgáltatást a rangsorokhoz kapcsolódó folyamatokban. A kutatói profilok pontos karbantartása biztosítja, hogy az egyetem kutatási teljesítménye hitelesen és pontosan jelenjen meg a nemzetközi adatbázisokban. Ezáltal az intézményi adatok megfelelően reprezentálódnak a rangsorok forrásrendszereiben (Scopus, Clarivate), ami minimalizálja a hibás/téves jelentés vagy a hibás affiliáció miatti kockázatokat.

A QS, THE és ARWU rangsorok közös jellemzője, hogy jelentős hangsúlyt fektetnek a publikációs és hivatkozási mutatókra. [21–23] A könyvtár a rangsorokban és kutatási értékelésekben használt mutatókra három fő mechanizmuson keresztül gyakorol hatást. Az első az adatintegritás biztosítása, amely magában foglalja a szerzők és intézmények pontos azonosítását, valamint a duplikációk és hibás hozzárendelések kiszűrését. Ez a folyamat alapvető a kutatási teljesítmény hiteles és megbízható megjelenítése szempontjából. A második a láthatóság növelése, amelynek keretében a könyvtár ösztönzi a nyílt hozzáférés arányának emelését, támogatja a publikációk intézményi repozitóriumba való feltöltését, és segíti a kutatói profilok folyamatos gondozását. Mindez hozzájárul ahhoz, hogy az egyetem kutatási eredményei szélesebb közönséghez jussanak el, és növekedjen a hivatkozási potenciál. A harmadik mechanizmus a reputációvédelem, amely a predátor folyóiratok felismerésére és a publikációs etikai vétségek megelőzésére irányul. A könyvtár e tevékenységekkel nemcsak az intézményi és kutatói hitelességet óvja, hanem elősegíti a tudományos kommunikáció biztonságos, átlátható és megbízható működését is.

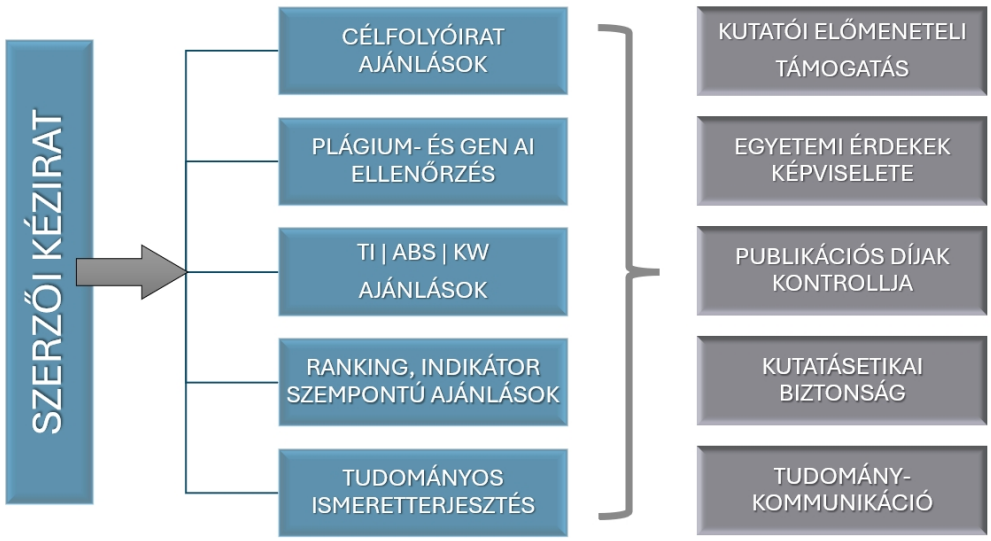
Az Ausztrália–Új-Zéland régióban az *evidence-based library service development* modell kimutathatóan javította a kutatási finanszírozások sikerességi arányát és a nemzetközi együttműködések (társszerzőség, interdiszciplinaritás) számát. [5][24] Észak-Amerikában a könyvtárak aktív részvétele az előléptetési és minősítési folyamatokban – például a hiteles folyóiratlisták karbantartása és a kétes kiadók kizárása révén – rövid távon javította

a publikációs portfóliók minőségét, hosszabb távon pedig a reputációs mutatók erősödéséhez vezetett. Ezzel szemben a predátor folyóiratokban való publikálás statisztikailag gyengíti az intézményi teljesítménymutatókat, különösen akkor, ha ezek a cikkek annak ellenére kerülnek indexelésre nagy adatbázisokban, hogy tudományos minőségük kifogásolható. [12]

Összességében az egyetemi könyvtár nem csupán támogató szolgáltatóként működik, hanem a kutatási láthatóság, hitelesség és fenntarthatóság garanciájaként is. A megbízható kutatási adatok, a predátormentes publikációs környezet fenntartása, valamint az Open Access és FAIR elvek gyakorlati alkalmazása együttesen járulnak hozzá az egyetemek globális rangsorokban való előkelőbb pozíciójához, miközben hosszú távon erősítik tudományos és társadalmi reputációjukat.

KÖVETKEZTETÉSEK

A szakirodalom korábbi kutatási eredményei és a tapasztalatok alapján szükséges egy egységes keretrendszer működtetése a korábbiakban felsorolt veszélyek elkerülésére és a kockázatok minimalizálására. A keretrendszer középpontjában a szerzői kézirat áll, vagyis az a tudományos munka, amelyet az egyetemi oktatók és kutatók publikálni kívánnak. (4. ábra) Természetesen a szerzők által publikált tudományos eredmények, publikációk nem csak az oktatót, kutatót jellemzik, minősítik, hanem az affiliációhoz kapcsolódó szervezeti egységet, kart vagy magát az intézményt. Ebből a szempontból elmondható, hogy a keretrendszer a folyamat gyökerénél tesz intézkedéseket, mivel a publikálást követően már visszafordíthatatlan következményei lehetnek mind a kutató, mind az egyetem számára a nem megfelelő publikálási gyakorlatnak.



4. Ábra. A keretrendszer részei és a folyamat eredményei. Saját szerkesztés.

A rendszer célja és működési logikája

A könyvtár kulcsszerepet tölt be az egyetemi kutatástámogatási folyamatban, különösen a publikációs előkészítés és minőségbiztosítás területén. A rendelkezésre álló nemzetközi és hazai adatbázisok (Scopus, Web of Science, IEEE, DOAJ, MTMT…) és releváns tudománymetriai indikátorok (Impact Factorm Scimago Journal Rank, CiteScore…) alapján a könyvtár célfolyóirat ajánlásokat készít, amelyek segítik a kutatókat abban, hogy kéziratait megfelelő, megbízható és nem predátor folyóiratokban helyezzék el. Ez a szolgáltatás hozzájárul a publikációs döntések tudatosabbá tételéhez, csökkenti a kifogásolható lapokban való megjelenés kockázatát, és elősegíti a láthatóság, valamint a tudományos hatás növelését.

A kéziratok benyújtása előtt a könyvtár kutatástámogató kollégái plágium- és generatív mesterséges intelligencia által generált szöveg ellenőrzést végeznek, így biztosítva, hogy a tudományos munka megfeleljen a kutatási integritás és a tudományetika alapelveinek. Az ilyen típusú előzetes kontroll nemcsak a szerzők, hanem az intézmény tudományos hitelességét is védi, és segít megelőzni az etikai vétségekből eredő reputációs kockázatokat. Ha egy „problémás" kézirat sikeresen átjut a folyóirat lektori és ellenőrzési folyamatain, és végül megjelenik, annak kedvezőtlen következményei akár több évvel a publikálás után is jelentkezhetnek.

A könyvtár szakértői továbbá javaslatokat adnak a kéziratok címének, absztraktjának és kulcsszavainak (TI | ABS | KW) optimalizálására. Ez a támogatás a nemzetközi adatbázisokban való hatékony indexelést, a kereshetőség növelését és a hivatkozási potenciál erősítését szolgálja. A publikációs célhelyek kiválasztásánál a könyvtár figyelembe veszi a releváns rangsorokat, valamint az intézményi teljesítménymutatókat és stratégiai célokat, így támogatva az egyetem publikációs teljesítményének javítását és nemzetközi rangsorokban való előrelépését.

A kutatástámogatási tevékenység további eleme a tudományos ismeretterjesztés és a tudománykommunikációs folyamatok elősegítése. A könyvtár közvetítő szerepet játszik a kutatási eredmények disszeminációjában, többek között az intézményi repozitórium, hírlevelek, közösségi médiafelületek és médiakapcsolatok révén. Ezáltal hozzájárul a tudományos eredmények társadalmi hasznosulásához, az egyetem láthatóságának növeléséhez és reputációjának erősítéséhez.

Összességében a könyvtári kutatástámogatási keretrendszer nemcsak a kéziratok szakmai és etikai minőségét garantálja, hanem stratégiai szinten is hozzájárul az intézményi teljesítmény, a tudományos biztonság és a reputáció fenntartható fejlesztéséhez.

A rendszer kedvező hatásai

Az ellenőrzési és ajánlási tevékenység hatásai több szinten is érvényesülnek, és közvetlenül hozzájárulnak az intézmény tudományos teljesítményének, biztonságának és nemzetközi megítélésének javításához. A 4. ábrán bemutatott elemek a kapcsolódó könyvtári szolgáltatások hatásmechanizmusát szemléltetik, hogy a kézirat előkészítési és ellenőrzési folyamatok milyen pozitív következményekkel járnak mind a kutatói, mind az intézményi szinten.

Az egyik legfontosabb hatás a kutatói előmenetel támogatása. A kéziratok minőségének javulása és a publikációs folyamat tudatosabbá válása közvetlenül segíti az oktatók és kutatók szakmai előrehaladását, legyen szó előléptetésről, habilitációról vagy doktori fokozatszerzésről. A könyvtár tanácsadói és szakértői szerepe így beépül a tudományos életpálya támogatásának rendszerébe, ahol a kutatók nemcsak technikai, hanem stratégiai támogatást is kapnak. A könyvtár ezen szolgáltatásával személyre szabott támogatást ad, mivel az adott kutató publikációs és citációs adatait egyébként is az MTMT kapcsán a könyvtáros kollégák kezelik. A kutatói előmeneteli folyamat egyes szakaszai esetében a követelményeknek való megfelelést és a kapcsolódó pontszámítást is a könyvtár végzi, így ténylegesen az adott kutatóra, igényeire szabott ajánlás dolgozható ki.

A folyamat az egyetemi érdekek képviseletét is szolgálja, hiszen az egységes ellenőrzési és ajánlási keret biztosítja, hogy az intézmény publikációs kibocsátása megbízható, magas minőségű és a nemzetközi rangsorok szempontjából is előnyös legyen. A rendszer működése tehát nem csupán adminisztratív jellegű, hanem a stratégiai reputációépítés eszköze, amely hozzájárul az egyetem láthatóságának, tudományos presztízsének és rangsorpozícióinak erősítéséhez.

Egy másik jelentős elem a publikációs díjak kontrollja, amely a célfolyóirat ajánlások révén segíti a kutatókat abban, hogy elkerüljék a túlzott vagy indokolatlan cikkeljárási díjakkal dolgozó folyóiratokat. Ez különösen fontos a kutatási források hatékony felhasználása szempontjából, mivel biztosítja, hogy a publikációk valódi értéket és láthatóságot nyújtsanak az intézmény számára.

A kutatásetikai biztonság szintén központi elem. A plágiumellenőrzés, a mesterséges intelligencia által generált szövegek vizsgálata és a folyóiratok etikai átvilágítása megelőző mechanizmusként működik, amely védelmet nyújt mind az egyéni kutatók, mind az egyetem számára. Ez a fajta proaktív etikai kontroll minimalizálja a tudományos visszaélések kockázatát, és hozzájárul az intézményi integritás fenntartásához.

Végül, a könyvtár tudománykommunikációs szerepe erősíti az egyetem nyilvános megjelenését és tudományos láthatóságát. Az intézmény kutatási eredményeinek disszeminációja – például az intézményi repozitóriumokon, hírleveleken, közösségi médiafelületeken keresztül – elősegíti a tudományos ismeretek társadalmi hasznosulását, és hozzájárul az egyetemi reputáció folyamatos erősödéséhez.

ÖSSZEGZÉS

A szakirodalom és az intézményi tapasztalatok alapján egy egységes kutatástámogató keretrendszer kialakítása elengedhetetlen az egyetemek számára, hogy megelőzzék a nem megfelelő publikálási gyakorlatból eredő kockázatokat, és biztosítsák a kutatási integritást. A rendszer középpontjában a szerzői kézirat áll, amely nemcsak a kutató vagy oktató tudományos tevékenységének lenyomata, hanem az affiliációhoz kapcsolódó kar, intézet és maga az egyetem megítélését is befolyásolja. Mivel a hibás publikációs döntések hosszú távú, akár évekkel később jelentkező reputációs és etikai következményekkel járhatnak, a folyamat korai szakaszában szükséges a minőségbiztosítás és az ellenőrzés beépítése.

A könyvtár ebben a folyamatban stratégiai szerepet tölt be: nemcsak információszolgáltató, hanem a tudományos közlés biztonsági és minőségbiztosítási központja. A keretrendszer elemei – a célfolyóirat-ajánlások, a plágium- és mesterséges intelligencia-ellenőrzések, a cím-, absztrakt. és kulcsszó optimalizálás, valamint az indikátorok és rangsorok figyelembevétele – mind azt szolgálják, hogy a kéziratok megbízható, etikus módon és még véletlen sem kétes minőségű folyóiratokban jelenjenek meg. A rendszer egyúttal a kutatók karrierfejlődését is támogatja, hiszen a könyvtár segíti az előmeneteli folyamatokat, a publikációs pontszámításokat és a nemzetközi láthatóság növelését.

A keretrendszer működése egyszerre erősíti az intézményi reputációt, a tudományos biztonságot és a források hatékony felhasználását. A könyvtár proaktív kapuőr szerepe révén megelőzi a tudományetikai vétségeket, támogatja a nyílt tudomány elveinek érvényesítését, és elősegíti a kutatási eredmények hiteles disszeminációját. A jövőben a rendszer továbbfejlesztése egy félautomatikus, online felület formájában valósulhat meg, amely lehetővé teszi, hogy az oktatók és kutatók önállóan vehessék igénybe a kutatástámogató funkciókat, miközben a könyvtár szakmai felügyelete a kritikus pontokon továbbra is biztosítja a szükséges szakértői közbeavatkozást, a folyamat minőségét és etikai megfelelőségét.

A kutatás a Kulturális és Innovációs Minisztérium 2024-2.1.1 kódszámú egyetemi Kutatói Ösztöndíj programjának a Nemzeti Kutatási, Fejlesztési és Innovációs alapból finanszírozott szakmai támogatásával készült.

FELHASZNÁLT IRODALOM

[1] J. Buitrago Ciro, L. Bowker, „Investigating academic library responses to predatory publishing in the United States, Canada and Spanish-speaking Latin America”, *Aslib J. Inf. Manage.*, vol. 72, no. 4, pp. 625–652, 2020. https://doi.org/10.1108/AJIM-03-2020-0089.
[2] A. Ducas, N. Michaud-Oystryk, M. Speare, „Reinventing ourselves: New and emerging roles of academic librarians in Canadian research- intensive universities”, *Coll. Res. Libr.*, vol. 81, no. 1, p. 43, 2020. https://doi.org/10.5860/crl.81.1.43
[3] L. Berek, „Az online tudományos kommunikáció hitelességét veszélyeztető tényezők”, *Biztonságtudományi Szemle*, vol. 4, no. 2. ksz., pp. 35–41, 2022.
[4] L. Berek, „A decade of predatory journals with an overview of the literature”, *Transactions on Internet Research- IPSI BGD*, vol. 18(1) pp. 4-8. 2022.
[5] G. Haddow, J. Mamtora, „Research Support in Australian Academic Libraries: Services, Resources, and Relationships” *New Rev Acad Librariansh*. vol. 23(2–3) pp. 89–109. 2017. https://doi.org/10.1080/13614533.2017.1318765
[6] K. Singh, AK. Siwach, „Researchers’ Expectations Towards Library Research Support Services (LRSS): A Case Study of Maharshi Dayanand University, Rohtak” *DESIDOC J Libr Inf Technol*. vol. 44(2) pp. 69–76. 2024. https://doi.org/10.14429/djlit.44.2.18976

[7] S. Corrall, MA. Kennan, W. Afzal, „Bibliometrics and research data management services: Emerging trends in library support for research" *Library Trends*, vol. 61(3), pp. 636–674. 2013.
[8] S. Corrall, S. Pinfield, „Research data management and libraries: Current activities and future priorities" *Journal of Librarianship and Information Science*, vol. 46(4), pp. 299–316. 2014.
[9] R. Drummond, R. Wartho, „The Research Impact Measurement Service At The University Of New South Wales" *Australian Academic & Research Libraries*. vol. 47(4) pp. 270–281. 2016. https://doi.org/10.1080/00048623.2016.1253427
[10] S. Alfaro Jimenez, J. Berbegal-Mirabent, R. de la Torre, „How do university libraries contribute to the research process?" *The Journal of Academic Librarianship*. vol. 50(5):102930. 2024. https://doi.org/10.1016/j.acalib.2024.102930
[11] L. Bredahl, „Bibliometric Service Models in Academia and Considerations Impacting Resourcing - Chapter 4." *Library Technology Reports*. vol. 58(8) pp. 32–36. 2022.
[12] L. Berek, „Researcher's choice or just a necessity? The consequences of publishing in a predatory journal" *Interdisciplinary Description of Complex Systems*. vol. 21(4) pp. 324-332. 2023. https://doi.org/10.7906/indecs.21.4.1
[13] SB. Demir, „Predatory journals: Who publishes in them and why?" *Journal of Informetrics* vol. 12(4), pp. 1296-1311.2018. https://doi.org/10.1016/j.joi.2018.10.008
[14] S. Kurt, „Why do authors publish in predatory journals?" *Learned Publishing* vol. 31(2), pp. 141-147. 2018. https://doi.org/10.1002/leap.1150
[15] TF. Frandsen, „Why do researchers decide to publish in questionable journals? A review of the literature" *Learned Publishing* vol. 32(1), pp. 57-62. 2019. https://doi.org/10.1002%2Fleap.1214
[16] TF. Frandsen, RB. Lamptey, EM. Borteye, „Promotion standards to discourage publishing in questionable journals: a follow-up study" *The Journal of Academic Librarianship*. vol. 50(5):102895. 2024. https://doi.org/10.1016/j.acalib.2024.102895
[17] L. Berek, „Predátor folyóiratok és félrevezető mérőszámok - ne hagyd, hogy becsapjanak!", *Biztonságtudományi Szemle*, vol. 6, no. 2., pp. 1–12, 2024.
[18] L. Berek, „Artificial Intelligence-Generated Text in Higher Education: Usage and Detection in the Literature" *Interdisciplinary Description of Complex Systems.* vol. 22(3) pp. 238-245. 2024. https://doi.org/10.7906/indecs.22.3.1
[19] Gy. Mester, „The 2022 ranking list of citation analysis researchers using H-index" *Interdisciplinary Description of Complex Systems* vol. 20(6), pp. 775-779. 2022. http://dx.doi.org/10.7906/indecs.20.6.8
[20] Gy. Mester, „Rankings Scientists, Journals and Countries Using h-index." *Interdisciplinary Description of Complex Systems*. vol. 14(1), pp. 1-9. 2016. http://dx.doi.org/10.7906/indecs.14.1.1
[21] QS Quacquarelli Symonds. QS World University Rankings. Methodology. https://www.topuniversities.com/
[22] Times Higher Education. World University Rankings. Methodology. https://www.timeshighereducation.com/

[23] Academic Ranking of World Universities. Methodology. https://www.shanghairanking.com/
[24] A. Keller, „Research Support in Australian University Libraries: An Outsider View” *Australian Academic & Research Libraries*. vol. 46(2) pp. 73–85. 2015. https://doi.org/10.1080/00048623.2015.1009528

DOI: https://doi.org/10.12700/btsz.2025.7.4.15

OPPORTUNITY OR CHALLENGE? NATO AND CHINA ON TWO SIDES OF THE GREAT WALL

LEHETŐSÉG VAGY KIHÍVÁS? NATO ÉS KÍNA A NAGY FAL KÉT OLDALÁN

SEPRÉNYI Patrik[1]

Abstract

In the 2019 London Summit Declaration, NATO characterized its relationship with China using the phrase "opportunities and challenges." In contrast, the 2022 Strategic Concept uses much stronger language to clearly identify the Asian country as a challenge to the Alliance, citing its hybrid and cyber activities, geopolitical ambitions, and rapid technological development, among other factors. This more recent approach has gradually intensified over recent years, presumably also influenced by the United States' shift in focus toward the Indo-Pacific region and its perception of China as a threat. The purpose of this study is to examine the security aspects that have led China to be viewed as a strategic challenger in NATO's strategic documents and communications. It also aims to investigate the resulting great power competition and China's perspective and communication regarding NATO.

Keywords

Technological development, NATO-China relations Hybrid threats, Strategic concept, Chinese economic and technological rise, Great Power Competition, Emerging and disruptive technologies (EDTs)

Absztrakt

2019-ben a Kínával való viszony jellemzésére a NATO még a „lehetőségek és kihívások” kifejezést használta a londoni csúcstalálkozó deklarációjának szövegében. Ezzel szemben a 2022-es stratégiai koncepcióban már jóval erősebb nyelvezet használatával egyértelműen kihívásként azonosítja a Szövetség az ázsiai országot, többek között annak hibrid- és kibertevékenységei, geopolitikai törekvései, valamint gyorsütemű technológiai fejlődése miatt. Utóbbi megközelítés az elmúlt években is fokozatosan erősödött, amihez feltehetően az Egyesült Államok figyelmének csendes-óceáni térség felé történő elmozdulása, illetve Kínáról alkotott fenyegetettségpercepciója is hozzájárult. Ezen tanulmány célja megvizsgálni azokat a biztonsági aspektusokat, amelyek miatt Kína napjainkra stratégiai kihívóként jelenik meg a NATO stratégiai dokumentumaiban és kommunikációjában, valamint szintén cél megvizsgálni a kialakult hatalmi versengést és a NATO-t érintő kínai nézőpontot és kommunikációt is.

Kulcsszavak

Technológiai fejlődés, NATO-Kína kapcsolatok, Hibrid fenyegetések, Stratégiai koncepció, Kínai gazdasági és technológiai felemelkedés, Nagyhatalmi versengés, Feltörekvő és felforgató technológiák (EDT)

[1] patrik.seprenyi@gmail.com | ORCID: 0000-0003-1223-4245 | PhD Student, University of Public Service | Doctoral School of Military Sciences | Doktorandusz, Nemzeti Közszolgálati Egyetem | Hadtudományi Doktori Iskola

BEVEZETÉS

A Kínai Népköztársaság 2025 októberében ünnepelte fennállásának 76. évfordulóját. Ez egyben azt is jelenti, hogy már csak 24 éve van Kínának elérnie a 2049-re kitűzött grandiózus célját, vagyis egy gazdag, erős, demokratikus, kulturálisan fejlett és harmóniában élő, minden területet érintően fejlett, 21. századi szocialista ország megteremtését. Utóbbi célkitűzések Hszi Csin-ping elnök még elnöki hivatalba lépése előtti, 2012. november 29-ei beszédében jelentek meg először, azóta pedig számtalanszor nyomatékosította ezen „Kínai Álom”[2] koncepcióhoz tartozó célok elérésének fontosságát.[1] Hszi elnök többek között a Kínai Kommunista Párt 20. Kongresszusának megnyitóján tartott több, mint kétórás beszédében is reflektált a modern szocialista Kína létrehozásának céljára, valamint, a tanulmány szempontjából kiemelten fontos katonai jellegű technológiai kutatás és fejlesztés jelentőségéről is hosszasan beszélt.[2]

Hszi Csin-ping elnök 2013-as hivatalba lépése óta a kínai külpolitika jóval asszertívebbé, ambiciózusabbá, retorika tekintetében jóval nyitottabbá vált, ami lényegében ellentéte a Teng Hsziao-ping kínai reformer politikus és vezető által a 80-as, 90-es években meghirdetett intelmeknek, amelyek arra szólították fel Kínát, hogy ne vállaljon központi szerepet a nemzetközi térben, illetve rejtse el képességeit és várjon türelemmel a megfelelő alkalomra.[3] Ezen intelmek ellenében napjainkban Kína erélyesen kommunikálja céljait és érdekeit a világ felé, valamint erőteljesen igyekszik helyreállítani az ország „Megszégyenülés évszázada”[3] előtti imázsát és befolyását, amihez felhasználja a napjainkra kiépült robosztus gazdasági-ipari kapacitásait, diplomáciai képességeit, kritikus fontosságú nyersanyag-készleteit és minden egyéb eszközt, amelyek segíthetnek Kínának abban, hogy a világ vezető nagyhatalmává váljon.[4]

Utóbbi gondolathoz kapcsolható a 2025 szeptemberében, Pekingben, a második világháború és a kínai-japán háborúk lezárásának emlékére megrendezett Kínai Győzelem Napi Parádé is, amelyen több ezer katona és haditechnikai eszköz vonult fel, beleértve olyan új-generációs fegyverrendszereket is, amelyeket korábban még nem mutattak be a nyilvánosság előtt, ezzel egyértelműen demonstrálva a kínai katonai irányú technológiai színvonal előrehaladott fejlettségi szintjét és elrettentő erejét.[5]Ezen események és trendek függvényében érthetővé válik, hogy különösen az Egyesült Államok, de a NATO-szövetségesek számára is miért jelenik meg Kína stratégiai kihívóként. A következőkben a tanulmány célja röviden bemutatni, hogyan emelkedett Kína arra a szintre, hogy a kínai politikai vezetők egy új világrend megalakulásáról kommunikálhassanak, illetve, hogy a NATO miképp reagál a Kína jelentette kihívásokra. Végül, de nem utolsó sorban a két nemzetközi szereplő viszonya és várható jövőbeli kapcsolata is vizsgálatra kerül.

[2] A Kínai Álom: A fogalom a kínai nemzet megfiatalítását jelenti, vagyis azt a történelmi célt, hogy Kína visszanyerje régi dicsőségét és vezető szerepét a világban azáltal, hogy Kína egy modern, erős, virágzó szocialista nagyhatalommá válik.[6]

[3] A Megszégyenülés évszázada: Az 1800-as években Kína részesedése a világ GDP-jéből több, mint 30% volt, amely az 1950-es évekre 5%-ra csökkent. A hatalmas visszaesést, illetve a kínai technológiai lemaradást a politikai vezetők az ópium háborúkkal, valamint az azokat követő külföldi behatolással és kizsákmányolással magyarázzák. Az elszenvedett sérelmeket Kína generációk óta próbálja orvosolni azáltal, hogy igyekszik visszaépíteni az ország világhatalmi státuszát és szerepét.[4]

KÍNA GAZDASÁGI FELEMELKEDÉSE

Miután a Kínai Kommunista Párt erői végleg legyőzték a Kuomintang4 erőit és Csang Kaj-sek a megmaradt követőivel együtt Tajvan szigetére menekült, 1949. október elsején megalakult a Kínai Népköztársaság, melynek élén egészen 1976-ig Mao Ce-tung állt, aki inkább kevesebb, mint több sikerrel próbálta különböző gazdasági tervek révén felzárkóztatni Kínát a világhoz. Az alapvető és elsődleges cél természetesen a második világháború és a polgárháború alatt keletkezett károk helyreállítása volt, ezt követően viszont jelentős erőforrásokat allokált a kínai vezetés az ipari termelés fellendítésére, valamint a mezőgazdasági termelés fejlesztésére. [8]

A Kínai Kommunista Párt szovjet mintát követve szervezte meg a gazdasági folyamatokat és ötéves tervekkel operált. Az ötvenes években 1952 és 1957 között négyszeresére nőtt az előállított fém mennyisége, jól lehet, a mennyiséghez nem feltétlenült párosult mindig megfelelő minőség, mert a cél az előírt termelési mennyiség elérése volt, továbbá nem mindenhol állt rendelkezésre a megfelelően kiépített termelési infrastruktúra – például az ötvenes évek végén országszerte létrehozott kisméretű népi kohók esetében. Az ipari szektort érintő minőségbéli hiányosságok mellett az agrárszektor sem volt képes az irracionálisan magas termelési célok maradéktalan elérésére, amelyet Mao Ce-tung többek között a népegészséget is szem előtt tartó, termelést segítő elképzelésével, a Négy Kártevő Elleni Programmal szeretett volna felélénkíteni.[8]

A kártevők elleni hadjárat része volt a primer és szekunder szektort érintő ötvenes évek végi gazdaságélénkítő és fejlesztő programjának, amelyet Nagy Ugrásnak neveztek, és amelynek kitűzött célja a többszázéves gazdasági lemaradás évtizedek alatti ledolgozása volt. A program számos intézkedést tartalmazott, de a katasztrofális eredménnyel záruló kártevőirtás kétségkívül az egyik legradikálisabb eleme a felzárkózási kísérleteknek. Az 1958-ban meghirdetett kampány a mezőgazdasági termelésre, illetve a népegészségre a kínai vezetés szerint legnagyobb veszélyt jelentő élőlényekre, a verebekre, patkányokra, szúnyogokra és legyekre irányult, mivel utóbbi három súlyos betegségeket terjeszt, a verebek pedig felcsipegethetik a magokat a termőföldről. A kampány eredményeképpen több, mint egy milliárd verebet, másfélmilliárd patkányt, valamint több tízmillió kilogramm szúnyogot és legyet irtottak ki országszerte, amelynek következtében olyan terméskárosító rovarok szaporodtak el a későbbiekben, mint például a sáskák, amelyek tevékenysége a következő években 40 millió ember halálát okozó éhínséghez vezetett. A keletkezett károk és az elhibázott gazdaságpolitika korrigálása a hatvanas évek végéig elhúzódott és a gazdaság csak lassú ütemben tudott növekedni, amit a politikai tisztogatások tovább nehezítettek.[9]

A Mao Ce-tung éra (1949-1976) tehát még nem indította el Kínát azon a fejlődési útvonalon, amely a mai viszonyokhoz vezetett. Utódja azonban, a kínai reformer politikus, Teng Hsziao-ping számos olyan intézkedést tett, amelyek alapjaiban változtatták meg Kína teljes politikai, társadalmi és gazdasági struktúráját, valamint felfogását és a Kínai Kommunista Párt kínai társadalommal ápolt viszonyát.

Teng Hsziao-ping 1982-ben kijelentette, hogy a szocializmus alapelveit újra kell gondolni és meg kell teremteni a kínai típusú szocializmust, amely lényegében az erőteljes

[4] A Kuomintang a Kínai Nacionalista Pártot jelenti, melynek vezetője Csang Kaj-sek volt. A párt a mai napig meghatározó politikai erő a Kínai Köztársaságban (Tajvan). [7]

gazdasági reformokat, de ezzel együtt a Kommunista Párt hatalmának megtartását is jelentette.[8]

A Reform és Nyitás politikája a mezőgazdaság, az ipar, a honvédelem, valamint a tudomány modernizációjára épült. A kínai politikai vezetés fokozatosan lebontotta a belső migráció korlátait, megszüntette a népi kohókat és kommunákat teret engedett az ipari szektor vállalatainak önállósodásának, nyitást kezdeményezett a külpolitikai és külgazdasági dimenziókban, valamint összességében csökkenni kezdett az állam jelenléte a gazdasági folyamatok irányításában és megjelentek a magánvállalatok is.[8] Az új gazdasági, illetve politikai irányvonal az elkövetkezendő évtizedekben a fokozatosan végrehajtott reformoknak köszönhetően jelentős lendületet adott a kínai gazdaságnak, amit tovább lendített a külföldi, különösen a kínai diaszpórából (például az egy ország, két rendszer zászlója alatt létező Hong Kongból vagy Makaóból) érkező befektetések növekvő beáramlása. Az 1979 és 1999 között Kínába áramló 307 milliárd dollárnyi külföldi befektetésből például 154 milliárd dollár Hong Kongból érkezett.[10]

A hetvenes évek végén, nyolcvanas évek elején fejlődésnek indult és később, a 2000-res évektől szinte exponenciális mértékben növekvő gazdaság napjainkra a világ második legnagyobb gazdaságává vált az Egyesült Államok után. 1980 és 2025 között a kínai GDP 400 milliárd dollárról 19 000 milliárd dollárra nőtt, amelyet csak csekély mértékben lassított a 2008-as gazdasági világválság vagy a későbbi koronavírus járvány.[11] Becslések szerint 2026-ban a kínai gazdaság mérete a 21 000 milliárd dollárt is megközelítheti, ami még egyelőre messze elmarad az Egyesült Államok 30 000 milliárd dolláros GDP-jétől, ennek ellenére versenyben van a világgazdasági vezető pozícióért.[12]

A BÉKÉS FEJLŐDÉS ÉS A KÍNAI FENYEGETÉS KONCEPCIÓI

A számtalanszor idézett ókori kínai író, Szun-Ce szerint akkor válik egy hadvezér a legjobbak között is a legjobbá, ha harc nélkül sikerül győzedelmeskednie ellenségei felett.[13] A gazdasági hatalom, illetve a befolyás gazdasági eszközökön keresztüli megszerzése és kiterjesztése, a földrajzi szempontból stratégiai jelentőséggel bíró infrastruktúrákba való beruházás és a kedvező világgazdasági útvonalak kiépítése, valamint akár az adósságcsapda politika alkalmazása olyan helyzeti előnyökhöz vezethet, amelyek révén az adott ország, jelen esetben Kína regionális vagy akár lokális szinten is érdekeltséget szerezhet és akár más országok belügyeit érintő befolyásra tehet szert.[14]

Ugyan Csiang Cö-min, a Kínai Népköztársaság egykori (1993-2003) elnöke már 2000-ben a külföldi befektetések növelésére és a mélyebb nemzetközi nyitásra bíztatta a kínai befektetőket, igazán robosztus méretekben csak a Hszi Csin-ping elnök által 2013-ban meghirdetett Egy Övezet, Egy Út Kezdeményezés (Belt and Road Initiative, BRI) terjesztette ki a kínai beruházások és ezáltal a kínai befolyás elérését a világgazdasági folyamatokra. A BRI mintegy 150 országot és 30 nemzetközi szervezetet érint, célja pedig mind szárazföldön, mind pedig vízen egyfajta modern selyemutakat építeni, amelyek elősegítik a világgazdasági folyamatok koordinációját, megteremtik az országok közötti erősebb konnektivitást, valamint Kína által ellenőrzött ellátási láncokat, világgazdasági útvonalakat hoznak létre.[15]

A BRI keretében 2013 óta már több, mint 1000 milliárd dollár összértékben [16] történtek befektetési – együttműködési megállapodások, így például ide sorolandó a görög

Pireusz kikötő infrastruktúrájának modernizálása és a Budapest-Belgrád vasútvonal megépítése is, amelyek mind részét képezik a Kína által kiépítendő egyik kereskedelmi útvonalnak.[17]

A beruházások, vagyis a BRI egybecseng Kína azon törekvéseivel, hogy végleg maga mögött hagyja a megszégyenülés évszázadát és újra felemelkedhessen, amely azonban gyanakvó hangokat ébreszt azon országokban, akik kihívásként vagy fenyegetésként értékelik Kína gyorsütemű fejlődését és befolyásszerzését. Éppen ezért Kína retorika szintjén minden eszközzel – például hivatalos deklarációval, Államtanács által kiadott dokumentumokkal – azon dolgozik, hogy eloszlassa a kételyeket és meggyőzze a világot arról, hogy Kína a békés fejlődés útján jár.[18]

A nyugaton ugyanakkor, legfőképp az Egyesült Államokban szkeptikusan figyelik a kínai infrastrukturális és egyéb jellegű beruházásokat, valamint a békés fejlődés koncepciójával kapcsolatban is felmerülnek aggályok. A kételyek éppen abból fakadnak, hogy a befektetések révén Kína olyan stratégiai fontosságú infrastruktúrák és területek felett szerezhet ellenőrzést, mint például az Indiai-óceán, illetve a Báb-el Mandeb szoros, amelyek felügyeletére a számos ország haditengerészetét befogadó Dzsibutiból adódik lehetőség, ahol az Egyesült Államok, Franciaország, Japán és Olaszország mellett Kína is rendelkezik katonai bázissal.[19]

A világ különböző pontjain zajló kínai infrastrukturális beruházások, valamint a gazdasági folyamatokon túlmenően olyan aspektusok, mint a kritikus infrastruktúrák egyes technológiai elemeinek vagy akár egészének kínai kézbe kerülése, továbbá a kínai eredetű hibrid- és kibertámadások, valamint a katonai erődemonstrációk és a kínai geopolitikai érdekekhez való erős ragaszkodás mind hozzájárul ahhoz, hogy elsősorban az Egyesült Államok, de a NATO is, mint szervezet – valamint olyan országok, mint például Japán, Dél-Korea egyre inkább fenyegetést, de legalábbis kihívást lát a kínai előretörésben.[20]

KÍNA, MINT STRATÉGIAI KIHÍVÓ

Kínai stratégia és innováció

Wang Xiangsui és Qiao Liang kínai katonai teoretikusok 1999-ben a korlátok nélküli háborúról szóló elméletükben kifejtették, hogy a modern háborúk már nem csak, hogy nem korlátozódnak a hagyományos értelemben vett katonai műveletekre, hanem egyenesen nincs olyan dimenzió, amelyben ne lehetne hadat viselni, legyen szó gazdasági, társadalmi, kulturális vagy akár ökológiai, pszichológiai stb. dimenziókról. A szerzők hosszan értekeznek az erősebb és a gyengébb országok által használható hadviselési módszerek lehetőségeiről, például arról, hogy gyengébb vagy felemelkedésben levő félként a cél megtalálni és kihasználni azokat a kiskapukat, amelyeken keresztül győzedelmeskedni lehet. Különösen erősen jelennek meg a gazdasági dimenziót érintő hadviselési módszerek, például a pénzügyi hadviselés, azon belül is a szankciók, embargók, illetve a hitelezésen keresztül történő befolyásszerzés, amelyeket a szerzők az Egyesült Államok mintájával szemléltetnek.[21]

Ugyan a kínai szerzőpáros könyve különösen az Egyesült Államokra fókuszál, a gazdasági térnyerés és befolyásszerzés kapcsán ma már leginkább Kína merül fel példaként, míg az Egyesült Államok inkább saját világgazdasági, illetve egyéb hatalmi szempontból

értékelhető vezető szerepének megőrzésére való törekvésének kontextusában kerül értékelésre.[22] Utóbbi mondatból kiderül, hogy Kína nem kizárólag a gazdasági befolyásszerzés miatt kelt aggodalmat nyugaton, hanem egyéb más aspektusok miatt is.

Mielőtt az említett aspektusok részletei kibontásra kerülnének, fontos leszögezni, hogy Kína jelenleg nem áll készen az amerikai globális vezető szerep leváltására, már csak azért sem, mert a világgazdasági térnyerése ellenére nem képes olyan univerzális, nemzetközi értékek közvetítésére, amelyek betölthetnék az amerikaiak után maradt űrt.[22] Részint ezért is jó kommunikációs stratégia Kína számára a multipoláris világrend megszületésének hangoztatása,[22] mivel így képes fenntartani azt a szerepet nemzetközi szinten, hogy egy békésen fejlődő, a világ kizárólagos vezetői pozíciójára igényt nem formáló, ugyanakkor a saját nemzeti érdekeit szem előtt tartó, felelős nagyhatalomként emelkedik fel, aki a fejlődésén keresztül a világ többi országának fejlődését is elősegíti – például az Egy Övezet, Egy Út kezdeményezésen keresztül.[18]

A békés fejlődésen átlendülve ugyanakkor érdemes megvizsgálni Kína stratégiai céljait, nemzeti érdekeit és a mindennapokban végzett tevékenységeit is. Amikor kínai stratégiai tervekről beszélünk, vissza kell térni a megszégyenülés évszázadának kiküszöböléséhez és Kína évszázadokkal ezelőtti hatalmi pozíciójának visszaállításához. Utóbbi egy olyan hosszú távú cél, amelyet csak türelmes és megfontolt lépéseken keresztül lehet elérni és ezzel Kína vezetői is tisztában vannak. Csiang Cö-min elnök például a 2000-res évek elején arról beszélt, hogy Kína újbóli naggyá tétele egy generációkon átívelő célkitűzés.[23] Ezen hosszú távú gondolkodást tükrözi vissza a 2049-ig kitűzött célegyüttes, amely megjelenik a Kína által 2021-ben elfogadott 14. ötéves tervben is és amely olyan részcélokból áll, mint például a kutatás-fejlesztés magasabb szintre emelése, az információs hálózatok modernizációja és a technológiai innovációs folyamatok fellendítése.[24]

Technológiai vonalon, különösen az olyan feltörekvő és felforgató technológiák (Emerging and Disruptive Technologies, EDTs) fejlesztése terén, mint a kvantumszámítás vagy a mesterséges intelligencia, Kína jelenleg a világ egyik élenjárója az Egyesült Államokkal egyetemben, ami nem véletlen, hiszen a NATO által nyilvánosságra hozott 2021-es adatok alapján az Egyesült Államok éves szinten legalább 800 milliárd dollárt fordít a kutatás-fejlesztés támogatására, míg Kína megközelítőleg 700 milliárd dollárt.[25] Utóbbi 2024-ből is rendelkezik friss adatokkal, amely alapján az éves ráfordítás 500 milliárd dollárt körül alakult.[26] Külön kiemelendő Kína esetében a nukleáris reaktortechnológia, valamint az űrtechnológia, amelyek területén Kína szintén élen jár. Előbbi esetében a sóolvadékos reaktorok fejlesztésében [27], míg utóbbinál különösen a műholdfelbocsátás terén tett jelentős előrelépést az ázsiai ország. 2015 és 2025 között mintegy 1000 egységgel növelte felbocsátott műholdjai számát, továbbá jelentős erőforrásokat fektet műholdelhárító képességei fejlesztésére. Mindezen túlmenően csak 2025-ben, nyár közepéig, Kína 19 ISR5 képességekkel rendelkező műholdat bocsátott fel az űrbe.[28]

A robosztus s gyorsütemű fejlesztések ugyanakkor más katonai képességekre is igazak. A 2025. szeptember 3-án megrendezett katonai győzelmi parádén a kínai haderő több olyan fegyverrendszert is felvonultatott, amelyek korábban nem kerültek a nyilvánosság elé. Ilyen fegyverrendszer például az LY-1 (Liaoyuan-1) irányított energiájú lézerfegyver,

[5] ISR: Intelligence, Survellance, Reconnaissance, vagyis Hírszerzés, Megfigyelés, Felderítés.

amely elsősorban hajóvédelemre szolgál drónok és rakéták ellen, viszont mivel a felvonuláson nyolc-kerekes (8x8) HZ141 típusú járműveken jelentek meg az eszközök, ezért feltételezhető, hogy szárazföldi alkalmazásukra is van lehetőség. [29]

A parádén szintén feltűntek a kínai haditengerészet által használt új, vízfelszíni célpontok ellen bevethető szuperszonikus és a nagyobb sebességre képes hiperszonikus rakéták, valamint a szintén haditengerészet által használt új típusú, tengeralattjáróról telepíthető víziaknák (AQS003A), illetve felderítésre és megfigyelésre használt pilóta nélküli, víz alatti HSU100 típusú drónok (Unmanned Underwater Vehicle, UUV). Végül, de nem utolsó sorban feltűntek pilóta nélküli felszíni drónok is (Unmanned Surface Vessel, USV), valamint repülőgéphordozóról indítható pilóta nélküli harci légijárművek is (Unmanned Combat Aerial Vehicle, UCAV). Az eseményen újonnan fejlesztett helikopterdrónok, tengeralattjáróról indítható, nukleáris robbanófejet hordozni képes ballisztikus rakéták, interkontinentális ballisztikus rakéták és új típusú harckocsik is feltűntek. [29]

Összességében a fejlesztési hangsúly egyértelműen a rakéta- és a dróntechnológiára helyeződött, különös tekintettel a haditengerészeti képességekre, ami szintén nem véletlen. Ugyan Kína korábban alapvetően az A2/AD képességeinek, vagyis a hozzáférést gátló, terület-megtagadó (Anti-Access/Area Denial, A2/AD) kapacitások fejlesztésére fókuszált leginkább a regionális érdekeinek védelmezése érdekében, napjainkra azonban a kínai fegyverkezés kezdi kiépíteni a globális erőkivetítési képességeket is, amelyeket a repülőgéphordozók építése és az azokra telepíthető új típusú fegyverzet is igazol.[30] Kína éppen 2025. novemberében állította hadrendbe harmadik, egyben legmodernebb repülőgéphordozóját, amelyet Fujian névre kereszteltek.[31]

Végezetül fontos megemlíteni, hogy többek között az orosz-ukrán háború tanulságait levonva, a kínai haderő folyamatos strukturális és doktrinális átalakuláson is átesik, többek között említve az ember és gép által közösen végrehajtható műveletek kivitelezésére irányuló képesség integrálásának célját, valamint a Stratégiai Támogató Erők feloszlatását és az Információs Támogató Erők (Information Support Force, ISF) létrehozását, amelynek célja a kínai versenyképesség fenntartása és fejlesztése az információs térben.[32]

Az eddig leírtakat összegezve arra lehet következtetni, hogy Kína ugyan kommunikációjában erősen hangsúlyozza a békés fejlődés (korábban békés felemelkedés) koncepcióját és igyekszik megőrizni a felelős és megfontolt, más országok belügyeibe bele nem avatkozó nemzet képét, másrészről ugyanakkor határozottan kiáll az állam érdekei mellett, amelyek elérésére ellentmondást nem tűrően törekszik, mint például Tajvan szigetének visszacsatolására és így Kína újraegyesítésére.[33] Mindemellett fontos hozzátenni, hogy a kínai haderő egyértelműen a legrosszabb forgatókönyvek megvalósulására, vagyis egy esetleges háború kitörésére is igyekszik felkészülni, ami már csak abból a szempontból is érthető, hogy Kínának reagálnia kell a nyugat felől érkező és ellene irányuló egyre erősödő aggodalomra és összezárásra.

A NATO Kínával kapcsolatos felfogása

Az Egyesült Államok már Barack Obama elnöksége alatt megkezdte az alapvető fókusz áthelyezését a csendes-óceáni térségre a kínai gazdasági előretörés, haderőfejlesztés, befolyásszerzés, valamint a Dél-kínai tenger körüli konfliktusos helyzet miatt. Obama elnök hivatali ideje alatt előtérbe került az a gondolkodás, hogy növelni kell a térségben az amerikai tengerészgyalogosok számát, valamint erősíteni kell a Kínával szembe helyezkedő,

vagy legalábbis Kínával szemben biztonsági aggályokkal rendelkező országokkal a diplomáciai és kereskedelmi kapcsolatokat. Az Ázsia felé fordulással Obama elnök tulajdonképpen felvállalta Kínával a stratégiai versengést. [34] Ugyan ekkor még nem volt teljesen nyílt a két nagyhatalom közötti nézeteltérés, Donald Trump első elnöksége alatt (2017-2021) gyakorlatilag nyílt szembenállássá változott a két ország viszonya. A 2017-ben kiadott amerikai Nemzeti Biztonsági Stratégia egyértelműen az amerikai érdekek, az amerikai befolyás, biztonság, jólét, illetve hatalom kihívójaként aposztrofálja mind Oroszországot, mind pedig Kínát, akiket egyúttal revizionista hatalmaknak is nevez.[35] Nem véletlen tehát az akkoriban kialakult vámháború sem, ahogy a Huawei elleni intézkedések és a jelenkorra csatolva, Donald Trump második elnöki ciklusa alatti újabb és erőteljesebb kereskedelmi háború sem.[36]

Végül, de nem utolsó sorban az Egyesült Államok és Kína közötti kapcsolat vonatkozásában meg kell említeni a Biden-adminisztráció (2021-2025) alatt 2022-ben kiadott Nemzeti Biztonsági Stratégiát, amely gyakorlatilag az indiai-csendes-óceáni térséget jelöli meg legfőbb amerikai fókuszterületnek a kínai befolyásszerzés és a jelenlegi világrend megváltoztatására irányuló kínai törekvések miatt. Ahogyan a dokumentum fogalmaz, egyedül Kínának van rá elegendő kapacitása, illetve szándéka, hogy újra formálja a világot, aminek elérése érdekében a gazdasági, katonai és technológiai dimenziókban is igyekszik vezető szerephez jutni. Ebből adódóan az Egyesült Államok nyíltan deklarált célja maga mögött tartani Kínát és a globálissá váló versenyben megőrizni a katonai, illetve a technológiai fölényt, amely biztosítja az amerikai állampolgárok, valamint az Egyesült Államok szövetségeseinek hosszú távú békéjét és biztonságát.[37]

Az amerikai érdekeket, illetve biztonsági percepciókat figyelembe véve érthetővé válik, hogy miért volt fontos az Egyesült Államok számára, hogy a Kínával való szembe helyezkedés a szövetségesi körében is megjelenjen, így a NATO-ban is. Elsőként 2019-ben a NATO-szövetségesek londoni csúcstalálkozóján kiadott kommünikében jelent meg Kína, mint kihívás, bár ekkor még a lehetőségek és kihívások kettősségével jellemezték a Kínával való viszonyt.[38] Bár az európai államok kezdetben – és részint ma is – elsősorban fontos gazdasági – kereskedelmi partnerként tekintettek és tekintenek Kínára, az Egyesült Államok felől érkező nyomás hatására, valamint az önálló felismerések mentén Európa is változtatott a Kínával kapcsolatos biztonsági percepcióin, különösen, ami a technológiai versenyt és a kritikus infrastruktúrák védelmét illeti.[39] A kínai információs és dezinformációs műveletek, a kritikus infrastruktúrák elleni kínai kibertámadások, a transzatlanti egység aláásására irányuló törekvések és az olyan kínai egyetemi tanulmányok, mint amelyek például az európai vagy az amerikai energiahálózat sebezhető pontjait próbálják felderíteni, megkongatták a vészharangot Európában is.[40] Külön aggodalomra adhatnak okot a kínai tiszta – vagy környezetbarát technológiák, amelyek terén az ázsiai ország élen jár és ezért számtalan európai országban megtalálhatók, mint például a napelemes rendszerekhez és áramátalakításhoz szükséges technikai berendezések, amelyeken keresztül akár szabotázsakciót is végre lehet hajtani az eszközök távvezérlésén keresztül, ezzel akár az egész európai elektromos hálózatot megbénítva.[41] Ilyen és ehhez hasonló aggodalmak igazolják, hogy a 2022-ben Madridban elfogadott új NATO Stratégiai Koncepció már a korábbinál jóval erőteljesebb nyelvezetet használ Kínával szemben. A dokumentum alapján a kínai kibertámadások, hibrid tevékenységek, a konfrontatív kommunikáció, a gazdasági függőségi viszonyok kialakítására való törekvés, illetve a dezinformációs műveletek veszélyt jelentenek a

Szövetségesek biztonságára nézve. Éppen ezért a Szövetség a jövőben mindent megtesz, hogy megbirkózzon a Kína, illetve más kihívók felől érkező kihívásokkal és fenyegetésekkel.[42] Többek között cél a technológiai fölény megtartása, ami azonban nem egyszerű feladat, hiszen a NATO mellett Kína is gőzerővel fejleszti és adaptálja a technológia újabb és újabb vívmányait, ami előre nem látható kimenetellel végződő hatalmi-stratégiai versenyt eredményez, mely verseny fontos területei például a mesterséges intelligencia, a rakétatechnológia vagy akár az űrtechnológia.

Összegezve, a NATO jelenlegi biztonsági megközelítése Kínával kapcsolatban elsősorban arra épül, hogy Kína nem közvetlen katonai ellenfél, de rendszerszintű kihívást jelent a szövetség biztonsága, értékei és működése szempontjából. Jelenünkben kiemelten fontos a döntéshozási folyamatok gyorsaságának szintje, valamint a rohamosan fejlődő technológiák sikeres és gyors adaptálása. Nem túlzás kijelenteni, hogy a 21. századi stratégiai versenyben az a fél érezheti majd közel magához a győzelmet, amelyik hatékonyabban és gyorsabb ütemben képes adaptálni és adaptálódni a dinamikusan változó és folyamatosan fejlődő technológiai innovációs környezethez. Nem véletlen tehát, hogy a NATO is mindent elkövet annak érdekében, hogy szorosabbra fűzze együttműködését a civil szférában tevékenykedő és sokszor jóval előrehaladottabb technológiával rendelkező vállalatokkal, amelyek segíthetnek a Szövetségnek megőrizni a technológiai fölényét, ezzel biztosítva a szervezet relevanciáját, valamint a hatékony kollektív védelmi képességeket.

ÖSSZEGZÉS ÉS A NATO-KÍNA KAPCSOLATOK JÖVŐJE

Jelenleg a NATO és Kína, valamint Kína és az Egyesült Államok nem ellenségek. Nyugati felfogás szerint Kína rendszerszintű kihívást jelent, és azon túlmenően, hogy lépést kell tartani gazdasági, katonai, technológiai vonatkozásban, biztosítani kell, hogy ne legyen képes aláásni a transzatlanti egységet és átformálni a jelenleg fennálló világrendet. A kihívótól való félelem tulajdonképpen szemlélhető John Herz biztonsági dilemma elméletén keresztül is, mivel a fegyverkezésre fegyverkezés a válasz a saját oldali biztonság megőrzése érdekében, amelyet azonban a szembenálló fél tart majd fenyegetésnek a saját biztonságára nézve.[43] Ezen szembenálló fél, Kína, egyértelműen Washington befolyását látja érvényesülni a NATO-ban, illetve minden ellene irányuló tevékenységet olyan kísérletként aposztrofál, amelyek megpróbálják Kínát meggátolni abban, hogy elérje a NATO-szövetségesek stratégiai fejlettségi szintjét. Ez utóbbi, a NATO és az Egyesült Államok stratégiai dokumentumai alapján igaznak is bizonyulnak. A NATO és Kína közötti viszony tehát némileg feszült, viszont egyelőre – és remélhetőleg a későbbiekben is – megmarad a stratégiai versengés szintjén, nyílt katonai konfliktusok nélkül.[44] A jövőben természetesen fontossá válik majd Tajvan helyzetének végleges rendezésének alakulása, a világgazdasági folyamatok további formálódása, a technológiai verseny kifutása, az erőforrásokért vívott harc és minden egyéb előre nem látható körülmény, amelyek befolyásolhatják ezen versengő hatalmak jövőbeli viszonyát.

FELHASZNÁLT IRODALOM

[1] Xi Jinping speech: Achieving Rejuvenation Is the Dream of the Chinese People. 2012. https://www.neac.gov.cn/seac/c103372/202201/1156514.shtml (2025.10.20.)

[2] Full text of the report to the 20th National Congress of the Communist Party of China. International Department, Central Committee of CPC. 2023. https://www.id-cpc.org.cn/english2023/tjzl/cpcjj/20thPartyCongrssReport/ (2025.10.20.)

[3] Deng Xiaoping, 24 Character Strategy. World Press. 2019. https://neverlamentcasually.wordpress.com/2019/10/03/hide-your-capabilities-deng-xiaoping-notes-3-10-2019/ (2025.10.20.)

[4] Jorge Antonio Chávez Mazuelos: The Chinese Dream of National Rejuvenation and Foreign Policy under Xi Jinping. Agenda Internacional. 29. évf. 2022. pp. 31-35. https://www.researchgate.net/publication/365112087_The_Chinese_Dream_of_National_Rejuvenation_and_Foreign_Policy_under_Xi_Jinping (2025.10.20.)

[5] Tessa Wong: What new weapons on show at huge parade say about China's military strength. BBC. 2025. https://www.bbc.com/news/articles/cjr1reyr059o (2025.10.21.)

[6] Xi Jinping: The Chinese Dream Is the People's Dream. 2015. Theory China. https://en.theorychina.org.cn/c/2021-04-30/1392382.shtml (2025.10.20.)

[7] Pradeek Krishna: Kuomintang Through The Ages. University of Nottingham – Taiwan Insight. 2022. https://taiwaninsight.org/2022/12/20/kuomintang-through-the-ages/ (2025.10.25.)

[8] Gyuris Ferenc: Kína Iparának Átalakulása a Gazdasági Reform Évtizedeiben, Földrajzi Közlemények, 2010. 134. évf. 2. sz. pp. 217-229. https://www.researchgate.net/publication/319523826_Kina_iparanak_atalakulasa_a_gazdasagi_reform_evtizedeiben_The_transformation_of_Chinese_industry_during_the_decades_of_the_economic_reform (2025.10.25.)

[9] John R. Platt: Six Lessons From the World's Deadliest Environmental Disaster. The Revelator. 2024. https://therevelator.org/china-sparrow-campaign/ (2025.10.27.)

[10] Alan Smart – Jinn-Yuh Hsu: The Chinese Diaspora, Foreign Investment and Economic Development in China. The Review of International Affairs, 2004. 3. évf. 4. sz. pp. 544-566. https://www.researchgate.net/publication/240237932_The_Chinese_Diaspora_Foreign_Investment_and_Economic_Development_in_China (2025.10.29.)

[11] World Bank Group: GDP – China. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD?locations=CN (2025.10.29.)

[12] Pallavi Rao – Miranda Smith: Ranked: The World's Largest Economies in 2026. Visual Capitalist. 2025. https://www.visualcapitalist.com/ranked-the-worlds-largest-economies-in-2026/ (2025.10.29.)

[13] Szun-Ce: A háború művészete, Helikon Kiadó, 2020.

[14] European Commission: Competence Centre on Foresight. China's economic power on uncertain speed. 2022. https://knowledge4policy.ec.europa.eu/foresight/chinas-economic-power-uncertain-speed_en (2025.11.05.)

[15] Spencer Feingold: China's Belt and Road Initiative turns 10. Here's what to know. World Economic Forum. 2023. https://www.weforum.org/stories/2023/11/china-belt-road-initiative-trade-bri-silk-road/ (2025.11.05.)

[16] Christoph Nedopil Wang: Green Finance and Development Center. 2025. https://greenfdc.org/china-belt-and-road-initiative-bri-investment-report-2025-h1/?cookie-state-change=1762867492983 (2025.11.05.)
[17] Mercator Institute for China Studies: Mapping the Belt and Road initiative: this is where we stand. 2018. https://merics.org/en/tracker/mapping-belt-and-road-initiative-where-we-stand (2025.11.05.)
[18] Information Office of the State Council of the People's Republic of China: China's Peaceful Development. 2011. http://www.china.org.cn/government/whitepaper/node_7126562.htm (2025.11.06.)
[19] Andrea Kuoman: Djibouti: Djibouti: The tiny valuable nation hosting the world's military giants. Universidad de Navarra. https://www.unav.edu/web/global-affairs/djibouti-the-tiny-valuable-nation-hosting-the-world-s-military-giants (2025.11.06.)
[20] U.S. Global Leadership Coalition: China's Growing Global Influence: What's at Stake? 2021. https://www.usglc.org/chinas-growing-influence-is-america-getting-left-behind/ (2025.11.06.)
[21] Qiao Liang – Wang Xiansui: Unrestricted Warfare. PLA Literature and Arts Publishing House. 1999. https://www.c4i.org/unrestricted.pdf (2025.11.07.)
[22] Suisheng Zhao: The Collapse of the US-led World Order: China Gains Ground but Not Ready to Replace It. The Asan Forum. 2025. https://theasanforum.org/the-collapse-of-the-us-led-world-order-china-gains-ground-but-not-ready-to-replace-it/ (2025.11.10.)
[23] Aust. Stefan – Geiges Adrian: Hszi Csin-ping: A világ legnagyobb hatalmú embere. Corvina Kiadó. 2022.
[24] Outline of the People's Republic of China 14th Five-Year Plan. Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf (2025.11.10.)
[25] NATO: Science and Technology Trends 2025-2045. https://sto-trends.com/ (2025.11.10.)
[26] The State Council – The People's Republic of China: China's R&D spending reports steady growth in 2024. https://english.www.gov.cn/archive/statistics/202509/29/content_WS68da7d8ec6d00ca5f9a06888.html (2025.11.10.)
[27] Portfolio: Kína átvette a vezetést: tudományos áttörés történt az atomversenyben. https://www.portfolio.hu/gazdasag/20250422/kina-atvette-a-vezetest-tudomanyos-attores-tortent-az-atomversenyben-756265# (2025.11.10.)
[28] United States Space Force: Space Threat Fact Sheet. 2025. https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet/ (2025.11.11.)
[29] Naval News: Chinese Military Parade Details New Naval Missiles, Drones. https://www.navalnews.com/naval-news/2025/09/chinese-military-parade-highlights-naval-drones-and-missiles/ (2025.11.11.)
[30] Fabian-Lucas Romero Meraner: China's Anti-Access/Area-Denial Strategy. The Defence Horizon Journal. 2023. https://tdhj.org/blog/post/china-a2ad-strategy/ (2025.11.11.)
[31] Laura Bicker: China launches new aircraft carrier in naval race with the US. BBC. 2025. https://www.bbc.com/news/articles/c62e0yx39g5o (2025.11.11.)

[32] Kartik Bommakanti – Rahul Rawat: Mapping the Recent Trends in China's Military Modernisation – 2025. Observer Research Foundation. 2025. https://www.orfonline.org/research/mapping-the-recent-trends-in-china-s-military-modernisation-2025 (2025.11.11.)
[33] White Paper: The Taiwan Question and China's Reunification in the New Era. 2022. https://us.china-embassy.gov.cn/eng/zgyw/202208/t20220810_10740168.htm (2025.11.11.)
[34] Richard Fontaine – Robert Blackwill: Obama tried to pivot to Asia in 2011. We must succeed this time. Center for a New American Security. 2024. https://www.cnas.org/publications/commentary/obama-tried-to-pivot-to-asia-in-2011-we-must-succeed-this-time (2025.11.13.)
[35] National Security Strategy of the United States of America. 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (2025.11.13.)
[36] Csurgó Dénes: Trump és Kína vámháborújában senki nem nyer, de van, aki jobban veszít. Telex. 2025. https://telex.hu/gazdasag/2025/05/04/trump-usa-kina-vamhaboru (2025.11.13.)
[37] National Security Strategy of the United States of America. 2022. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (2025.11.13.)
[38] NATO: London Declaration. 2019. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/12/04/london-declaration (2025.11.14.)
[39] Chris Kremidas-Courtney: Hybrid storm rising: Russia and China's axis against democracy. European Policy Center. 2025. https://www.epc.eu/publication/Hybrid-storm-rising-Russia-and-Chinas-axis-against-democracy-64b158/ (2025.11.14.)
[40] Jianhua Zhang et al.: Vulnerability analysis of the US power grid based on local load-redistribution. Jiangsu Normal University, Safety Science 80. sz. 2015. pp. 156–162.
[41] Erika Langerová: China Holds a Kill Switch to European Power Grids. Choice. 2025. https://chinaobservers.eu/china-holds-a-kill-switch-to-european-power-grids/ (2025.11.14.)
[42] NATO 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (2025.11.14.)
[43] John H. Herz.: Idealist Internationalism and the Security Dilemma. World Politics. 2. évf. 2. szám. 1950. pp. 157-180. https://www.jstor.org/stable/2009187?seq=18 (2025.11.14.)
[44] Jamie Shea: NATO-China Relations. CERIS. https://www.ceris.be/blog/nato-china-relations-charting-the-way-forward/ (2025.11.14.)

DOI: https://doi.org/10.12700/btsz.2025.7.4.27

SAFETY AND SECURITY ENGINEERING OF DIGITAL SUBSTATIONS IN CRITICAL INFRASTRUCTURE

DIGITÁLIS ALÁLLOMÁSOK BIZTONSÁGTECHNIKÁJA A KRITIKUS INFRASTRUKTÚRÁBAN

MÓROCZ Máté[1]

Abstract

The digitalization of power systems has become one of the most significant technological transformations in critical infrastructures over the past decade. During the modernization of transmission and distribution networks, the introduction of digital control and protection technologies particularly those based on the IEC 61850 standard family has fundamentally reshaped the operation of network architectures. In parallel, however, digitalization has also introduced new security and reliability risks. The transition highlights that as the level of automation in energy systems increases, the boundary between physical and cyber security layers becomes increasingly blurred, since substation infrastructure now clearly operates as a cyber-physical system. From a critical infrastructure protection perspective, a key characteristic of digital substations is that the simultaneous flow of data and energy greatly amplifies the impact of security incidents.
The aim of this study is to examine the operation and protection of digital substations from the perspective of critical infrastructure protection.

Keywords

critical infrastructure, digital substation, IEC 61850, physical security, cyber-physical system, energy protection

Absztrakt

A villamosenergia-rendszerek digitalizációja az elmúlt évtizedben a kritikus infrastruktúrák átalakulásának egyik legjelentősebb technológiai folyamata lett. A villamosenergia-átviteli és -elosztó rendszerek korszerűsítése során a digitalizált irányítási és védelmi technológiák bevezetése, különösen az IEC 61850 szabványcsalád alapvetően átalakította a hálózati architektúrák működését. Ezzel párhuzamosan azonban a digitalizáció új biztonságtechnikai és megbízhatósági kockázatokat is teremtett. Az átállás rámutat arra, hogy az energetikai rendszerek automatizáltsági fokának növekedésével a fizikai és kiberbiztonsági rétegek közötti határ elmosódik, mivel az alállomási infrastruktúra már egyértelműen kiberfizikai rendszerként működik. A kritikus infrastruktúra-védelem szempontjából a digitális alállomások sajátossága, hogy az adat- és energiaáramlás egyidejűsége miatt a biztonsági incidensek hatása sokszorosan felerősödik.
Jelen tanulmány célja, hogy a digitális alállomások működését és védelmét kritikus infrastruktúra-védelmi szemszögből vizsgálja.

Kulcsszavak

kritikus infrastruktúra, digitális alállomás, IEC 61850, fizikai biztonság, kiberfizikai rendszer, energetikai védelem

[1] morocz.mate@stud.uni-obuda.hu | ORCID: 0009-0007-2150-2893 | PhD Student, Doctoral School on Safety and Secu-rity Sciences Óbuda University | Doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az energetikai infrastruktúra a modern társadalmak egyik legösszetettebb, legnagyobb kockázati kitettségű és egyben legkritikusabb rendszere. A villamosenergia-ellátás folyamatossága alapvető feltétele az állam gazdasági, katonai és társadalmi stabilitásának. A Nemzetközi Energiaügynökség (IEA) 2024-es jelentése szerint a globális villamosenergia-fogyasztás 2014 és 2024 között mintegy 32%-kal emelkedett, miközben az elektromos hálózatok automatizáltsági és digitalizáltsági foka több mint kétszeresére nőtt és a hálózati digitalizációs beruházások értéke meghaladta a 230 milliárd USD-t évente [1]. Ezzel párhuzamosan az energiaelosztás és -felügyelet rendszerei egyre inkább adatvezérelt és hálózati architektúrákra épülnek, ami a megbízhatóság javulását hozza, ugyanakkor növeli a biztonsági kockázatok komplexitását.

A digitális alállomások (Digital Substations) olyan, nagymértékben automatizált és kommunikáció-orientált energetikai létesítmények, amelyekben a hagyományos, analóg jelátvitelt Ethernet-alapú kommunikációs rétegek, a berendezések közötti valós idejű adatkapcsolatot pedig Intelligent Electronic Devices (IED) és Merging Unit egységek biztosítják [5], [6]. Ezek az eszközök képesek automatikusan felismerni, izolálni és kezelni hálózati eseményeket, ezzel csökkentve az üzemzavarok kockázatát. A modern alállomási architektúrákban a mérési, vezérlési és védelmi folyamatok digitális adatfolyamokként (Sampled Values, GOOSE üzenetek) áramlanak a process bus és station bus hálózatokon keresztül, amely jelentős előrelépést jelent az interoperabilitás és üzemviteli hatékonyság terén [7].

Ugyanakkor a digitalizált architektúrák új típusú sérülékenységi mintázatokat hoznak létre. A fizikai infrastruktúra (berendezésházak, kábelezés, hálózati kapcsolók), a kommunikációs eszközök, valamint a távfelügyeleti interfészek mind potenciális támadási pontokká válnak [9]. Az IEC 61850 process-bus és station-bus hálózatainak nyitottsága, az időszinkronizációs protokollok (IEEE 1588 PTP) függősége, illetve a valós idejű adatkapcsolatok érzékenysége miatt a fizikai védelem és a kiberbiztonság már nem kezelhető külön területekként. A biztonságtechnikai fókusz a 2020-as évektől kezdve a komplex rezilienciaalapú megközelítés felé tolódott el. Nem csak pusztán az eszközök vagy építmények védelmét, hanem a rendszerszintű működőképesség megőrzését tekintik elsődleges célkitűzésnek [8], [10]. A kritikus infrastruktúrák — így az energetikai alállomások — védelmében a fizikai, kiber és üzemviteli rétegek integrált, egymást erősítő biztonsági architektúrája vált meghatározóvá.

E kontextusban a digitális alállomások nem csupán technológiai fejlesztési irányt, hanem nemzetbiztonsági szempontból kiemelt kockázati területet is jelentenek. Az e rendszerekhez kapcsolódó fizikai hozzáférési pontok, berendezések és hálózati infrastruktúrák biztonságtechnikai kezelése ma már elválaszthatatlan része a kritikus infrastruktúra-védelmi stratégiáknak Magyarországon és az Európai Unióban egyaránt.

KUTATÁSMÓDSZERTAN

A kutatás módszertana a digitális alállomások kiberfizikai sérülékenységeinek, támadási felületeinek és rendszerszintű következményeinek feltárására irányul, különös hangsúlyt helyezve a kritikus infrastruktúrák – ezen belül az energetikai ellátórendszer – védelmi követelményeire. A vizsgálat alapját a modern, IEC 61850-alapú digitális alállomások kommunikációs és védelmi architektúrája képezi, mivel ezekben az állomásokban a

fizikai folyamatok (áram, feszültség, teljesítményáramlás) és a digitális vezérlési rétegek (GOOSE, Sampled Values, MMS) szoros, nagysebességű kölcsönhatása olyan összetett kiberfizikai rendszert eredményez, amely a hagyományos alállomásokhoz képest jelentősen más kockázati profilt mutat. A módszertani megközelítés ennek megfelelően egymásra épülő, több szintű elemzési struktúrát követ.

A kutatás első lépése a digitális alállomások működését meghatározó kommunikációs és védelmi protokollok, valamint a kritikus infrastruktúrákra vonatkozó hazai és európai szabályozások kritikus szemmel való elemzése. Ezen belül kiemelt fókuszt kap az IEC 61850-szabványcsalád (GOOSE, SV, MMS, SCL) architektúrája, továbbá az ENISA smartgrid biztonsági elemzéseiben azonosított kockázati kategóriák, valamint a magyar létfontosságú rendszerelemeket szabályozó jogszabályi keretek. Ez a lépés biztosítja a kutatás normatív hátterét, és rögzíti azokat a rendszerszintű követelményeket, amelyekhez a vizsgálatok és értékelések igazodnak.

A második lépésben a kutatás a digitális alállomások technológiai architektúrájának műszaki modellezésére épít. Ennek célja annak feltárása, hogy a GOOSE-, SV- és MMS-szinteken bekövetkező manipulációk miként befolyásolják a védelmi döntési folyamatokat és a fizikai berendezések működését.

A harmadik módszertani komponens a kiberfizikai támadásszenáriók elemzése. A támadási vektorok – hamisítás, késleltetés, blokkolás, torzítás, replay, DoS és konfigurációmanipuláció – a teljesség igénye nélkül külön értékelésre kerül abból a szempontból, hogy milyen mértékben veszélyezteti a rendszer működési integritását. A vizsgálat során nemcsak a protokollszintű hatások (pl. GOOSE-késleltetés), hanem a kiberfizikai lánc szintjei is elemzés tárgyát képezik, vagyis az, hogy egy adott támadás milyen kockázattal vezet hibás mezőszinti működéshez vagy rendszerszintű instabilitáshoz.

A módszertan negyedik eleme a kockázatfeltárás, amelynek célja a különböző támadásszintek hatásmechanizmusának strukturált vizsgálata. Az FMEA-megközelítés a hibamódokat (pl. SV-manipuláció, hamis GOOSE-üzenet, MMS-parancsinjektálás) a lehetséges okokkal, következményekkel és észlelhetőséggel összefüggésben vizsgálja, meghatározva azokat a pontokat, ahol a védelmi logika különösen érzékeny, ezzel feltárva a kaszkád folyamatok logikai felépítését. Ez az elemzésmód különösen fontos, mivel a digitális alállomásokban a támadások nem elszigetelt eseményként, hanem egymást erősítő folyamatként jelennek meg.

A kutatás módszertanának utolsó eleme a kritikus infrastruktúra szemszögű értékelés. Ez a lépés a műszaki elemzéseket és a kockázati modelleket összekapcsolja a létfontosságú rendszerekre vonatkozó szabályozási és biztonsági követelményekkel, kiemelve azt, hogy a digitális alállomások sérülékenysége milyen rendszerszintű kockázatot jelent a villamosenergia-ellátás folytonosságára. A vizsgálat célja annak meghatározása, hogy mely támadási vektorok jelentenek valós, rendszerszintű fenyegetést, és mely pontokon szükséges a védelmi architektúra megerősítése a fizikai és kiberbiztonsági kontrollok integrációjával. A kutatási módszertan olyan holisztikus keretet biztosít, amely egyszerre vizsgálja a digitális alállomások kommunikációs, védelmi és fizikai rétegeit, és amely alkalmas arra, hogy a kritikus infrastruktúrák sajátos követelményeihez igazodva átfogó képet adjon a digitális alállomások biztonságtechnikai megvalósíthatóságáról, sebezhetőségi profiljáról és kockázati szintjéről.

KRITIKUS INFRASTRUKTÚRÁK SZABÁLYOZÁSI HÁTTERE

Magyar szabályozási háttér

Magyarországon a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról a villamosenergia-ellátást a nemzeti létfontosságú infrastruktúrák egyik alapvető ágazataként határozza meg, összhangban az Európai Unió kritikusinfrastruktúra-védelmi keretrendszerével [11]. A törvény célja, hogy azonosítsa azokat a rendszereket, amelyek működése nélkülözhetetlen az állam alapvető funkciói, a lakosság ellátásbiztonsága és a gazdaság stabilitása szempontjából. A jogszabály a villamos energia átviteli, elosztási és irányítási infrastruktúráit – beleértve a nagyfeszültségű alállomásokat, vezetékhálózatokat, diszpécserközpontokat és az ezekhez kapcsolódó infokommunikációs rendszereket – létfontosságú rendszerelemként definiálja. Ez azért is kiemelt jelentőségű, mert a villamosenergia-szektor a kritikus infrastruktúrák közötti leginkább hálózatfüggő és interdependens ágazatok közé tartozik: meghibásodása vagy támadása súlyos következményekkel járhat más létfontosságú szolgáltatások működésére (pl. távközlés, vízellátás, egészségügy, közlekedés) [4].

A törvény végrehajtásának részletes követelményeit a 65/2013. (III. 8.) Korm. rendelet határozza meg, amely átfogó eljárásrendet ír elő a létfontosságú rendszerek azonosítására, minősítésére és védelmére [12]. A rendelet bevezeti a biztonsági osztályba sorolás kötelezettségét, amely az adott létesítmény kritikus szerepét, fenyegetettségi szintjét és sérülékenységét figyelembe véve határozza meg a minimálisan szükséges védelmi szintet. Emellett előírja a komplex biztonsági dokumentáció elkészítését, amely tartalmazza a fizikai védelem, a technikai és kiberbiztonság, az üzemvitel-biztonság, valamint a humánbiztonság koordinált elemzését és integrált tervezését. A rendelet kötelezővé teszi továbbá a rendszeres kockázatelemzést, az incidenskezelési protokollok kialakítását, a működési folyamatok vészhelyzeti eljárásrendjét, valamint a biztonsági intézkedések éves felülvizsgálatát.

A magyar szabályozás lényegi eleme, hogy a létfontosságú rendszerelemek védelmét integrált, többdimenziós biztonsági modellben értelmezi, amelyben a fizikai biztonsági intézkedések (pl. kerítés, beléptetés, CCTV, behatolásjelzés) és a kiberbiztonsági rétegek (tűzfalak, hálózati szegmentáció, naplózás, titkosítás, hozzáférés-kezelés) egyetlen egységes védelmi architektúra részeként működnek. Ez a megközelítés különösen releváns a modern, IEC 61850 alapú digitális alállomások vonatkozásában, amelyek kiberfizikai rendszerként működnek, így a fizikai és digitális sérülékenységek kölcsönösen hatnak egymásra. A rendelet hangsúlyozza a védelmi koordinátorok kijelölésének kötelezettségét is, akik a létesítmény és a hatóságok közötti szakmai-jogi kapcsolattartást biztosítják, valamint az éves jelentések és auditok végrehajtásáért felelnek.

Európai Uniós szabályozási háttér

Az Európai Unió 2022/2555 számú (NIS2) irányelve [13] a kritikus infrastruktúrák biztonságának szabályozásában mérföldkőnek számít, mivel jelentős szigorítást vezetett be a kiberfizikai rendszerek védelmében, különösen az energetikai ágazat tekintetében. Az irányelv az energiaellátást „magas kockázatú, stratégiai jelentőségű ágazatként” határozza meg, és előírja, hogy az energetikai szolgáltatók — ideértve az átviteli rendszerirányítókat

(TSO), az elosztóhálózat-üzemeltetőket (DSO), valamint a villamosenergia-ipari szolgáltatókat — átfogó, reziliens biztonságirányítási rendszert hozzanak létre. Ez a rendszer kiterjed a kiberbiztonsági, fizikai biztonsági és üzemviteli biztonsági folyamatok együttes kezelésére, felismerve, hogy a modern energiahálózatok működése kiberfizikai integrációra épül, ahol a digitális és fizikai folyamatok szétválaszthatatlanul kapcsolódnak egymáshoz [3].

A NIS2 külön hangsúlyt fektet a kockázatalapú megközelítésre, amely kötelezi a szolgáltatókat a fenyegetettségek folyamatos értékelésére, a beszállítói lánc biztonságának felügyeletére, valamint a kritikus folyamatokhoz kapcsolódó incidenskezelési, üzemfolytonossági és helyreállítási kapacitások biztosítására. A szabályozás kitér arra is, hogy a létfontosságú energetikai rendszerek esetében nem elegendő a hagyományos, reaktív biztonság, hanem proaktív, előrejelzésen, automatizált és intelligens észlelésen alapuló védelemre van szükség, különösen a villamosenergia-rendszerek digitalizációjának előrehaladása miatt. Az ENISA 2022-es ágazati jelentése rámutat, hogy az uniós tagállamok energetikai infrastruktúráinak mintegy 82 %-a közvetlen függésben áll digitalizált irányítási rendszerekkel, mint például a SCADA (Supervisory Control and Data Acquisition), a DCS (Distributed Control System) vagy az IEC 61850 alapú digitális alállomási technológia [14]. A jelentés szerint a villamosenergia-hálózatok több mint 60 %-a már alkalmaz valamilyen digitális alállomási megoldást, és az átviteli hálózat modernizációjára irányuló beruházások több mint fele közvetlenül az alállomások digitalizációjához kötődik. Ezek az adatok alátámasztják, hogy a hálózati automatizáció és a kiberfizikai rendszerek terjedése az ellátásbiztonság alapfeltételévé vált Európában [1].

Ugyanakkor a digitalizáció növekedése új típusú kitettségeket is eredményezett. A kiberfizikai rendszerek összekapcsoltsága miatt egyetlen sérülékenység — legyen az hálózati protokollban (pl. MMS, GOOSE), időszinkronizációban (IEEE 1588), vagy akár egy IED eszköz szoftverében — rendszerszintű zavarokat idézhet elő. ENISA arra is felhívja a figyelmet, hogy 2020–2022 között az energetikai ágazat ellen irányuló kiberincidensek száma több mint 59 %-kal növekedett, és ezek jelentős része éppen a digitalizált alállomási kommunikációs rétegeket célozta. A hatékonyság és automatizáció növekedésével párhuzamosan tehát a sérülékenységi térkép is bővül, amely indokolttá teszi az integrált biztonsági kontrollok kiépítését, valamint az előírásoknak megfelelő, folyamatos rezilienciafejlesztést [2].

A DIGITÁLIS ALÁLLOMÁSOK TECHNOLÓGIAI ALAPJAI

A modern villamosenergia-átviteli és -elosztási rendszerekben a digitális alállomások (Digital Substations, DSS) az egyik legdinamikusabban fejlődő kritikus infrastruktúrakomponensek közé tartoznak. A nemzetközi statisztikák szerint a nagy feszültségű alállomások digitalizációja 2020–2025 között átlagosan évi 12 %-kal nőtt, amelyet a megújuló energiaforrások integrálása, az IoT-érzékelők terjedése és az energiahálózatok automatizálása motivál. A „digitális átállás” koncepciója olyan átfogó technológiai paradigmát képvisel, amely a primer és szekunder villamos berendezések összekapcsolását Ethernet-alapú, nagy rendelkezésre állású és determinisztikus kommunikációs architektúrára alapozza. A digitális alállomások célja a hagyományos, analóg jelátvitelű rendszerek kiváltása szabványosított adatmodellekkel, protokollokkal és intelligens elektronikus eszközökkel (IED-ek, Merging Unit-ok), amelyek valós időben biztosítják a mérési, vezérlési és védelmi funkciók

adatcseréjét [15]. A szakirodalom kiemeli, hogy a digitalizált alállomási infrastruktúrák lehetővé teszik a kábelezési mennyiség akár 80%-os csökkentését, a hibadetektálás felgyorsítását, valamint a konfigurációs rugalmasság jelentős növelését, különösen a process bus és station bus topológiák bevezetésével [16].

A digitális alállomások technológiai gerincét az IEC 61850 szabványcsalád adja, amely egységes adatmodellt, kommunikációs profilt, konfigurációs nyelvet (SCL), valamint hálózati viselkedési elveket definiál az alállomási automatizáláshoz. A szabvány három hierarchikus működési szintet különít el: a folyamat-szintet (process level), ahol a Merging Unit-ok Sampled Values üzenetekkel digitalizálják és továbbítják a primer áram- és feszültséginformációkat; a mező-szintet (bay level), ahol az intelligens védelmi és vezérlési IED-ek működnek és GOOSE üzeneteken keresztül kommunikálnak; valamint az állomásszintet (station level), ahol a HMI/SCADA rendszerek, a naplózás, felügyelet és az irányítási folyamatok összegződnek [2]. Ez a háromszintű struktúra biztosítja az alállomási automatizálás interoperabilitását, valós idejű kommunikációját és gyors reakcióképességét hálózati események esetén [17].

A digitális alállomások elterjedése ugyanakkor új kockázati dimenziókat is megnyit. A digitális alállomások kiberfenyegetettségi profilja lényegesen komplexebb, mint a hagyományos rendszereké, mivel az IED-ek, a process bus és station bus elemei olyan hálózati protokollokra épülnek, amelyek célzott támadási felületet teremthetnek – különösen a GOOSE, MMS és SV kommunikáció sérülékenységein keresztül [9]. A digitális alállomások legjelentősebb fenyegetései közé tartoznak a manipulált Sampled Values üzenetek, a késleltetett vagy blokkolt GOOSE csomagok, a PTP alapú időszinkronizáció megzavarása, valamint az IED-ek firmware-szintű kompromittálása. Ezen támadástípusok hatása kiterjedhet az automatikus védelmi funkciók hibás működésére, meghibásodások késleltetett felismerésére, vagy akár a megszakítók indokolatlan kapcsolására is – ezáltal a digitális alállomások kiberfizikai integritásának sérülésére. A IEC 61850 architektúra ugyan számos biztonsági és redundanciaelemet tartalmaz (pl. PRP/HSR protokollok, determinisztikus üzenetszórás, hálózati szeparáció lehetősége), azonban a szakirodalom szerint a digitális alállomások biztonsága csak akkor tartható fenn, ha a folyamat-, mező- és állomás-szinten azonosított kockázatokra integrált, kiberfizikai biztonságirányítási modell épül [9]. E modellnek egyszerre kell kezelnie a hálózati protokollsérülékenységeket, az IED-ek eszközszintű biztonsági hibáit, a kommunikációs folyamatok integritását, valamint a fizikai hozzáférés- és környezetvédelmi kontrollokat. A digitális alállomások rezilienciája tehát nem pusztán a technológiai modernizáció függvénye, hanem a többdimenziós biztonsági architektúra megbízható implementációjáé is. Ezért a kiberfenyegetések taxonómiájának kialakítása elengedhetetlen, mivel a digitális alállomások működése olyan időkritikus, többprotokollos környezetben zajlik, ahol a támadások akár néhány ezredmásodperc alatt befolyásolhatják a védelmi döntéseket. A szakirodalomban a fenyegetéseket négy fő kategóriába sorolják: a kommunikációs protokollok elleni támadások, az eszköz- és firmware-szintű támadások, az időszinkronizáció elleni fenyegetések és a fizikai–kiber kombinált (CPS) támadások, amelyek együttesen határozzák meg a digitális alállomások kockázati profilját [5], [9], [10], [16], [18].

A kommunikációs protokollok elleni támadások a digitális alállomások elsődleges sérülékenységi területét jelentik, mivel a rendszer működését az IEC 61850 szabványon alapuló protokollok – GOOSE, Sampled Values (SV) és MMS – valósítják meg. A GOOSE-

üzenetek módosításával vagy késleltetésével a támadók képesek befolyásolni a védelmi IED-ek közötti döntéseket, ami hibás kioldásokhoz, védelmi koordinációs zavarokhoz vagy a hibák késleltetett felismeréséhez vezethet. A Sampled Values torzítása különösen veszélyes, mivel a digitális mérési értékek manipulálása a rendszer teljes védelemfilozófiáját torzíthatja, meghamisítva az áram- és feszültségadatokat, így akár berendezéskárosodást is előidézhet. Hasonlóképpen, az MMS-alapú támadások hozzáférést biztosíthatnak a támadók számára az alállomási konfigurációkhoz vagy a naplóállományokhoz. Kolosok és Korkina kiemelik, hogy ezen kommunikációs sérülékenységek jelentős része abból ered, hogy az IEC 61850 eredeti tervezésekor az adatbiztonsági mechanizmusok – például a kriptográfiai védelem – még nem voltak széles körben alkalmazottak a nagy rendelkezésre állás és a késleltetésminimalizálás érdekében [9].

Az eszköz-, firmware- és konfigurációs szintű támadások a digitális alállomások másik kritikus fenyegetési kategóriáját alkotják. Az IED-ek, Merging Unit-ok és alállomási switch-ek olyan beágyazott rendszerek, amelyek támadhatók hibás firmware-frissítéseken, vagy nem biztonságos konfigurációkon keresztül. A firmware-manipuláció lehetővé teszi a támadó számára, hogy rejtett, rosszindulatú funkciókat illesszen be az eszköz működésébe, amely akár hónapokig észrevétlen maradhat. A konfigurációs állományok – különösen az IEC 61850 SCL fájlok – módosítása az egész alállomás viselkedésére kihat, mivel ezek tartalmazzák a topológiát, a kommunikációs logikát és a védelmi összefüggéseket. A kutatások rámutatnak, hogy a digitális alállomások tervezésében alkalmazott centralizált konfigurációkezelés ugyan egyszerűsíti a mérnöki folyamatokat, de célponttá válhat a támadók számára, akik egyetlen konfigurációs manipulációval a teljes alállomást destabilizálhatják [5], [10].

Az időszinkronizáció elleni támadások különösen súlyos következményekkel járhatnak, mivel a digitális alállomások működése – ideértve a védelmi algoritmusokat, a naplózást és az események sorrendiségét – a mikroszekundumos pontosságú időszinkronizációtól függ. Az IEEE 1588 Precision Time Protocol (PTP) manipulálása, például késleltetés beszúrásával vagy hamis időjel generálásával, hamis időbélyegekhez és hibás védelmi döntésekhez vezethet. A GPS-spoofing szintén valós fenyegetést jelent, mivel több alállomás továbbra is külső időforrásokra támaszkodik, amelyek megzavarása esetén a teljes védelemkoordináció összecsúszhat, torzulva a hibák lokális detektálását [18]. Mivel a digitális alállomások szinkronizációja az SV és GOOSE üzenetek korrekt időértelmezésétől függ, az időszinkron elleni támadások képesek minimális láthatóság mellett is jelentős zavart okozni.

A fizikai–kiber kombinált támadások (CPS – Cyber-Physical Systems támadások) a digitális alállomások egyik legveszélyesebb fenyegetését jelentik, mivel egyszerre célozzák a fizikai berendezéseket és az informatikai rendszereket. Ezekben a támadás-szcenáriókban a támadók például fizikai hozzáférést szerezhetnek egy Merging Unit-hoz vagy IED-szekrényhez, majd hardveralapú manipulációval vagy rogue-eszköz beillesztésével meghamisíthatják a kommunikációs folyamokat. Ugyancsak ide tartoznak a process bus optikai kábeleinek megszakítását követő hamis eszközillesztések, vagy a hálózati switch-ek fizikai resetelése, amelyek a GOOSE és SV üzenetek teljes leállásához vezethetnek [10].

KIBERFIZIKAI TÁMADÁSSZENÁRIÓK ELEMZÉSE

Sampled Values (SV) manipuláció bemutatása

A Sampled Values (SV) üzenetek manipulációja a digitális alállomások legkritikusabb fenyegetései közé tartozik, mivel az SV a primer villamos jelleggörbék – áram, feszültség, teljesítmény – nagy pontosságú, 4 kHz–96 kHz mintavételezési frekvencián továbbított digitális reprezentációja, amely közvetlenül meghatározza a védelmi IED-ek döntéshozatali folyamatát. A szabványosított IEC 61850-9-2LE profilban rögzített SV-keretek akár 256 mintát másodpercenként, fázisonként továbbítanak, ami azt jelenti, hogy már néhány mintapont eltérése is jelentős hibát indukálhat a védelmi algoritmusokban. A kutatások kimutatták, hogy a differenciálvédelemnél alkalmazott védelmi egyenletek érzékenysége olyan mértékű, hogy mindössze 1–3%-os amplitúdótorzítás is elegendő lehet a hibás kioldáshoz, míg a fázistolás akár 2–3 fokos eltérése hibarejtést okozhat nagyfeszültségű távvezetékek esetében [19].

A támadók által végrehajtott SV-érték-manipuláció több formában jelentkezhet. A legegyszerűbb támadás az amplitúdó torzítása, amikor a valós áram- vagy feszültségértékeket egy konstans vagy időben változó skálafaktorral módosítják. Ennek következtében a túláramvédelmi funkciók tévesen alulfeszültség- vagy alulterhelés-jelenséget érzékelhetnek. Még súlyosabb a fázismódosítás, amely a távolsági védelem zónaérzékelését torzítja el: kísérletek szerint 4–5° fáziseltérés a védelem érzékelési tartományát akár 20–25%-kal is eltolhatja, ezzel hibás zónaváltást okozva [20]. A támadók gyakran alkalmaznak hullámforma-alapú manipulációt (waveform crafting), amely során a jel alakját magasabb harmonikus komponensekkel vagy modulált zajjal torzítják, miközben fenntartják az üzenet időzítési és formátumkövetelményeit, így az IED-ek számára a jel továbbra is érvényesnek tűnik. Az ilyen támadások különösen veszélyesek, mivel képesek reprodukálni egy valódi zárlati esemény mintázatát, hamis hibajelzést generálva, amely indokolatlan kioldást vált ki a megszakítókon. A SV-kommunikáció elvesztése (drop-attack) szintén súlyos kockázatot jelent. A process bus topológiákban a SV-áramlat megszakadása azt eredményezi, hogy az IED-ek nem kapnak friss mérési adatot, és az IEC 61850-8-1 szabvány szerinti biztonsági működés miatt „freeze" állapotba kapcsolnak, amelyben a védelmi funkciók jelentős része ideiglenesen letiltásra kerül vagy alapállapotba áll. Ez azt jelenti, hogy a védelem nem képes valós hibákat detektálni, amely – a rendelkezésre álló redundanciától függően – akár teljes védelmi vakfoltokat okozhat az alállomás egyes részein. Az ENISA elemzései rámutatnak, hogy 2020–2022 között az európai energetikai rendszerekben regisztrált védelmi zavarok mintegy 17%-a adatfolyam-szakadásra vagy időzítési anomáliára volt visszavezethető, ami alátámasztja a process bus stabilitásának kritikus szerepét [10]. A SV-réteg elleni támadások kiberfizikai hatása rendkívül magas, mivel közvetlenül a villamos méréseket és a védelmi döntések alapját képező valós idejű információáramlást befolyásolják. Mivel az SV-adatok alapján számított villamos paraméterek – például a komplex teljesítmény, a szinkronpozíció vagy a hibairány – közvetlen összefüggésben állnak a megszakítók vezérlésével és a hálózati stabilitással, az értékek bármilyen manipulációja azonnal, fizikai szinten jelenik meg. Ez különösen érvényes a differenciálvédelemre, amely az egyik leggyorsabb és legérzékenyebb védelem a nagyfeszültségű alállomásokban: már minimális jelhibákra is reagál, hogy megakadályozza a berendezések károsodását. A támadások súlyosságát tovább növeli, hogy az SV-csatornák integritását hagyományosan nem védik olyan kriptográfiai

eszközök, mint a GOOSE-Sec vagy az IEC 62351-6 szerinti hitelesítés, így a támadók számára a legközvetlenebb támadási felületet kínálják [21], [9].

MMS protokoll fenyegetései, rövid elemzése

Az MMS (Manufacturing Message Specification) protokoll a digitális alállomások állomásszintű kommunikációs rétegének gerincét képezi, amelyen keresztül a SCADA-rendszerek, IED-gatewayek, mérnöki munkaállomások és archívumkezelő rendszerek valósítják meg a konfigurációs, irányítási és felügyeleti funkciókat. Az IEC 61850-8-1 által definiált MMS-szolgáltatások teszik lehetővé az IED-ek adatbázisának lekérdezését, a védelmi logikák módosítását, a paraméterezést, a valós idejű adatok olvasását, valamint a parancsok (control commands) kiadását. Bár az MMS kommunikáció nem olyan szigorúan időkritikus, mint a GOOSE vagy a Sampled Values üzenetek, stratégiai jelentősége lényegesen nagyobb, mivel az alállomás teljes konfigurációs és vezérlési felépítésére rálátást és beavatkozási lehetőséget biztosít [2], [10].

A támadók különféle technikákkal élhetnek annak érdekében, hogy kihasználják az MMS-protokoll sajátosságait. A leggyakoribb módszer a jogosultság-kiterjesztés (privilege escalation), amely lehetővé teszi, hogy a támadó adminisztratív hozzáférést szerezzen egy SCADA-szerverhez, mérnöki munkaállomáshoz vagy IED-gatewayhez. A kutatások szerint a digitális alállomásokban használt mérnöki eszközök több mint 65%-a olyan Windows-alapú környezetben fut, amelyek ismert sebezhetőségei – például szolgáltatásmegszakítás, DLL-eltérítés vagy nem biztonságos frissítési mechanizmus – kihasználhatók az MMS-csatornák kompromittálására. Az IED-gatewayek és alállomási adatkoncentrátorok hálózati szolgáltatásait vizsgáló tanulmányok azt is kimutatták, hogy a konfigurációs portokra érkező nem hitelesített MMS-üzenetek egy része képes volt a berendezések újraindítására vagy memóriahibák kiváltására, ami a védelmi funkciók átmeneti kieséséhez vezethet [2].

A Substation Configuration Language (SCL) állományok manipulációja különösen súlyos következményekkel járhat, mivel az SCL-fájlok definiálják az alállomási topológiát, a kommunikációs kapcsolatok struktúráját, az IED-ek interfészeit, a GOOSE- és SV-feltéképezését, valamint a védelmi funkciók közötti logikai összefüggéseket. Egyetlen XML-alapú SCL-elem módosítása – például egy Logical Node átirányítása, egy GOOSE-üzenet új célcímének megadása vagy egy IED-hez rendelt védelmi funkció paramétereinek átírása – az alállomás teljes automatikai logikájának működésére hatással lehet. A rosszindulatú MMS-parancsok kiadása az egyik legközvetlenebb módja annak, hogy a támadó fizikai folyamatokat befolyásoljon. Az IEC 61850 szerint az MMS-szintű „Select-Before-Operate” (SBO) mechanizmus hivatott garantálni, hogy a parancsok nem kerülnek véletlen vagy illetéktelen kiadásra, azonban számos implementáció sérülékenynek bizonyult a jogosultságellenőrzés, session-menedzsment vagy titkosítás hiányosságai miatt. Egy rosszindulatú MMS „Operate” parancs – amelyet a támadó hiteles, de kompromittált sessionön keresztül ad ki – indokolatlan megszakítónyitást vagy -zárást eredményezhet. A rendszer-szimulációk és ENISA által közzétett esettanulmányok rámutattak, hogy már egyetlen, indokolatlan nyitás is súlyos feszültségesést, terhelési átrendeződést és frekvenciainstabilitást válthat ki a hálózatban, különösen nagy terhelési csomópontok közelében. Az ilyen típusú „logikai támadások” különösen veszélyesek, mert nem generálnak látványos hálózati forgalmi anomáliát, hanem a legitim irányítási csatornán keresztül történnek, így az észlelésük különösen nehéz. [9]

A DIGITÁLIS ALÁLLOMÁS KIBERFIZIKAI KASZKÁD SÉRÜLÉKENYSÉGE

A digitális alállomások kiberfizikai kitettségének legsúlyosabb sajátossága, hogy az egyes támadási vektorok nem elszigetelten hatnak, hanem egymást erősítő, többlépcsős kaszkád-folyamatokat indítanak el, amelyekben a kiber- és fizikai események szorosan összekapcsolódnak. Ez a kaszkád-természet élesen eltér a hagyományos, analóg alállomások meghibásodási modelljeitől, mivel a digitális alállomásokban a védelem, az irányítás és az automatizálás funkciói a nagyfelbontású digitális kommunikációs csatornákra és valós idejű adatfeldolgozásra épülnek. A támadások ezért nem egyszerűen „zavaró tényezők", hanem a védelmi döntések integritását megbontó, nagy hatású rendszerszintű zavarok forrásai [5], [10].

Egy tipikus támadási lánc már a process busz manipulációjával megkezdődhet. Ha a támadó a Sampled Values (SV) üzeneteket módosítja – akár amplitúdó- vagy fázistorzítással, akár hullámforma-szintű beavatkozással –, a védelmi IED-ek hibás fázorbecslést végeznek, ami a primer hálózati állapot téves értelmezéséhez vezet. Kutatások kimutatták, hogy 1–3 %-os amplitúdó-hiba vagy 2–5°-os fáziseltérés már elegendő ahhoz, hogy a differenciálvédelem látszólagos hibát észleljen, míg a távolsági védelem zónahatárai 5–10 %-kal is eltolódhatnak a névlegestől [20], [10]. A hibás fázorbecslés közvetlen következménye, hogy a védelmi logika olyan GOOSE-parancsot generál, amely valójában nem felel meg a hálózat fizikai állapotának. A védelmi logikában keletkező hamis GOOSE-üzenetek a kaszkád folyamat második szintjét alkotják. A GOOSE-üzenetek időkritikus, multicast alapú jelzések, amelyek 3–4 ms alatt eljutnak a mezőszinti IED-ekhez. Amennyiben a támadó manipulált bemeneti adatokkal hamis „trip", „block" vagy „interlock" üzenetet generáltat, az IED-ek — a protokoll determinisztikus működése miatt — teljes bizalommal fogadják el azt, mivel a GOOSE-üzenetek eredeti tervezési filozófiája a megbízhatóságra (dependability) és nem a biztonságra (security) épült [22], [10]. Laboratóriumi vizsgálatok szerint egyetlen hamis GOOSE-üzenet képes volt 6–8 mezőszinti megszakító koordinált működését kiváltani, ami az alállomás teljes konfigurációját megváltoztatta [9].

A kaszkád harmadik fázisában a mezőszinten hibásan működő megszakítók fizikai következményeket okoznak. Ezek közé tartozhat a téves leválasztás, amely túlterheli a szomszédos tápvonalakat, a teljesítményáramlási útvonalak hirtelen átrendeződése pedig korlátozási és stabilitási problémákhoz vezethet. Valós hálózati esetek alapján egyetlen, nem tervezett megszakító-nyitás azonnal 20–40 MW teljesítményátrendeződést okozhat a regionális középfeszültségű hálózatokon, míg nagyfeszültségű átviteli szinten ez az érték akár a 150–250 MW tartományba is eshet [23]. Amennyiben a hibás kioldás egyszerre több elosztó vagy átviteli csomópontot érint, a rendszer fokozott valószínűséggel kerül frekvencia-érzékeny tartományba (49,0–49,3 Hz), amely tovább növeli az automatikus terheléslekapcsolási mechanizmusok aktiválódásának esélyét [23].

Az utolsó kaszkádszint a rendszerszintű instabilitás, amely a fizikai működési zavarokból ered. A hibás megszakító-állapotok miatt létrejövő hálózati topológiaváltozások veszélyeztetik a tranziens stabilitást, rontják a szinkrongépek közötti fázisszög-koordinációt és jelentős módosulást okoznak az áramlási interfészek terhelésében. Ez a kaszkádmechanizmus jól illusztrálja, hogy a digitális alállomások sérülékenysége nem egyetlen komponens meghibásodásának következménye, hanem a teljes irányítási és védelmi architektúra integritását determináló rendszerjellemző. Az így kialakuló sérülékenység struktúrája rávi-

lágít arra, hogy a digitális alállomások védelmét integrált, rendszerszemléletű megközelítésben kell kezelni – különösen a kritikus infrastruktúrák esetében –, mivel a mérési adatok, a kommunikációs protokollok és a védelmi logikák harmóniája bontakozik ki a sérülékenység mechanizmusaként [24].

TÁMADÁSOK JÖVŐKÉPE, JAVASLATOK

A kutatás eredményei egyértelműen rámutatnak arra, hogy a digitális alállomások – különösen az IEC 61850 kommunikációs és védelmi architektúrára épülő rendszerek – működése alapvetően kiberfizikai természetű, amelyben a kommunikációs rétegek sérülékenysége közvetlenül hat a villamos berendezések fizikai működésére és ezáltal az energetikai ellátás folytonosságára. A GOOSE-, Sampled Values- és MMS-szinteken azonosított támadások bizonyítottan képesek olyan kaszkád folyamatokat elindítani, amelyek téves védelmi működést, indokolatlan megszakító-állapotváltozásokat, hálózati instabilitást és szélsőséges esetben regionális ellátáskimaradást okozhatnak. E sérülékenységek különösen kritikusak Magyarország és az Európai Unió létfontosságú energetikai infrastruktúrái szempontjából, ahol a digitális alállomások térnyerése gyors ütemben zajlik, miközben a rendszerek nagy része még nem rendelkezik teljes körű, szabványosított kiberbiztonsági védelemmel. A vizsgálat rámutatott arra is, hogy a jelenlegi védelem elsősorban a megbízhatóságra és rendelkezésre állásra koncentrál, miközben a kommunikációs integritás, hitelesítés, valamint a valós idejű adatfolyamok kiberfizikai sérülékenységei továbbra is alulértékelt kockázati tényezők. A hibaterjedési modellek egyértelműen bizonyítják, hogy már kismértékű, célzott manipuláció is elegendő ahhoz, hogy a védelmi logika téves döntést hozzon, ezért a védelem funkcionális biztonsága a jövőben nem választható el a kiberbiztonsági kontrolloktól.

A kutatás alapján a következő főbb javaslatok fogalmazhatók meg:

- *Integrált kiberfizikai biztonsági architektúra kialakítása:* Az alállomások védelmi és irányítási rendszerét úgy szükséges továbbfejleszteni, hogy a kiber- és fizikai védelem ne különálló rétegekként, hanem egységes, egymást kiegészítő rendszerként működjön. A kommunikációs integritás, hitelesítés és időszinkron-védelem beépítése kiemelt prioritás.
- *Rendszerszintű monitoring és anomália-detektálás:* A digitális alállomások kiberfizikai jellegéből adódóan a támadások gyakran a fizikai rétegben mutatkoznak meg. Ezért olyan monitoring-rendszerek szükségesek, amelyek összevetik a kommunikációs réteg (GOOSE/SV/MMS) és a fizikai réteg (áram, feszültség, teljesítmény) viselkedését, és képesek az összefüggéstelen mintázatok korai felismerésére.
- *Szimulációs és HIL-alapú tesztelési infrastruktúra kiépítése:* A digitális alállomások biztonsági értékelése nem végezhető csupán elméleti alapon. A valós idejű HIL- és RTDS-szimulációk lehetővé teszik a kiberfizikai támadásszenáriók és azok fizikai hatásainak hiteles vizsgálatát, amely alapfeltétele a reziliens védelem kialakításának.
- *Kritikus infrastruktúra-specifikus kockázatkezelési keretrendszer alkalmazása:* A digitális alállomások kockázatait a NIS2, a nemzeti kritikus infrastruktúra törvény és az ENISA ajánlások alapján szükséges értékelni. A sérülékenységi profilok és

kaszkád-hatásláncok alapján a védelemnek a legkritikusabb támadási vektorokra kell koncentrálnia.

ÖSSZEGZÉS

A kutatás átfogóan vizsgálta a digitális alállomások kiberfizikai biztonságát és megvalósíthatóságát a kritikus infrastruktúrák védelmének szemszögéből. A digitális alállomások elterjedésével az energetikai rendszer egy olyan, korábban nem létező kitettségi formával szembesül, ahol a primer berendezések működése és a kommunikációs rétegek integritása közötti kapcsolat közvetlenné vált. Ennek következtében a villamosenergia-rendszer működése ma már nagymértékben függ a GOOSE-, Sampled Values- (SV) és MMS-protokollokra épülő digitális vezérlési és védelmi folyamatoktól. A kutatás egyik legfontosabb megállapítása, hogy e protokollok sérülékenységei – különösen az adatintegritás, időderminált ság és hitelesítés hiányosságai – olyan kiberfizikai támadási felületet hoznak létre, amely közvetlen fizikai következményekkel járhat.

A kritikus infrastruktúra szemszögéből a kutatás rámutatott arra, hogy a digitális alállomások biztonsága ma már elválaszthatatlan az energetikai ellátás folytonosságától. Az európai NIS2 irányelv, valamint a magyar 2012. évi CLXVI. törvény és kapcsolódó szabályozások egyértelművé teszik, hogy a digitális alállomások a nemzeti létfontosságú rendszerelemek részei, így védelmük nemcsak műszaki, hanem stratégiai követelmény is. A kutatás eredményei szerint a legnagyobb kitettséget a kommunikációs integritás hiánya, az időszinkronizáció sérülékenysége, a konfigurációs állományok hitelesítésének hiánya és a valós idejű adatfolyamok manipulálhatósága jelenti.

A vizsgálatok feltárták, hogy az SV-üzenetek kismértékű manipulációja is jelentős hatással van a védelmi algoritmusokra. A hibás fázorbecslésből eredő hamis GOOSE-üzenetek tovább erősítik a kaszkádszerű sérülékenységet: egyetlen rosszindulatú vagy manipulált parancs több mezőszinti megszakító koordinált működését válthatja ki, amely teljesítményátrendeződést, üzemzavart és – szélsőséges esetben – regionális ellátáskimaradást okozhat. A kutatás kimutatta továbbá, hogy az MMS-alapú támadások stratégiai kockázatot jelentenek, mivel az állomásszintű irányítás és konfiguráció sérülékenységei lehetővé teszik a támadók számára a védelmi beállítások átírását, a védelmi topológia átstrukturálását vagy akár indokolatlan megszakító-vezérlések kiadását. Ezért a védelem kizárólag integrált megközelítéssel valósítható meg: a kommunikációs biztonság, a védelmi funkciók jóváhagyási mechanizmusai, az időszinkronizáció és a fizikai eszközök megbízhatósága együttesen határozzák meg az alállomás ellenálló képességét.

A jelenlegi technológiai érettség mellett egyértelmű, hogy a jövőben a védelmi architektúrák fejlesztése, a szabványokon alapuló biztonsági mechanizmusok beépítése, valamint a rendszerszintű monitoring és detektálás alkalmazása válik kulcsfontosságúvá. A digitális alállomások nem pusztán modernizációs lépést jelentenek az energetikai szektorban, hanem olyan komplex kiberfizikai rendszerek, amelyek biztonsága meghatározza az ellátásbiztonságot, a hálózati stabilitást és végső soron a nemzeti energiarendszer reziliencáját.

FELHASZNÁLT IRODALOM

[1] International Energy Agency (IEA), Digitalization and Energy 2024 Report, 2024. [Online]: https://www.iea.org/reports/digitalisation-and-energy

[2] IEC 61850-1, Communication Networks and Systems for Power Utility Automation – Part 1: Introduction and Overview, International Electrotechnical Commission, Geneva, 2013. [Online]: https://webstore.iec.ch/publication/6028

[3] European Union, Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union, Official Journal of the European Union, 2022. [Online]: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[4] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, Magyar Közlöny, 2012. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1200166.TV

[5] SEL, "Digital Substation or Digital Secondary Systems — What's the difference?," Schweitzer Engineering Laboratories, 2024. [Online]: https://selinc.com/solutions/p/digital-substation/

[6] Hitachi Energy, "Digital Substations Overview," 2024. [Online]: https://www.hitachienergy.com/us/en/products-and-solutions/digitalization/digital-substation

[7] NEMA, Expanding the Adoption of IEC 61850, National Electrical Manufacturers Association, White Paper, 2021. [Online]: https://www.nema.org/docs/default-source/distribution-automation-toolkit-library/expanding-the-adoption-of-iec-61850.pdf

[8] G. Pázmándi, Kritikus infrastruktúrák védelme Magyarországon, Nemzeti Közszolgálati Egyetem, Budapest, 2021.

[9] I. Kolosok and E. Korkina, "Problems of Cyber Security of Digital Substations," IWCI 2019 Proceedings, pp. 75–78

[10] ENISA, Cybersecurity and Resilience of Smart Grids, European Union Agency for Cybersecurity, 2022. [Online]: https://www.enisa.europa.eu/news/enisa-news/smart-grids-cyber-security-measures-a-risk-based-approach-is-key-to-secure-implementation [Letöltve: 02-Nov-2025]

[11] Magyarország Országgyűlése, 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, 2012. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1200166.TV

[12] Magyarország Kormánya, 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények védelméről, 2013. [Online]: https://net.jogtar.hu/jogszabaly?docid=A1300065.KOR

[13] European Union, Directive (EU) 2022/2555 (NIS2) on Measures for a High Common Level of Cybersecurity Across the Union, Official Journal of the European Union, 2022. [Online]: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[14] European Union Agency for Cybersecurity (ENISA), Smart Grid Security: Recommendations for Europe and Member States, 2012; and ENISA, Cybersecurity and Resilience of Smart Grids, 2022. [Online]: https://www.enisa.europa.eu/publications/smart-grid-security-recommendations

[15] Schweitzer Engineering Laboratories (SEL), Digital Substation Solutions, 2024. [Online]: https://selinc.com/solutions/p/digital-substation/

[16] COPA-DATA, Digital Substations – How IEC 61850 and zenon Help You to Future-Proof Substation Operation, White Paper, 2024. [Online]:

https://www.copadata.com/hubfs/Downloads/Brochures/Digital-Substations_A5_2024_EN.pdf
[17] J. C. Lozano, Digital Substations and IEC 61850: A Primer, University of California eScholarship, 2023. [Online]: https://escholarship.org/uc/item/5kp7n3cn
[18] IEEE Std 1588-2019, Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. [Online]: https://standards.ieee.org/standard/1588-2019.html
[19] A. Apostolov, "The Evolution of Sampled Values in IEC 61850 Process Bus Systems," PAC World Magazine, 2021. [Online]: https://www.pacw.org
[20] M. Chen, X. Jiang, "False Data Injection on IEC 61850-9-2 Process Bus: Attack Feasibility and Impacts," IEEE Transactions on Smart Grid, vol. 12, no. 4, 2021. [Online]: https://ieeexplore.ieee.org/document/9354472
[21] IEC 62351-6, Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 6: Security for IEC 61850, 2020. [Online]: https://webstore.iec.ch/publication/31669
[22] IEC 61850-8-1, Communication Networks and Systems for Power Utility Automation – Part 8-1: Specific Communication Service Mapping – MMS Mapping, IEC, 2011.
[23] G. P. Chatzivasileiadis et al., "A Probabilistic Wide-Area Approach to Supply Restoration Following Extreme Events in Transmission Grids," IEEE Trans. Power Systems, vol. 34, no. 4, pp. 3461–3470, 2019.
[24] ENTSO-E, System Defence and Restoration (SDR) Report 2023. [Online]: https://www.entsoe.eu/publications/system-defence-and-restoration-sdr-report/
[25] 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
[26] BEREK L.–BEREK T.–BEREK L., Személy-és vagyonbiztonság. Óbudai Egyetem, 2016. [Online] http://nbn.urn.hu/N2L?urn:nbn:hu-6315

DOI: https://doi.org/10.12700/btsz.2025.7.4.41

INTELLIGENT VENTILATION STRATEGIES IN HOME AUTOMATION SYSTEMS

INTELLIGENS SZELLŐZTETÉSI STRATÉGIÁK A DOMOTIKA RENDSZERBEN

MÁRKOS Szilárd Attila[1]

Abstract

The development of home automation and intelligent building management has created new opportunities for automating ventilation, optimizing energy consumption, and harmonizing comfort and health considerations. The aim of this study is to provide a comprehensive and systematic perspective on the architectural structure of various ventilation technologies, from the technical characteristics of basic components to the development of complex demand-based ventilation strategies. Special focus is given to the measurement and derivation of occupancy levels, which is the most critical input parameter for control. The study describes predictive, artificial intelligence-based control, which is one of the most effective ventilation strategies based on system forecasts. The parameters that determine air quality (CO_2, relative humidity, PM, VOC) and their health and physiological risks are described in detail.

Keywords

Mechanical ventilation, predictive control, occupancy level, geo-fencing, air quality

Absztrakt

A domotika és az intelligens épületirányítás fejlődése új lehetőségeket teremtett a szellőztetés automatizálásában, az energiafelhasználás optimalizálásában, valamint a komfort és egészségügyi szempontok összehangolásában. A tanulmány célja, hogy átfogó és rendszerszintű perspektívát nyújtson a különböző szellőztetési technológiák architekturális felépítéséről, az elemi komponensek műszaki sajátosságaitól kezdve egészen a komplex igényalapú szellőztetési stratégiák kialakításáig. Kiemelt fókuszt kap a foglaltsági szint mérése, származtatása, ami a szabályozás legkritikusabb bemeneti paramétere. A tanulmány ismerteti a prediktív, mesterséges intelligencián alapuló szabályozást, amely a rendszer előrejelzéseire támaszkodó egyik leghatékonyabb szellőztetési stratégia. Részletes ismertetésre kerülnek a levegő minőségét meghatározó paraméterek (CO_2, a relatív páratartalom, PM, VOC) valamint azok egészségügyi és élettani kockázatai.

Kulcsszavak

Gépi szellőztetés, prediktív szabályozás, foglaltsági szint, geo-fencing, levegőminőség

[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

Életünk jelentős részét (60-90%) beltérben töltjük így a beltéri környezet minősége kiemelten fontos a mentális és a fizikális egészség megőrzése szempontjából. Számos terület hatással van a beltéri környezet minőségére, ilyenek például a beltéri levegő minőség, termikus komfort, akusztikai környezet, vizuális komfort, ergonómia, épületbiológiai tényezők és az okosotthon rendszerek. Ez a tanulmány a levegőminőségre és az azzal kapcsolatos rendszerek elemzésére korlátozódik. A beltér levegőminősége kiemelten fontos mivel közvetlenül hatással van az emberek egészségi állapotára és kognitív teljesítményére.

Az alacsony vagy zéró energiaigényű épületek iránti kereslet és a különböző építésügyi szabályozás megkövetelte az épületek filtrációs veszteségének minimaliázását. A légtömör épületek szellőztetése komoly kihívás elé állította az épületek üzemeltetőit. Ezen technológiai fejlődéssel jelentős energiamegtakarítás érhető el, különösen az alacsony energiaigényű épületek esetében, és egyúttal pontosabban szabályozható légcserét tesz lehetővé. Azonban a légtömör épületek megjelenése még jobban kiemeli a természetes szellőztetés korlátait, ezáltal a beltér levegő minőségére kedvezőtlenül hathat, elindulhatnának a penészedési folyamatok és felhalmozódhatnának a különböző szennyezőanyagok, amik egészségügyi kockázatot jelentenének. Ezért az ilyen épületek légcseréjét, mesterséges szellőztetési rendszerek kiépítésével és szabályozási stratégiák kidolgozásával kell megoldani. Az USA-ban és több európai országban (Belgiumban, Franciaországban, Spanyolországban, Lengyelországban, Svájcban, Dániában, Svédországban, Hollandiában és Németországban) az építésügyihatóságok különböző irányelveket dolgoztak ki a mesterséges szellőztetés szabályozásával és a hozzá tartozó energetikai megtakarítások számításával kapcsolatban. A központi szellőztető rendszerrel ellátott épületek esetén az energiafogyasztásának számításakor csökkentés alkalmazható a készülék besorolásától függően 15% illetve 35%. [12]

Az épületek energiafelhasználásra vonatkozó szabályozások rendkívül szigorúak Dániában, Észtországban, Norvégiában, Svájcban és Svédországban. A közel nulla energia igényű épületek építésügyiszabályozásánál, direkt módon nem térnek ki az eltérő szellőztetési megoldások alkalmazhatóságára, de egy ilyen alacsony energia felhasználású épület megvalósítása elképzelhetetlen igény alapú hőcserélős szellőztető rendszer üzemeltetése nélkül. [13]

A SZELLŐZTETÉS TECHNOLÓGIÁK ÖSSZEHASONLÍTÁSA

Az épületek szellőztetésének megvalósítása két jól elkülönülő csoportra osztható, az egyik az ablaknyitásos a másik a szellőztetőgépes. Az ablaknyitásos csoport tovább bontható a hagyományos kézi ablaknyitás és a szabályozás által időzített aktuátoros ablaknyitásos módszerre. A szellőztetőgépes csoporton belül megkülönböztetünk decentralizált (helyi) és centralizált (központi) szellőztetőgépes megoldásokat. [1][2]Az alábbiakban ezen technológiák műszaki sajátosságai kerülnek bemutatásra.

Kézi ablaknyitásos szellőztetés

A legrégibb formája a hagyományos (**kézi**) ablakokon keresztül történő szellőztetés, ilyenkor a légcsere jelentős része az ablak nyitások alkalmával valósul meg, bár jellemzően az ilyen szellőztetési technikát alkalmazó épületeknél nem elhanyagolható a légzárási problémákból adódó természetes filtráció[3].

- A módszer előnyei közé sorolható, hogy nincs szükség többlet beruházásra, üzemeltetésének sem költség, sem energia vonzata sincs.
- Hátrányok közé sorolható, az, hogy folyamatos odafigyelést igényel a felhasználók részéről, ami miatt a tervezett szellőztetések megvalósítása esetlegessé válhat, ebből adódóan jelentős kockázata van a penész kialakulásának. A légcsere szakaszos, ezért a beltér levegő minősége nagy szórást mutat. Mivel nincs hőcserélő, ezért a nem kívánt hőkülönbség tiszta fűtési/hűtési veszteségnek tekinthető. A légcsere során az épületbe jutó levegő kezeletlenül érkezik, így a por és pollen terheltsége a helyi adottságoktól függ. Nem kívánt huzat-hatás léphet fel a szellőztetések időtartama alatt.[4]

Aktuátoros ablaknyitásos szellőztetés

A kézi szellőztetés tovább fejlesztése a gépi ablaknyitásos módszer. Az ablakokat aktuátorok nyitják, melyeket időzítését, nyitási mértékét és nyitvatartási idejét egy központi vezérlő szabályozza. A módszer az alábbi eltéréseket mutatja a kézi ablaknyitásos szellőztetéshez képest.[5]

- A módszer előnye, hogy részben automatizált légcserével elkerülhető az alul vagy túlszellőztetés. A mennyiben a rendszer érzékelőkkel felszerelt, akkor a páracsúcsok kezelhetők ezzel a penészedési kockázat csökkenthető, és a CO_2 és a VOC koncentráció bizonyos keretek között kordában tartható. Független a felhasználók külső beavatkozásaitól, így az ütemezett légcsere minden estben megvalósul.[6]
- A módszer hátránya, hogy jelentős beruházási költsége van, mint például az ablak nyitó aktuátorok, különböző érzékelők, vezérlő, telepítési költségek mellett megjelennek az üzemeltetésének költségek is.[14]

Decentralizált gépi szellőztetés

A decentralizált rendszerben helységenként telepített berendezések működnek. A készülék a fali átvezetésben helyezkedik el, légcserét ezen keresztül végez. Jellemzően ellenáramú hőcserélővel rendelkeznek, az elszívás és a befúvás ideje megegyezik, ezalatt az átáramló levegő a hőmérsékletét egy kerámia hőcserélőnek adja át, ami ezt az ellenáramú működtetés során visszatáplálja a levegőbe.[14]

- A módszer előnye, hogy viszonylag alacsony beruházási költséggel kiépíthető, telepítése nem igényel jelentős átalakításokat, ami felújításoknál különösen előnyös. A berendezés része a vezérlés és a levegő minőség elemző szenzorok, így komplett légkezelő egységet kapunk. Hővisszanyerési hatásfoka magas 75-85%. Rendelkezik levegőszűréssel (osztálya F5-F7), így ezzel csökkenthető a beszívott levegő pollen és szállópor koncentrációja. **[15]**
- A módszer hátránya, hogy egyrészt a helyi ventilátor működéséből eredő, másrészt a kültérből beszűrődő zajterhelése viszonylag magas. A helységenként beépített egységek megfelelő működését könnyen felboríthatja az egymásra kifejtett hatásuk, vagyis, a kialakult légnyomás különbségek miatt egységenként számottevően eltérhet a beszívott és a kifújt levegő aránya, ami drasztikusan ronthatja a hőcserélési hatásfokot.[16]

Centralizált gépi szellőztetés

A rendszer egy központi légkezelő berendezésből, kiterjedt légcsatorna rendszerből, vezérlőből és levegőminőség szenzorokból áll. Általában egy zónás felépítésű, azonban motoros pillangószelepek beépítésével több zóna is kialakítható. Dedikált befúvási pontokat a száraz helységekben helyezik el, mint például a nappali vagy a hálószobák, az elszívási pontokat a nedves helységekben, konyha, fürdőszoba és a wc-ben alakítják ki. A légcsatorna rendszer tervezésekor kiemelt jelentőséggel bír a végpontok helységeken belüli elhelyezése. Csak abban az esetben biztosítható a beltér levegőjének teljes átöblítése, ha a légáramlás az egész helységen áthalad.

- A módszer előnye, hogy biztosítható a teljes légcsere, tartható a konstans, egészséges levegő összetétel. Hővisszanyerési hatásfoka rendkívül magas 80-90% entalpiás hőcserélővel. Szűrési teljesítménye rendkívül magas (F9 vagy HEPA). [17]Könnyen integrálható összetett domotika rendszerekbe. Zajterhelése alacsony, ami egyrészt abból ered, hogy a ventilátor egy távolabbi átmeneti tartózkodásra kijelölt helységben üzemel, másrészt a megfelelően méretezett légtechnikai hangcsillapító beépítése tovább csökkenti a ventilátor zajának terjedését.
- A módszer hátránya, hogy kifejezetten költségigényes, a légcsatorna hálózat helyigénye miatt, kiépítése a legtöbb esetben csak új építésű épületek esetén valósítható meg.[18]

INTELLIGENS SZELLŐZTETÉSI TECHNOLÓGIÁK

Az intelligens szellőztetés célja a beltéri levegőminőség folyamatos biztosítása a lehető legalacsonyabb energia-felhasználás mellett. A korszerű rendszerek a valós idejű környezeti és használati adatokra alapozott automatizált vezérléssel működnek, amely az optimális légcsere, hőkomfort és energiahatékonyság együttes megvalósítását támogatja. Ezen technológiák szerepe az épületenergetikai követelmények szigorodásával, valamint a légtömörebb épületszerkezetek terjedésével párhuzamosan egyre inkább felértékelődik.

Beltéri terhelés és szennyezőanyag-koncentráció

A szenzor vezérelt rendszerek mérésből, vezérlésből és visszacsatolásból állnak. A beltér levegőminőségét számos levegőminőségszenzor figyeli és a vezérlő a beérkezett adatok kiértékelése után az előzetesen beállított forgatókönyvet követi. A beltéri levegőminőséget befolyásoló tényezők a kémiai komponensek (pl. CO_2, VOC) a páratartalom, valamint a szálló por tartalom (PM2.5, PM10). Ahhoz, hogy kontextusba lehessen helyezni a különböző levegőminőségre befolyásoló komponensek jelentőségét, az alábbiakban ezeket és a megemelkedett jelenlétükből eredő egészségügyi kockázatokat ismertetem.

CO_2

A légkör CO_2-szintje jellemzően 400 ppm körül alakul. Jelenleg ezt tekintjük referenciának a beltéri levegő minőség kiértékelése során. Ez az érték elsősorban a fosszilis tüzelőanyagok égetése miatt folyamatosan emelkedik. Az ipari forradalom előtt a légkör CO_2-szintje 280 ppm volt

A rosszul szellőztetett, nagy kihasználtságú terekben ez az érték 800-1000 ppm körül alakul. 1000 ppm koncentráció felett több tanulmány kimutatható negatív hatásokról számol be, így ez az érték tekinthető a kockázati küszöb határértékének.[7]

A megemelkedett CO_2-szint hatással van a következő képeségekre/folyamatokra.:

- Kognitív teljesítmény és döntéshozatal: Lawrence Berkeley National Laboratory kutatói kimutatták, hogy 1000 ppm CO_2-szintnél a döntéshozatali teljesítmény több mérőskálán is szignifikánsan csökkent, és 2500 ppm körül drasztikusabb romlás jelentkezett. [8] Nicola Davis cikkében rámutatott arra, hogy 1400 ppm-nél egy csoportban az intelligencia- és problémamegoldási feladatok eredménye 50 %-kal rosszabb lett 550 ppm-hez viszonyítva. Tehát ha a CO_2-szint kis mértékkel meghaladja a kockázati küszöb értéket, akkor a kognitív képességeink drasztikusan csökkennek.[7]
- Komfortérzet, alvás: Wang és társai tanulmányukban azt vizsgálták, hogy különböző (680 ppm, 920 ppm és 1350 ppm) CO_2 koncentráció hogyan befolyásolja az alvásminőséget és a közérzetet. A kísérletben 10 ember vett részt és az eredmények azt mutatják, hogy a CO_2-koncentráció szintjének növekedésével az alanyok alvási nyugalma és elégedettsége fokozatosan csökkent.[9]
- Egészségügyi kockázat, fizikai tünetek: Rosszul szellőztetett helységekben a 100 ppm-enkénti CO_2-emelkedés +1.2–1.5-szeres eséllyel társulhat felső légúti irritációval például orr, torok vagy szemirritációval.[10] A CO_2 nagyobb koncentrációban megnövelheti a légzési frekvenciát, értágulatot válthat ki az agyi erekben.[11]

Relatív páratartalom

A relatív páratartalom hatással van az emberi komfortra az épületfizikai folyamatokra és a levegőminőségre.[19][20] A páratartalom befolyásolja a hőérzetünket a levegőben lévő kórokozók életképességét és penészesedési folyamatok kockázatát.[21] Emiatt a szellőztetési stratégiákban kiemelt figyelmet igényel.

Optimálisnak tekinthető páratartalom 40-60% között van, ez az tartomány biztosítja a nyálkahártyák megfelelő működését a hőérzet stabilitását és a kórokozók szaporodásának minimalizálását. Az ettől való eltérés pozitív vagy negatív irányba az alábbi problémákat veti fel.:

- Alacsony relatív páratartalom <40%: Szem és bőr irritáció jelenhet meg, növekszik a légúti kiszáradás kockázata, ami megkönnyíti a fertőzések terjedését. A hőérzet lecsökken, hidegebbnek érezzük a környezetünket a valós hőmérséklettől. Gyakoribb az elektrosztatikus feltöltődés. Az épületekben található természetes anyagok, mint például a fa érzékenyek az alacsony páratartamra, vetemednek az egyenetlen száradás miatt és repedések jelenhetnek meg rajtuk. [20]
- Magas relatív páratartalom >60%: Megemelkedik a penészgombák szaporodása különösen a 70%-os páratartalmat meghaladó környezetben. Továbbá allergiás és asztmatikus tünetek súlyosbodásához vezethet, és a diffúziós folyamatok révén az épületszerkezetbe jutva rontja a szerkezet hőszigetelő képességét.[21]

VOC (illékony szerves vegyületek)

Az illékony szerves vegyületek (VOC) a beltéri levegőminőség egyik legösszetettebb szennyezőanyag-csoportját alkotják. [22] Olyan anyagokról van szó, amelyek alacsony forráspontjuk következtében a szokásos beltéri hőmérsékleten is könnyen elpárolognak, így gázfázisban kerülnek a légkörbe.[23] A VOC-k esetében nem csak a közvetlen szennyezéssel kell számolni, hanem közvetett módon kémiai reakciók révén veszélyt jelenthetnek. A

főbb VOC források a következők: építőipari anyagok, bútorok, háztartási szerek, főzési folyamatok, dohányzás, emberi jelenlét anyagcsere, elektronikai eszközök.[24] Legveszélyesebb komponensek a formaldehid benzol, toluol, xilolok triklóretilén és egyéb oldószerek ftalátok és égésgátlók származékai.[22]

PM2.5 / PM10 µm részecskék

A kis méretű részecskék vagy a direkt szellőztetés alkalmával, vagy a beltéri forrásokból kerülnek a levegőbe. [25]Ilyen forrás például a főzés, dohányzás, gyertya vagy kandalló használat. A levegőben ezek a részecskék mindig jelen vannak, csak a koncentráció a kérdés. Különböző irányelveket dolgoztak ki a szervezetek, mint például a WHO (World Health Organization), USA – EPA (Environmental Protection Agency) vagy az Európai Unió (EU). [26]A szervezetek megkülönböztetnek 24órás átlagot és éves átlagot. A továbbiakban a földrajzi elhelyezkedés miatt csak a EU szabályozásával foglalkozom. Érdekes, hogy a EU szabályozása szerint a PM2.5 éves átlagának határértéke 25 µm/m^3, ami 5 -szöröse a WHO és 2- szerese a USA-EPA által elfogadott határértékeknek. A 24 órás átlag veszélyességi határérték értelemszerűen magasabb érték, hozzávetőlegesen 3 -szorosa az éves átlagnak.

Egészségügyi hatások: A PM 2.5 µm-nél kisebb részecskék jelenléte jelentősebb egészségügyi kockázatot jelent, mint a PM 10 µm méretű részecskék, mivel a tüdő mélyebb részeibe tudnak hatolni, így a természetes kiürülés csak részlegesen valósul meg és a folyamat sokkal több időbe kerül a szervezetnek. Egészségügyi kockázatok közé tartoznak a különböző irritációk (nyálkahártya, szem), asztma és allergiás reakciók erősödése és krónikus légzőszervi betegségek is előfordulhatnak (hörghurut, tüdőfunkciók csökkenése) [27]

A gépi szellőztetés során a kültéri szennyezők beltérbe jutása minimalizálható, a megfelelő HEPA szűrő alkalmazása mellett, a beltéri szennyezők esetében, kerülendő a dohányzás, nyílt láng használata és a főzésnél célszerű mindig konyhai elszívót használni.

FOGLALTSÁGI SZINT

Jelenlét érzékelés

Az igény alapú szellőztetés egyik kulcs tényezője a foglaltsági szint, amely meghatározza az épületen belüli személyek számát, térbeli elhelyezkedésüket és jelenlétük időbeli eloszlását.[28] Ez azért kiemelten fontos, mert a legtöbb nem kívánatos anyag felhalmozódása az emberi jelenléttel köthető össze. Ilyen például a légzési folyamatok terméke a CO_2 a különböző kozmetikumok/takarítószerek használat során kipárolgó VOC és főzéssel, fürdéssel, mosással, lélegzéssel a levegőbe juttatott páratartalom és a főzés során felszabaduló PM2.5/10.[29]

Az igény alapú szellőztetés célja, hogy úgy szabályozza a légcserét, hogy ezzel a helység levegőjének különböző összetevőinek arányát az egészségügyi határértéken belül tartsa, a lehető legkevesebb energia felhasználásával.[30]

A foglaltsági adatok a rendszer bemeneti paramétereit képezik, amelyek alapján akár zónánként szabályozni képes a légcserét.

A jelenlét érzékelés adatai a következő szenzorokból érkezhetnek.:

- Passzív infravörös érzékelő: Ezek az eszközök az emberi test által kibocsátott infravörös sugárzás változását képesek észlelni, így statikus jelenlétet nem képes érzékelni. A technológia előnye, hogy ezek az eszközök rendkívül költséghatékonyak.[31]
- Radaralapú érzékelők: A radar érzékelők Doppler eltolódást mérnek a visszaverődő mikrohullámokban, ezzel lehetővé válik a mozdulatlan személyek jelenlétének érzékelése. A szenzorok képesek mikrórezgéseket detektálni, mint például amilyet a légzés okoz és ebből megbízhatóbban következtet az emberi jelenléte.[32][33]
- Ultrahangos kombinált érzékelők: Ezek a szenzorok az emberi fül számára nem érzékelhető tartományba eső hanghullámokat bocsátanak ki és különböző tárgyakról érkező visszaverődő jelekből következtetnek az emberi jelenlétre. A megbízhatóbb azonosítás érdekében PIR érzékelőkkel kombinálják.[34]
- Kamerás rendszerek: Az anonimizált képfeldolgozáson alapuló kamerás rendszerek képesek valós idejű személyszámlálásra. Két féle anonimizálási technikát alkalmaznak. Az egyiknél mesterséges intelligencia dolgozza fel a képi felvételeket, miközben személyazonosságot nem rögzíti. Az AI az esetek túlnyomó részében felhőalapú szolgáltatás alatt üzemel, ezért biztonsági kockázatot jelent, hogy szenzitív információk szivárognak ki. [35] A másik módszer, ami fizikailag szabotázs védett az, hogy olyan alacsony felbontású érzékelőket alkalmazunk, ami nem teszi lehetővé az érzékelt személyek azonosítását. Egy ilyen szenzort dolgozott ki a Panasonic, Grid-EYE elnevezéssel, ami egy 8x8-as raszterű pontmátrix (64 pixel) hőérzékelő, ami az emberi alakokról csak egy elmosódott hőtérképet állít elő. Ezzel a szenzorral nem csak a jelenlét állapítható meg, hanem a mozgás közbeni haladási irány, vagy egy karlendítés, amihez megfelelően kialakított okosotthon rendszerben egy tetszőlegesen kiválasztott folyamatot indíthat el (Tipikus példa a világítás vezérlés, de bármilyen folyamatot indíthat, amit a rendszer kezelni képes.).

INDIREKT FOGLALTSÁG MÉRÉS

Szenzor-alapú indirekt foglaltság mérés

CO_2-vezérelt rendszerek

A CO_2-vezérlés az egyik legelterjedtebb mód a beltéri szellőztetés optimalizálására, a humán jelenlét indikátorának tekintik.[28] Számos egyéb tényező befolyásolja az optimális szellőztetési volument a korábban említett szennyezőkön felül, ilyen például az OLF („1 OLF = az a szagmennyiség, amelyet egy „standard ember" bocsát ki, tiszta ruhában, 21 °C és 50% relatív páratartalom mellett, ülő helyzetben, irodai aktivitással.") Ez az érték fizikai munka esetén 2-3 OLF, de erős izzadás esetén akár 6 OLF is lehet. Az OLF egység a szagérzeti szennyezés érzékszervi megfelelője. Mivel a fizikai terhelés megnövekedésével a humán légcsere szám is növekszik, ezért a két érték erősen korrelál egymással. Ezen szerencsés összefüggésnek köszönhető, hogy ha a rendszer CO_2-vezérlést végez, akkor azzal egyidőben az emberi kibocsátásból adódó szagterhelés kellemetlenségét is kiküszöböli. Természetesen rendelkezésre állnak a megfelelő összefüggések, amelyek alapján kalkulálható az OLF érték alapján a szükséges légcsere szám, de a tényleges megvalósítás szempontjából több problémába ütközünk. Az egyik az OLF érték meghatározása egy előzetes foglaltsági

becslésen alapszik, ami nem veszi figyelembe az emberi különbségeket és tisztálkodási szokásokat, nem számol a valós jelenléttel és a koncentráció szenzorokkal nem mérhető. Mérésére van kidolgozott módszer, de az az emberi szagláson alapszik, ezért az adatok közvetlenül nem építhetők be jelfeldolgozó rendszerekbe.

A CO_2-vezérlés előnye, hogy valós időben reagál a tényleges emberi jelenlétre, így biztosítja az megfelelő mennyiségű friss levegőt anélkül, hogy a túlszellőztetés állna fenn. [36] Ezzel a vezérléssel egy megfelelően méretezett központi szellőztető berendezéssel a CO_2 szint 700 ppm alatt tartható, ami jóval az egészségügyi határérték alatt van.[29]

A CO_2- vezérlés legnagyobb hiányossága, hogy bár az emberi jelenlét és a párakibocsátás összefügésben áll, de nincs összefüggésben a VOC kipárolgással. A VOC kibocsátás időarányos, a hőmérséklet emelkedéssel fokozódik. [39]Ezért, ha beltér kihasználtsága alacsony és CO_2 koncentrációra szabályozunk akkor a VOC koncentráció meghaladhatja az egészségügyileg elfogadható határértéket.

VOC-vezérelt rendszerek

A VOC vezérlés a kémiai szennyeződések arányát figyeli, ezek lehetnek építőipari anyagok, bútorok, háztartási szerek, főzési folyamatok, dohányzás, emberi jelenlétből származó kibocsátás. [37]A VOC szint közvetlen indikátora az egészség károsító vegyületek túlzott felhalmozódásának.

A vezérlés előnye, hogy közvetlenül képes reagálni a kémiai szennyeződésekre, ami különösen olyan esetekben lehet hasznos, ha ezek feldúsulása nem hozható közvetlen összefüggésbe az emberi jelenléttel. Ilyen tipikus alkalmazás lehet a például a vegyi laborok, festő üzemek, legcseréjének szabályozása, de ide sorolható akár az új építésű lakásoknál megfigyelhető építőanyagokból származó fokozott kipárolgás eredményeként megjelenő magas VOC koncentráció.[38]

A rendszer korlátjai közé tartozik, hogy a VOC mérés a szennyezőanyagok változatossága miatt rendkívül bonyolult feladat, külön-külön kalibrálni kellen a szenzorokat anyag fajtánként, ami figyelembe véve azt, hogy több mint 200 féle szennyező létezik túlságosan nagy komplexitást jelent. Ezért el kell fogadnunk azt, hogy a mérési pontosság alacsony lesz. A másik hátránya a VOC szint szerinti vezérlésnek, hogy nem képes figyelembe venni az emberi jelenlétet ezért, ha az adott környezetben éppen alacsony a levegő szennyezettsége, akkor a CO_2 szint megemelkedik, mivel nem követi le a friss levegő igényt.[39]

PM-vezérelt rendszerek

A PM szint vezérlés a levegőben megtalálható PM2.5 és PM10 részecskék koncentrációja alapján hozza meg a szükséges beavatkozásokat. [40][41]Elsősorban olyan környezetekbe megfelelő, ahol a szálló por koncentráció kifejezetten magas, ilyen például, a dohányzásra kijelölt helység. Ebben az esetben, ha a CO_2 koncentrációra szabályoznánk, akkor a PM koncentráció bőven meghaladná az egészségügyi határértéket.

A rendszer előnye, hogy szálló por koncentráció jól mérhető mennyiség, így a vezérlés valós időben le tudja követni a szellőztetési igényeket.[42]

Alkalmazási korlátok közé sorolható, hogy nem képes figyelembe venni a CO_2 és a VOC koncentráció egészségügyi határértéket meghaladó koncentrációját.[42]

Relatív páratartalom-vezérelt rendszerek

A CO_2, VOC és a PM vezérlés egy előre beállított küszöbérték alatt tartja a szennyezők mértéket, ezzel szemben a páratartalom vezérlés esetében álltalában 40-60% -között tartja a levegő nedvesség tartalmát. 60% feletti páratartalom esetén légcserét hajt végre, vagy kondenzáció segítségével nedvességet von el a levegőbőt, vagyis szárítja. 40% alatti páratartalom esetében nedvesíti a levegőt. Télen amikor a kinti levegő hőmérséklete és ezáltal a nedvesség felvevőképessége alacsony, akkor központi szellőztető berendezések hagyományos hőcserélővel hajlamosak túlszárítani a beltéri levegőt, ez azonban elkerülhető az entalpiás hőcserélő használatával, ahol a léghőmérséklet cserével egyidőben a légnedvesség csere is megtörténik.[45]

A szabályozás előnye, hogy megakadályozza a légzőszervi irritációkat, szemszárazságot, csökkenti a penészgombák szaporodását, megóvja a porózus anyagok szerkezeti épségét, növeli a hőérzetet.[43][44]

Alkalmazásának hátrányai közé sorolható, hogy nem érzékeli a levegőminőség többi szennyezőjének feldúsulása.

Integrált megoldások

A tudományos és a gyakorlati tapasztalatok azt mutatják, hogy a leghatékonyabb beltéri levegőminőség rendszerek működése több paraméter együttes monitorozásán alapul.[46][47][48]

Csak egy ilyen rendszerrel érhető el az, hogy ha a használati mintáktól eltérő módon kihasznált terekben sem dúsul fel a levegőben egyik nem kívánt komponens sem.[49]

Geo-fencing

A geo-fencing olyan helyalapú vezérlési technológia, amely előre kijelölt zónákat monitoroz, és képes detektálni a zónába az emberi jelenlétet.[50] Ezt oly módon valósítja meg, hogy a mobilkészülékek helyzetinformációira támaszkodva képes megállapítani a zónába be és kilépést időbélyeggel ellátva, és ezek alapján az előzetesen meghatározott eseményeket indítja. Tipikus példa a fűtés, hűtés, szellőztetés, ami a felhasználó közeledésével aktiválódik és mire megérkezik, addigra az elvárt paramétereket produkálja a rendszer.[51] A technológia felhasználási köre egyre bővül, már az okos-zárak is használják a technológiát, bár ott nem a mobilkészülék helyzetadataira támaszkodik a helymeghatározásnál, hanem a bluetooth kapcsolódással indítja el az ajtó nyitást- zárást. Ez egy kis hatótávolságú technológia (néhány tíz méter) ami ezen célnak tökéletesen megfelelő. [52][55]

A technika elsődleges célja a felhasználói komfort megtartása melletti energia megtakarítás. Akát 10-20% energia megtakarítás érhető el az egyszerű direkt működésű jelenlét érzékelőkhöz képest. Ennek oka, hogy a rendszer csak akkor tartja az elvárt paramétereket amikor arra valóban szükség van, ezzel jobban leköveti a tényleges használati mintázatot.

Például a gépi szellőztetés esetében az emberi jelenléttől függetlenül a természetes kipárolgás hatására az egészségügyi határértéket meghaladó VOC szint koncentrációja elfogadható, abban az esetben, ha a felhasználó megérkezésnek pillanatában már az egészségügyi határértéken belül helyezkedik el. [53] Ennek megvalósításához az geo-fencing, mint vezérlési technológia alkalmazása elengedhetetlen.

Biztonsági és adatvédelmi kockázzatok csökkentésének érdekében a rendszer a beérkező helyzetadatokhoz nem konkrét személyt társít, hanem egy kódot, ami alapján külső

megfigyelőként a személyazonosság nem visszakövethető.[54] A helyadatokat nem továbbítja a felhőbe, hanem helyileg kezeli. Döntéseket a helyi vezérlőn hozza meg.

A geo-fencing egy rendkívül hatékony és jól integrálható igényalapú szellőztetési stratégia különösen a lakóépületek vonatkozásában. Egy munkahely esetében, ahol az érkezés és a távozás egy jól ütemezhető folyamat, ami pontosan leírja a foglaltsági szintet nincs valós hozadéka ennek a vezérlésnek, nem beszélve a magas számú felhasználó helyadatainak kezelési és felhasználási nehézségeiről. Minél sztochasztikusabb egy terület/zóna foglaltsága annál jelentősebb energetikai megtakarítások érhetők el geo-fancing alapú jelenlét érzékeléssel.

PREDIKTÍV SZABÁLYOZÁS

A prediktív szabályozás a korszerű épületautomatizálás egyik legfejleteb irányítási stratégiája, amely a rendszer jövőbeli előrejelzéseire alapul. Alkalmazása a mesterséges intelligencián alapuló gépi szellőztetés területén is kiemelten fontossá vált. Egyszerre képes a termikus komfort, energiahatékonyság és a beltéri levegőminőség optimalizálására.

A hagyományos, szenzor alapú visszacsatoláson alapuló szabályozással szemben nemcsak a jelenlegi állapotokra tud reagálni, hanem képes az AI különböző szenzor adatokból következtetéseket levonni és előre jelezni a jövőben történő paraméter változásokat. Ez lehetőséget biztosít arra, hogy az esemény bekövetkezése előtt felkészülhessen, és megelőző intézkedéseket hozzon. A prediktív szabályozás egy optimalizálási feladatra épít, amit minden szabályozási lépés során megold.

Dinamika-modell alapjául szolgáló épületgépészeti modell olyan rendszerleírás, amely fizikai vagy empirikusan megalapozott módon leírja a szellőztetési rendszer és az épület időben változó, dinamikus viselkedését. A modellezés történhet fizikai alapú megközelítéssel hő- és anyagáramok precíz leírásával, ahol az eredmények pontosságának érdekében figyelembe veszi az összes létező paramétert, mint például a szerkezeti rétegek hőkapacitását, légcsere térfogatáramát, szellőztető berendezés válaszidejét, beltéri levegő hőmérsékletét és összetételét. Előnye, hogy egy jól paraméterezett rendszer felépítése, logikája könnyen értelmezhető, és jól reprodukálható egy másik rendszer kialakításánál. Hátránya, hogy a részletes paraméterezés időigényes feladat, valamint az eredmények nemlinearitása miatt kezelése komplexitásokat képez.

Predikciós horizont azon időintervallum, amire a rendszer előrejelzéseket készít a várható állapotváltozásokról, a szellőztetéstechnikában ez jellemzően 0,5-3 órás időtartam.

A predikciós horizont hosszának meghatározásával orientáljuk a modellt, rövidebb horizont gyorsabb reakciót, hosszabb horizont fejlett optimalizációt eredményez. A szimuláció során használt bemeneti paramétere a belső hő és szennyezőanyag terhelés, illetve a külső klimatikus hatások ismerete, ez alapján építi fel a rendszer dinamikájának modelljét. A modellezés során kapott különböző kimenetek közül az energetikailag legkedvezőbb megoldást választja.

A rendszer figyelembe veszi az üzemi korlátokat, mint például a maximális ventilátor fordulatszám, ami esti órákban a komfort érdekében akár egy csökkentett érték is lehet. A rendszer aktívan szabályozza az egyes levegőösszetételi paramétereket. A hőcserélési vesztesség csökkentésének érdekében a szükséges légcsere jelentős részét a kisebb hőmérséklet különbségű órákra időzíti. A prediktív szabályozás a meteorológiai előrejelzési ada-

tok (kültéri hőmérséklet, páratartalom) felhasználásával, a mért levegőösszetételi paraméterek (CO_2, VOC, PM, relatív páratartalom) és a mért vagy származtatott foglaltsági minták alapján, figyelembe véve az épületfizikai modelleket (hőtárolás, filtráció) hozza meg és hajtja végre az optimalizálási folyamatot. [56] Az optimalizálási folyamatban a számos paraméter közül, jellemzően az energiafelhasználás csökkentése áll a középpontban, de lehet CO_2, VOC, PM és relatív páratartalom koncentrációra is szabályozni. Az energetikai optimalizáció során nagy jelentőséggel bír a központi szellőztető gépek bypass funkciója, melynek használatánál ahogy a megnevezés is leírja a hőcserélő megkerülésével a levegőszűrőn keresztül a légcsere során megvalósul a hőtranszport. Ezt akkor alkalmazzák amikor nyáron a kültéri levegő hőmérséklet az esti órákban lecsökken és ezzel a levegővel direkt módon tudják hűteni a belteret amivel energiát takarítanak meg.

Park tanulmányában nyolc gépi tanulási algoritmus segítségével vizsgálta a természetes szellőztetési-ráta (NVR) prediktív modelljeit, amelyek alkalmasak a mért beltéri és kültéri környezeti változók közötti nemlineáris kapcsolatok értelmezésére. Az összes algoritmus közül a mély neurális hálózat biztosította a legjobb predikciós teljesítményt az NVR esetében. A Shapley-féle additív magyarázat alapján megvizsgálták a prediktív modellek eredményeit leginkább befolyásoló tényezőket, a legtöbb gépi tanulás alapú megközelítés hasonló jellemzőkkel rendelkezett (nyomáskülönbség, kültéri hőmérséklet, szélsebesség, beltéri relatív páratartalom, napsugárzás, beltéri/kültéri relatív páratartalom különbsége és szélirány). Az összes jellemző közötti korrelációs elemzés során az NVR-rel leginkább pozitívan korreláló változók a szélsebesség, a kültéri hőmérséklet és a napsugárzás voltak, míg a nyomáskülönbség negatívan korrelált az NVR-rel. Ezenkívül a kültéri hőmérséklet és a napsugárzás szorosan összefüggött a szélsebesség változásával. A tanulmány eredményei javíthatják az NVR előrejelzési teljesítményét, és ez hozzájárulhat egy intelligens természetes szellőzési-rendszer fejlesztéséhez.[57]

ÖSSZEFOGLALÓ

A domotika és az intelligens épületirányítási rendszerek fejlődése új lehetőségeket teremt a szellőztetési rendszerek automatizálásában, és az energiafogyasztás és az egészség finom egyensúlyának megteremtésében. A tanulmány átfogó képet ad a különböző szellőztetési technológiákról, a legegyszerűbb kézi ablaknyitásos módszertől egészen az igényalapú és prediktív mesterséges intelligenciával támogatott komplex hő-visszanyeréses központi szellőztető rendszereken át. Kiemelt szerepet kapott a foglaltsági szint (direkt-indirekt) megállapítása és annak technikai és szabályozástechnikai ismertetése, hiszen a legtöbb beltéri szennyező megjelenése közvetlenül az emberi jelenléthez köthető. A tanulmány részletesen ismerteti a beltéri levegőminőséget meghatározó komponensek, és ezek egészségügyi és fiziológiai hatásait, kockázatait. A tanulmány bemutatja a geo-fencing azaz helyalapú foglaltság mérésben rejlő lehetőségeket és a prediktív szabályozási rendszert. A prediktív, mesterséges intelligencia alapú szabályozási rendszer a rendelkezésére álló kültéri és beltéri körülményeket leíró paraméterek alapján képes magas valószínűségű előrejelzést készíteni, amit az esemény bekövetkezése előtt a modelltérben több alternatív megoldással szimulál és a legkedvezőbb paraméterekkel rendelkezőt kiválasztva, elindítja a megelőző, felkészülő folyamatokat. Jelenleg ez a legfejlettebb szabályozási rendszer, amely jelentős energia megtakarítási potenciállal rendelkezik különösen a beltér hűtése, fűtése és szellőztetésének területén.

Összességében a tanulmány rámutat arra, hogy a szellőztetés korszerű megközelítése csak egy komplex domotika rendszerben működtethető energiatakarékos módon, miközben figyelembe veszi a beltéri levegő egészségességét és aktívan hozzájárul a felhasználók komfortjához.

FELHASZNÁLT IRODALOM

[1] ANSI/ASHRAE Standard 62.1-2022, *Ventilation and Acceptable Indoor Air Quality*. ASHRAE, 2022. [Online]. Available: https://www.ashrae.org/technical-resources/bookstore/standards-62-1-62-2

[2] ANSI/ASHRAE Standard 62.2-2025, *Ventilation and Acceptable Indoor Air Quality in Residential Buildings*. ASHRAE, 2025. [Online]. Available: https://www.ashrae.org/technical-resources/standards-and-guidelines/read-only-versions-of-ashrae-standards

[3] F. L. Rashid *et al.*, "Mechanical Ventilation Strategies in Buildings: A Comprehensive Review of Climate Management, Indoor Air Quality, and Energy Efficiency," *Buildings*, vol. 15, no. 14, p. 2579, Jul. 2025. doi: 10.3390/buildings15142579

[4] A. Sporr, G. Zucker, and R. Hofmann, "Automated HVAC Control Creation based on Building Information Modeling (BIM): Ventilation System," *IEEE Access*, 2019. doi: 10.1109/ACCESS.2019.2919262

[5] X. Zhang *et al.*, "Decentralized and Distributed Temperature Control via HVAC Systems in Energy Efficient Buildings," in *Proc. IEEE Global Conf. on Signal and Information Processing*, Arlington, VA, USA, Dec. 2016.

[6] S. Lindvall, "Comparison of centralized and decentralized ventilation in a multifamily building in Stockholm: An LCA-study," Master's thesis, KTH Royal Institute of Technology, Stockholm, 2018.

[7] https://www.theguardian.com/environment/2019/jul/08/indoor-carbon-dioxide-levels-could-be-a-health-hazard-scientists-warn?CMP=share_btn_url

[8] Usha Satish, Mark J. Mendell, Krishnamurthy Shekhar, Toshifumi Hotchi, Douglas Sullivan, Siegfried Streufert, and William J. Fisk 2012 Is CO2 an Indoor Pollutant? Direct Effects of Low-to-Moderate CO2 Concentrations on Human Decision-Making Performance Environmental Health Perspectives 120:12 CID: https://doi.org/10.1289/ehp.1104789

[9] Wang, R.; Li, W.; Gao, J.; Zhao, C.; Zhang, J.; Bie, Q.; Zhang, M.; Chen, X. The Influence of Bedroom CO_2 Concentration on Sleep Quality. *Buildings* **2023**, *13*, 2768. https://doi.org/10.3390/buildings13112768

[10] Mold Remediaiton in Schools and Commercial Buildings EPA 402-K-01-001, September 2008

[11] Özgür Küçükhüseyin 01/2021 The REHVA European HVAC Journal 54-59 URL REHVA Journal CO_2 monitoring and indoor air quality

[12] Gaëlle Guyot, Max Sherman, Iain Walker, Jordan D Clark. Residential smart ventilation: a review. [Research Report] LBNL-2001056, LAWRENCE BERKELEY NATIONAL LABORATORY. 2017. ffhal-01670527f

[13] Jarek Kurnitski 06/2019 The REHVA European HVAC Journal 8-12 URL REHVA Journal NZEB requirements in Nordic countries

[14] B. Gulai *et al.*, "Modelling of Innovative Energy-Efficient Decentralized Ventilation Systems to Reduce the Carbon Footprint," in *Proc. CEE 2025*, Lecture Notes in Civil Engineering, vol. 781, Springer, 2025.
[15] F. Tolvaly-Roșca, A.-Z. Fekete, and Z. Forgó, "Investigation of the Real Efficiency of a Decentralized Heat Recovery Ventilation System," *Műszaki Tudományos Közlemények*, vol. 20, pp. 78–82, 2024. doi: 10.33894/mtk-2024.20.15
[16] S. K. Chowdary, "Evaluation of Decentralized Ventilation System with Heat Recovery," Master's thesis, Lund University, Sweden, 2020.
[17] J. Zemitis and A. Borodinecs, "Energy Saving Potential of Ventilation Systems with Exhaust Air Heat Recovery," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 660, p. 012019, 2019. doi: 10.1088/1757-899X/660/1/012019.
[18] M. Kremer, K. Rewitz, and D. Müller, "Introducing an Optimization Approach for Enthalpy Exchangers for Residential Ventilation," *International Journal of Ventilation*, vol. 24, no. 1, pp. 17–33, 2025. doi: 10.1080/14733315.2024.2380626.
[19] K. Rewitz, P. Seiwert, and D. Müller, "Influence of humidity on humans and their health," RWTH-EBC White Paper 2024-008, Aachen, 2024. doi: 10.18154/RWTH-2024-08075.
[20] D. Amaripadath *et al.*, "A systematic review on role of humidity as an indoor thermal comfort parameter in humid climates," *Journal of Building Engineering*, vol. 68, p. 106039, 2023. doi: 10.1016/j.jobe.2023.106039.
[21] E. R. Jones *et al.*, "Indoor humidity levels and associations with reported symptoms in office buildings," *Indoor Air*, vol. 32, no. 1, e12961, 2022. doi: 10.1111/ina.12961.
[22] T. Horvat, G. Pehnec, and I. Jakovljević, "Volatile Organic Compounds in Indoor Air: Sampling, Determination, Sources, Health Risk, and Regulatory Insights," *Toxics*, vol. 13, no. 5, p. 344, Apr. 2025. doi: 10.3390/toxics13050344.
[23] D. Kotzias, "Built environment and indoor air quality: The case of volatile organic compounds," *AIMS Environmental Science*, vol. 8, no. 2, pp. 135–147, Mar. 2021. doi: 10.3934/environsci.2021010.
[24] M. Piasecki *et al.*, "The Approach of Including TVOCs Concentration in the Indoor Environmental Quality Model (IEQ)—Case Studies of BREEAM Certified Office Buildings," *Sustainability*, vol. 10, no. 11, p. 3902, Oct. 2018. doi: 10.3390/su10113902
[25] WHO, *Global Air Quality Guidelines: Particulate Matter (PM2.5 and PM10), Ozone, Nitrogen Dioxide, Sulfur Dioxide and Carbon Monoxide*, Geneva: World Health Organization, 2021.
[26] European Commission, *EU Air Quality Standards*, Directive 2008/50/EC and updates, Brussels, 2024.
[27] W. R. W. Mahiyuddin *et al.*, "Cardiovascular and Respiratory Health Effects of Fine Particulate Matters (PM2.5): A Review," *Atmosphere*, vol. 14, no. 5, p. 856, May 2023. doi: 10.3390/atmos14050856.
[28] B. Chenari, S. Saadatian, and M. G. da Silva, "Experimental Assessment of Demand-Controlled Ventilation Strategies for Energy Efficiency and Indoor Air Quality in Office Spaces," *Air*, vol. 3, no. 2, p. 17, Jun. 2025. doi: 10.3390/air3020017.
[29] G. Rojas, "Assessing demand-controlled ventilation strategies based on one CO_2 sensor," *AIVC Proceedings*, 2022.

[30] S. Azimi and W. O'Brien, "Analysis of energy and cost savings potential of occupancy detection for commercial building operations," *IBPSA Proceedings*, 2022.
[31] Texas Instruments, "Occupancy Detection Using Passive Infrared-Based Technology," Application Note, 2023.
[32] M. Abedia and F. Jazizadeh, "Deep-learning for Occupancy Detection Using Doppler Radar and Infrared Thermal Array Sensors," *Proc. ISARC*, 2019.
[33] IEEE, "Doppler Radar Occupancy Sensing and Monitoring for Smart Buildings," *TELSIKS Conf.*, Oct. 2023. doi: 10.1109/TELSIKS.2023.10316022.
[34] I. Ciuffreda *et al.*, "A Multi-Sensor Fusion Approach Based on PIR and Ultrasonic Sensors Installed on a Robot to Localise People in Indoor Environments," *Sensors*, vol. 23, no. 15, p. 6963, Aug. 2023. doi: 10.3390/s23156963.
[35] H. Ochiai *et al.*, "Logic-Free Building Automation: Learning the Control of Room Facilities with Wall Switches and Ceiling Camera," *arXiv preprint*, Oct. 2024.
[36] Trane, "CO_2-Based Demand-Controlled Ventilation with ASHRAE Standard 62.1," Technical Report, 2024.
[37] M. Großklos, "Use of VOC sensors for air quality control of building ventilation systems," *J. Sens. Sens. Syst.*, vol. 4, pp. 159–168, 2015.
[38] J. Kolarik *et al.*, "Metal Oxide Semiconductor sensors to measure VOCs for ventilation control," AIVC Webinar Report, 2018.
[39] S. Li, "Review of Engineering Controls for Indoor Air Quality: A Systems Design Perspective," *Sustainability*, vol. 15, no. 19, p. 14232, Sep. 2023.
[40] J.-H. Kim *et al.*, "Ventilation and Filtration Control Strategy Considering PM2.5, IAQ, and System Energy," *Atmosphere*, vol. 11, no. 11, p. 1140, Oct. 2020.
[41] J. Vasquez Cubas *et al.*, "PM10 and PM2.5 Particulate Matter Monitoring Systems: A Systematic Review," *Proc. CSEI Conf.*, Springer LNNS, vol. 797, pp. 281–295, Dec. 2024.
[42] AESG, "Control of Particulates and Indoor Air Quality," Technical Report, 2023.
[43] D. Mallay, "Advanced HVAC Humidity Control for Hot-Humid Climates," NREL Report, 2024.
[44] ASHRAE, *Humidity Control Resources*, 2019.
[45] Condair, "Humidity Control Planning Guidelines," Technical Guide, 2024.
[46] H.-C. Zhu *et al.*, "Fast prediction for multi-parameters of indoor environment towards online HVAC control," *Building Simulation*, vol. 14, pp. 649–665, 2021.
[47] Y. Yang *et al.*, "Distributed Control of Multi-zone HVAC Systems Considering Indoor Air Quality," *IEEE Trans. Control Systems Technology*, 2020.
[48] C. Laughman *et al.*, "Integrated Control of Multi-Zone Buildings with Ventilation and VRF Systems," *Proc. IHPBC*, 2018.
[49] X. Zhu and H. Li, "HVAC Temperature and Humidity Control Optimization Based on Large Language Models," *Energies*, vol. 18, no. 7, p. 1813, Apr. 2025.
[50] L. Yu *et al.*, "Distributed Real-Time HVAC Control for Cost-Efficient Commercial Buildings Under Smart Grid Environment," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 545–556, Feb. 2018. doi: 10.1109/JIOT.2017.2768558.
[51] B. T. Smith-Cortez, "Demonstrations of Geo-Fencing Occupancy-Based Control in Smart and Connected Homes," M.S. thesis, Texas A&M Univ., 2023.
[52] US Patent US10516965B2, "HVAC Control Using Geofencing," Dec. 2019.

[53] T. Horvat *et al.*, "VOC Management in Smart Ventilation Systems," *Indoor Air Quality Journal*, vol. 15, no. 4, pp. 225–239, 2024.
[54] U. Matchi Aïvodji *et al.*, "IOTFLA: A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning," *IEEE Security and Privacy Workshops*, 2019.
[55] S. Kumbhar *et al.*, "B-Lock: A Smart Door Lock System Using Bluetooth Technology," *IJARSCT*, vol. 12, no. 11, pp. 1046–1055, 2025.
[56] M. Shin, S. Lee, J. Kim, and H. Park, "Development of an HVAC System Control Method Using Weather Forecasting Data with Deep Reinforcement Learning Algorithms," *Building and Environment*, vol. 111069, Nov. 2023. doi: 10.1016/j.buildenv.2023.111069.
[57] H. Park and D. Y. Park, "Comparative analysis on predictability of natural ventilation rate based on machine learning algorithms," *Building and Environment*, vol. 197, p. 107744, 2021. doi: 10.1016/j.buildenv.2021.107744.

DOI: https://doi.org/10.12700/btsz.2025.7.4.57

SAFETY CULTURE ELEMENTS IN LIGHT OF QUALITATIVE RESEARCH CONDUCTED WITH HUNGARIAN COMPANY EXECUTIVES

BIZTONSÁGI KULTÚRA ELEMEK VIZSGÁLATA MAGYAR VÁLLALATOK VEZETŐIVEL KÉSZÍTETT KVALITATÍV KUTATÁS TÜKRÉBEN

KERTAI-KISS Ildikó[1]

Abstract

Safety and security, as interpreted in the socio-technical system, are among the most important assets of adaptable organizations. This study presents the results of qualitative research conducted with Hungarian safety and security managers. The essence of the research is that, based on safety culture models, it is possible to identify the cultural elements specific to each company and their background, and, beyond that, to define new areas of research. In addition, this article highlights the effectiveness and legitimacy of qualitative research, which is a key issue because safety is an extremely sensitive area in the life of companies, especially when trust is declining at both the organizational and societal levels. My research is applied research, the main goal of which is the practical application of new knowledge.

Keywords

safety culture, qualitative methods, managerial perceptions, new research focuses

Absztrakt

A szocio-technikai rendszerben értelmezett biztonság (Safety) és védelem (Security) az adaptivitásra képes szervezetek egyik legfőbb vagyoneleme. Jelen tanulmány magyar biztonsági vezetőkkel készített kvalitatív kutatás eredményeit mutatja be. A kutatás lényege, hogy a kultúra modellekből kiindulva, beazonosíthatók az egyes vállalatokra speciálisan jellemző elemek és azok háttere, valamint új kutatási területek határozhatók meg. Mindezek mellett jelen cikk rámutat a kvalitatív vizsgáltok eredményességére és létjogosultságára, ami azért is kulcskérdés, mert a vállalatok életében a biztonság rendkívül szenzitív terület, különösen akkor, ha a bizalom mind szervezeti, mind társadalmi szinten hanyatlóban van. Kutatásom alkalmazott kutatás, amelynek fő célja az új ismeretek gyakorlati felhasználása.

Kulcsszavak

biztonsági kultúra, kvalitatív módszerek, vezetői percepciók, új kutatási fókuszok

[1] kertai.kiss.ildiko@gmail.com | ORCID: 0000-0002-0981-2385 | PhD candidate, PhD School of Safety and Security Sciences, Óbuda University | PhD jelölt, Biztonságtudományi Doktori Iskola, Óbudai Egyetem

BEVEZETÉS

A tanulmány egy hazai biztonsági kultúra kutatás kvalitatív szakaszának és eredményeinek összefoglalója, melynek célja, hogy rámutasson a professzionális biztonsági területen dolgozó vezetőkkel készített kvalitatív vizsgálatok szerepére a szervezeti biztonsági kultúra kapcsán. Kutató munkám két szakaszból állt: a kvantitatív vizsgálatokhoz egy 45 itemből álló elmélet alapú, saját szerkesztésű kérdőívet dolgoztam ki, amely a biztonsággal kapcsolatos attitűdöket, motivációkat, értékrendeket, valamint a kultúra modellekben [1] [2] [3] [4] [5] [6] [7] [8] megfogalmazott elemeket, tulajdonságokat tartalmazta. Mérőeszközöm a munkavállalók által észlelt szervezeti valóságra kérdezett rá, melynek eredményeire építettem a kutatás második, kvalitatív szakaszát. Strukturált, valamint mélyinterjúkat, tartalom elemzést és fókusz csoportos beszélgetést készítettem a szervezetek biztonsági vezetőivel, szakértőivel, valamint terepkutatást végeztem az egyes vállalatoknál. Hipotézisem az volt, hogy kvalitatív módszerekkel mélyebben határozhatók meg az adott szervezet speciális, egyedi biztonsági kultúra jellemzői, azok háttere / magyarázata, összefüggései és ezeken túlmutatva az eredmények új fókuszokat tárnak fel a javítás érdekében alkalmazható szakmai ajánlásokhoz és a jövőbeli kutatásokhoz. Emellett feltételeztem, hogy iparágtól és adott vállalati kultúrától függetlenül is létezik egy erős biztonsági szakmakultúra.

ELMÉLETI HÁTTÉR

A biztonsági kultúra negyedik szakasza

A biztonsági kultúra szakirodalom öt korszakot különböztet meg, melyeknek fókusz területei kronológiai sorrendben: 1., technológia, 2., magatartás és humán faktor, 3., szocio-technikai rendszer, *4., kultúra*, 5., reziliencia és adaptálódás. A negyedik korszak (1980-90-es évek) kutatásinak fő területe tehát a kulturális tényezők és a szervezeti biztonság kapcsolata. A biztonsági kultúra aktív szerepét a balesetek okozati összefüggéseinek vizsgálatában már régóta elismerik a HRO-k (nagykockázatú szervezetek). [9] [10] Az első biztonsági kultúra modellt is a Nemzetközi Atomenergia Ügynökség [11] alkotta meg, melynek központi fogalmai az elkötelezettség a szervezeti biztonságpolitika, a menedzsment és az egyéni attitűdök. A téma történeti ívéhez kapcsolódik, hogy amíg a biztonsági (safety) kultúra kutatását és fejlesztését első alkalommal az 1986-os Csernobili katasztrófa hívta életre, addig az önálló nukleáris védettségi (security) kultúra gondolata a 2001. szeptember 11-i eseményekben gyökerezik. [12]

A biztonsági kultúra iránti érdeklődés és kutatás a XXI. század kezdetével új lendületet kapott, a biztonság javítására irányuló stratégiák már nem csak az eddig meghatározott valamennyi szempontot veszik figyelembe (technológia, egyének és a két alrendszer közötti kölcsönhatás), hanem a szervezeti irányítás és a szervezetközi tényezőket is, illetve azoknak a rendszerek biztonságára gyakorolt hatását, valamint a biztonsági kultúrák fejlesztése, a biztonsági teljesítmény növelése prioritássá vált.

A negyedik korszak első szakaszában a nagy kockázatú szervezetek körében (nukleáris ipar, légi közlekedés és légiforgalmi irányítás, olaj- és gázipar, bányászat, egészségügy, vegyipar), tekintették a kultúrát fontos biztonsági hajtóerőnek, a „nagy megbízhatóság” elmélet [13] és a „kollektív éberség” (más szóval tudatos jelenlét) teória [14][15] mindinkább előtérbe került.

A korszak későbbi szakaszában, a szervezetek közötti (inter-organizational) megközelítés képviselői kiemelik, hogy a balesetek okai nem mindig korlátozódnak magára a vizsgált szervezetre. A nagy hatású ipari katasztrófák biztonsági elemzései azt mutatták, hogy a szervezeti folyamatok közötti működési zavarok is aktív szerepet játszanak a balesetek ok-okozati összefüggésében. Így például figyelmet kaptak a nukleáris biztonság-orientált szervezetek, a kormányok, szabályozó intézmények, közművek, az üzemi menedzsment, kutatóintézetek, gyártók, tanácsadó szervek és az atomerőmű személyzet közötti kapcsolatok, amiből azt a következtetést vonták le, hogy a rendszer tartós biztonságának érdekében gondoskodni kell a különböző szereplők közötti diszfunkcionális kapcsolatok korrigálásáról is. [16]

A negyedik korszakban felismerték azt is, hogy a szervezeti kultúrát nemcsak a tágabb társadalmi kultúra, hanem az iparági kultúra is befolyásolja, mert ugyanabban az iparágban működő vállalatok általában közös kulturális értékeket és gyakorlatokat alkalmaznak. Ezek arra késztetik a vállalatokat, hogy olyan stratégiákat, struktúrákat és folyamatokat dolgozzanak ki, amelyek összhangban vannak az adott ipari kultúrával, és nem "ellenségesek" velük szemben [17]. Másrészről az ipari szintű kultúrák közötti kapcsolat azért is erős, mert a szervezetek beágyazódtak az ágazataik intézményi rendszer hálózatába és ez meghatározza az értékeket, hiedelmeket, szabályokat, gyakorlatokat, elfogadott követelményeket. Ennek megfelelően a funkcionalista megközelítést alkalmazó szervezetek rendszeresen értékelik kultúrájukat kvantitatív munkavállalói attitűd, észlelési felmérések segítségével. Az adatokat a kulturális hiányosságok azonosítására használják fel és stratégiai beavatkozásokat dolgoznak ki, valamint hajtanak végre a kulturális fejlődés érdekében.

A fejlődés szakaszait összegezve a kutatások lényeges szempontja az is, hogy természetesen az egyes korszakokat meghatározó vegytiszta típusjellemzőkkel működő vállalat nem létezik. Általában többféle korszak jellemzőinek kombinációja határozza meg a szervezetek biztonsági kultúráját.

A biztonsági kultúra definíciója

A fentieket szem előtt tartva, jelen tudásom és kutatási eredményeim alapján, a következőképpen határozom meg a biztonság kultúrát, amelynek célja, hogy egyrészt tükrözze a kutatók által, az elmúlt harminc évben elért elméleti és gyakorlati eredményeket, másrészt, ezzel a definícióval szeretném ráirányítani a figyelmet azokra a fókuszpontokra, amelyek a jövő biztonságát befolyásolják globális, társadalmi, szervezeti és egyéni szinten.

A (szervezeti) biztonsági kultúra a biztonság tartós, nagy értékű prioritása, amely a szervezeti tagok által közösen vallott értékekbe, hiedelmekbe és normákba ágyazva, a tagok munkahelyi attitűdjében, felfogásában, gondolkodásában és viselkedésében, valamint a szervezeti politikákban, eljárásokban és gyakorlatokban nyilvánul meg. Elemeit tekintve egy olyan erős (konzisztens, konszenzusos, egyértelmű) és összetett szocio-technikai rendszer, amely képes hatékonyan támogatni a szervezet biztonsági teljesítményét a munkavállalók, a társadalom és a környezet védelmét a kockázatoktól, balesetektől, betegségektől és krízisektől.

Más szóval, rövidebben: *a biztonsági kultúra a szervezeti kultúra szerves része, olyan értékprioritásokon alapuló látható és nem látható elemek komplex rendszere, amely meghatározza, elősegíti és fenntartja a vállalat rendeltetésszerű működését veszélyeztető*

tényezők hiányát. A definícióban szereplő erős kultúra kifejezés magában foglalja a konzisztencia, konszenzus és egyértelműség fogalmát. Ez azt jelenti, hogy stabilitást teremtenek azáltal, hogy a struktúra, szervezeti folyamatok, vezetői szerepek, hatalmi viszonyok belső ellentmondásoktól menetesen működnek a szervezetben.

Tudományos megközelítések a biztonsági kultúra kutatásában

A biztonsági kultúra empirikus kutatása alkalmazott tudományterület, amely egy nagyobb tanulás-fejlesztés-javítás ciklus és ezek állandó monitorozása folyamat részének tekinthető. Az új kutatási területek megtalálásához és vizsgálatához indokolt a multidiszciplináris megközelítés és a különböző módszerek komplex alkalmazása. [18] [19]

A biztonsági kultúra funkcionalista vizsgálata

A funkcionalista megközelítés jellemzői, hogy (1) a biztonsági kultúrát közös viselkedési mintaként értelmezik [20], (2) meghatározó, hogy vezetői beavatkozással könnyen megváltoztatható, (3) alkalmas a felülről lefelé irányuló ellenőrzésre, valamint (4) felhasználható a szervezeti biztonsági stratégiák és rendszerek támogatására. [21] A funkcionalista megközelítés a biztonsági kultúrát "ideális állapotnak", más szóval egy erős és egységes kultúrának tekinti, amelyet a szervezeteknek el kell érni. Ezt a vezetők által kezdeményezett és kialakított egységes megközelítést a biztonsági kultúra iránti "integrációs" orientációként is jellemzik [22], amelyben feltételezhető, hogy egy ideális kultúrában a szervezet minden tagja közös elképzeléseket és meggyőződéseket alakít ki a biztonság kockázataival összefüggésben. [23] [24] A funkcionalista perspektíva tehát egy kultúrát (általában a vezetését) tekinti dominánsnak és kevésbé veszi figyelembe, hogy különböző biztonsági kultúrák, egyetlen szervezeten belül is létezhetnek. Módszertanilag a funkcionalista megközelítés *szociálpszichológiai alapokon* nyugszik, és a kvantitatív kutatási eszközöket részesíti előnyben (pl. kérdőíves észlelési és attitűdfelmérések). [25]

A biztonsági kultúra interpretatív vizsgálata *(Interpretive view of safety culture)*

Az interpretatív megközelítés lényege, hogy a biztonsági kultúra a szervezet (vagy csoport) tagjai által kifejlesztett hit, viselkedés és kollektív identitás értelmezésére használt közös jelentésminták összessége [26] [27] [28] Ennek megfelelően nincs egyetlen domináns kultúra, hanem az egyes csoportok, például különböző generációk vagy szakmai teamek stb., a biztonsági kultúrával összefüggő jelentéstartalmakat eltérően értelmezik és használják. Más szóval a differenciált kultúrákat különböző típusú szociális csoportosulások eredményének tekintik, elismerve, hogy egyetlen szervezeten belül több szubkultúra is létezhet, ami a biztonsági kultúra "differenciálódását" is jelenti [22] A biztonsági kultúra értelmező megközelítése a *szociológia és az antropológia* eszközeit alkalmazza és a kvalitatív módszereket részesíti előnyben. (pl. esettanulmány, mélyinterjú, megfigyelések, dokumentumelemzés).

Összességében a biztonsági kultúra vizsgálatának két fejlődési szakasza egymástól nagyon különböző szemléletmódot tükröz. Az első hullám (1990-2005) jellemzője az értelmező, funkcionalista szemlélet, a második hullámban (2005-2020) azonban az egyes tanulmányok azt mutatják, hogy a kutatások nagy utat jártak be, a biztonsági kultúra elutasításától, kritikájától, a nyitott gondolkodáson keresztül a biztonsági kultúra módszereinek, programjainak, modelljeinek előmozdításáig. Napjainkban a biztonsági kultúrát, mint eszközt kell fejleszteni a biztonság elősegítésére [29].

A következő táblázat a biztonsági kultúra vizsgálatának fejlődését foglalja össze:

Biztonsági kultúra tanulmányok, ellentmondások, álláspontok és viták

1. hullám, 1990–2005	**2. hullám, 2005–2020**	
Értelmező szemlélet és Funkcionalista szemlélet	**1. fázis:** a biztonsági kultúra elutasítása vagy kritikája	A biztonsági kultúra domináns megközelítését a menedzsment egyéni módon értelmezi. A vállalatoknál megfigyelhető, hogy a fogalmat nem kellően használják, ez a biztonsági kultúra elhagyásához kellene, hogy vezessen.
	2. fázis: semlegesebb, különállóbb tudományos érdeklődés a biztonsági kultúrával, mint tárggyal kapcsolatban	A biztonsági kultúrának sok, különböző nézőpontja létezik, ezek nem kizárólagosak és esettől függően még ki is egészítik egymást.
	3. fázis: bizonyos feltételek mellett nyitott gondolkodás a biztonsági kultúra gyakorlati értékéről	A biztonsági kultúra fontos koncepció, de mély megértése szükséges ahhoz, hogy hasznos is legyen, kombinálva például a hatalom fogalmával.
	4. fázis: a biztonsági kultúra módszereinek, programjainak, modelljeinek előmozdítása	A biztonsági kultúrát, mint eszközt kell fejleszteni a biztonság elősegítésére, például érettségi modellek segítségével.

1.táblázat: A biztonsági kultúra kutatásának fázisai és vizsgálatának perspektívái
Forrás: Le Cose, 2019 [29].

A felsoroltakon túl a biztonsági kultúra kutatások módszertani szakirodalmában speciális megközelítés Schein un. klinikai módszere [30]., mely azt szorgalmazza, hogy a kutatás és a változtatás céljait, módszereit össze kell kapcsolni. Ebben az esetben a vizsgálat célja már nem csupán a kultúra jellemzőinek meghatározása, hanem a jobbítása. Ez a szervezet résztvevőivel közösen történik [31] [32], oly módon, hogy az információk jelentős részét a bevont résztvevőktől önkéntesen gyűjtik össze a kutatók, akik kifejezetten a beavatkozás, változtatás, fejlesztés céljával végzik a kutatásaikat. E megközelítés másik gyökere az akciótanulás iskolájából ered [33], amely azzal érvel, hogy ameddig a szervezeti tagok nem érdekeltek közvetlenül a kutatás eredményében, addig nem számíthatunk tőlük hiteles és rendszeres információra és együttműködésre. Ezért a kutatás és szervezeti változás folyamatait össze kell hangolni.

Mindezek alapján biztonsági kultúra kutatásom komplex szemléletű megközelítés (kvantitatív, kvalitatív, interszubjektív) [34] [35] a szervezeti kultúra biztonság fókuszú vizsgálata, amelyet az alábbi táblázat foglal össze.

Kutatói alapállás (tudományfilozófia)	KLÍMA		KULTÚRA
	KVANTITATÍV objektivista-pozitivista	KVALITATÍV objektivista-pozitivista	INTERPRETATÍV kvalítatív módon alkalmazott szupervizor szemléletű, szubjektivista
Megközelítés	Étikus = a jelenség leírása és operacionalizálása elméleti változókkal történik (pl. bizonytalanságkerülés index).		Émikus = konkrét helyen és adott közösség fogalmi rendszerében vizsgálja a valóságot.
Szervezetelmélet természete	Releváns változókkal, minél érvényesebb magyarázat általános (univerzális) törvényszerűségekről, működési mechanizmusokról.		Releváns változók, szubjektív, konstruált valóság, fogalomrendszer alapján.
Cél	Magyarázó, funkcionalista.		Jelentés megértés által a szervezeti valóság mélyelemzése.
Kutatói szerep, fókusz	Objektív, független értékmentes.		● Független, de része a szervezetnek, ● figyelembe veszi a résztvevők nézőpontjait, ● „belekérdezés" technikája ● a belső, mögöttes, jelentésvilágot is kutatja ● miről szól a jelenség „itt és most"?, ● nem feltétlen, értékítéletmentes.
Speciális jellemző	Nem épít a felmérést végző személy, a szervezet és tagjainak kapcsolatára, interakcióira.		Az interakciók is a kutatás tárgya, interszubjektívitás, érzelmi együtthatók vizsgálata.
Szervezeti kultúra-felfogás	A kultúra az, amivel a szervezet rendelkezik.		Az, ami a szervezet maga (jelentésvilága).
Szervezet lényege	Szervezeti jellemzők, dimenziók, konstruktumok beazonosítása, mérése, elemzése.		A látható szervezeti jellemzők mögött a rejtett dimenziók, a dolgok másról szólnak, mint aminek látszanak.

Módszerek, eszközök	● (Kontrollált) kísérletek, ● kérdőív, ● természettudományos, ● statisztikai eljárások (SPSS), ● összevethető minták, ● standardizált.	● (Félig) strukturált interjú, ● tartalom elemzés, ● fókusz-csoport, ● dokumentum elemzés, ● trianguláció.	● Félig strukturált interjú, ● strukturálatlan mélyinterjú, ● résztvevő megfigyelés, ● fókusz-csoport és megértő elemzés, ● tárgyak, terek, szimbólumok elemzése, ● kognitív térképek alapján értelmezési tartományok, ● naplózás technikák, ● részvételi akciókutatás (RAK), ● Grounded Theory, ● trianguláció
Orientáció	Magyarázat, kategória rendszer feltárása.	Megértés, a feltárt kategória rendszer alapján a vizsgált szervezet illesztése, elhelyezése.	(Mély) megértés, (ön)reflektív, kritikus.
Vizsgálódás iránya (metafora)	● „Madártávlat”, ● kívülről, felülről-lefelé, több kultúra azonos szempontok szerinti összehasonlítása.	● „Lift”, ● felülről-lefelé és alulról-felfelé is építkezik.	● „Etnográfus”, ● antropológiai módszertanok, ● hermeneutikai (megértés, magyarázás, értelmezés tudománya), ● artisztikus jellemzők ● helyi, önálló, egyedi értelmezése, mélyelemzése, ● „itt és most” dimenzió
Valóság-észlelés	Determináns, az emberi cselekvésmintákat a cselekvők tudatától függetlenül létező struktúrák, törvényszerűségek határozzák meg.	Nem determináns, az emberi cselekvésmintákat a cselekvők tudatától nem függetlenül létező struktúrák, törvényszerűségek határozzák meg.	
Kutatási területek, példák	társadalmi, szervezeti kultúra		(szervezet) pszichológia

Meddig jut el?	● Szervezeti valóság általános magyarázata, ● „nagy elméletek" megalkotása, ● létező elméletek tesztelése.	● Szervezeti igazság „sűrű leírása", ● helyi kontextustól függő elemzések, ● olyan kérdésekre is választ adhat, amit a kutató, előzetesen nem tudott volna megfogalmazni, ● „(ön)reflektív" dialógus, tudatosítás.

2.táblázat: A primer kutatás módszertani összefoglaló táblázata (saját szerkesztés)

PRIMER KUTATÁS

A kutatásban résztvevő szervezetek

A biztonsági kultúra felméréssel kapcsolatban 41 Magyarországon működő szervezetet kerestem meg, (szektorok: biztonsági, védelmi, szolgáltatás, energia, közlekedés, IT, tanácsadó, kereskedelmi, infokommunikációs, gyógyszeripar, vegyipar). Kérdőíves adatfelvételt 8 vállalatnál készítettem, (biztonsági, védelmi, szolgáltatás, kereskedelem, közlekedés, energia szektor, nukleáris ipar). A kérdőívet összesen 301 munkavállaló töltötte ki, ebből 280 volt értékelhető. A megkérdezettek célzottan, szakértői mintavételi eljárás alapján vettek részt a kutatásban. Ezt követően a kvalitatív szakaszban három szervezet vezetői vállalták a részvételt.

A minta jellemzői

Az értékelhető kérdőívek (N=280) 70,4%-át nagyvállalatok munkavállalói (64,6% állami) 197-en töltötték ki, a többi résztvevő (83 munkavállaló) a KKV szektorban dolgozik, ebből 41,1% (N=113) vezető, 57,9% (N=162) nem vezetői feladatokat lát el. (Öt kérdőívben nem volt értékelhető az erre a kérdésre adott válasz.) A megkérdezett vállalatokra jellemző, hogy 85,4% magyar, 14,6% német tulajdonosi háttérrel rendelkezik. A kitöltők demográfiai megoszlása: legnagyobb arányban (63,8%) az X generáció, ezt követően csökkenő sorrendben 30,1% az y generáció, 5,1% baby boomer, 1,1% pedig Z generációhoz tartozik. A vizsgálatban részt vettek 91,1%-a a biztonság területén dolgozik, 8,9%-ban pedig a demográfiai kérdésre nem biztonsággal kapcsolatos szakmai területet jelöltek meg.

A kvalitatív kutatás

A kvalitatív vizsgálatok célja: (1) a biztonsági kultúra elemeinek vállalatspecifikus beazonosítása, a jelenségek hátterének, ok-okozati megértése, (2) a saját szerkesztésű kérdőív statisztikai eredmények értelmezése, elemzése helyi szinten, magyarázó jelleggel, (3) az összefüggések mélyítése, (4) új kutatási fókuszok megtalálása és (5) magának a kutatási módszernek az alkalmazhatósági vizsgálata volt. Ebben a fázisban a következő módszereket alkalmaztam:

- strukturált interjú,
- mélyinterjú (reflektív, interszubjektív, interpretatív megközelítés),
- tematikus kvalitatív tartalomanalízis, az interjúk szövegéből készült átiratok alapján [36].

A kutatás ezen szakaszában a kinyert eredményeket trianguláltam, amelynek célja a biztonsági kultúra elemeinek mélyebb vizsgálata, más nézőpontból való bemutatása, többrétegű értelmezése, az eredmények érvényességének bizonyítása. [37][38][39]. A triangulációalkalmazása túlmutat a különböző módszerek kombinálásán. Kutatásomban a triangulációhárom perspektívája: (1) a kvantitatív adatok, (2) a kvalitatív adatok és (3) a kutatói / vezetői megértés, értelmezés [40].

A résztvevő három vállalat szignifikancia vizsgálatai

A kérdőíves vizsgálatban résztvevő nyolc szervezet közül ebben a szakaszban 3 vállalat vett részt, három különböző ipari szektorból: (1) HRO/energia ipar, (2) hazai közlekedési ágazat, (3) multinacionális nagykereskedelem. Az első szervezet esetében fókuszcsoportos interjú és mélyinterjú formájában is történt adatfelvétel. A leíró statisztikák kapcsán szignifikancia vizsgálatot ezen három szervezet esetében végeztem az adott vállalat és az összes többi különbségeinek összehasonlítására. Az elemzés célja az volt, hogy szempontokat adjon az interjúk elkészítéséhez.

A HRO és a többi vállalat összehasonlítása

A HRO szervezetben szignifikánsan nagyobb értéket mutatnak a következő biztonsági kultúra elemek: (1) a szervezet biztonságpolitikáját ismerik, a vezetők tudatosítják és a benne szereplő irányelveket alkalmazzák a mindennapi munkában (összefoglalóan az un. „Kemény elemek”, rövidítve KE faktor), (2) a standardok, dokumentumok megfelelőek, naprakészek, összhangban vannak a technológiával, valamint az előírásokat számon kérik (KE faktor), (3) a szükséges anyagi források, a technika és humán erőforrás rendelkezésre állnak, és a problémák elhárításához segítséget kapnak (KE, és „Lágy elemek”, röviden LE faktorok), (4) proaktivitás, a hierarchia minden szintjén keresik a biztonsági megoldásokat, a menedzsment elkötelezett (LE, „Hatalmi távolság”, röviden HT faktorok), (5) működik az igazságos, a jelentő és a tanuló kultúra (LE, „Tanulás”, röviden T faktorok). Ezzel szemben szignifikánsan kisebb értékű elemek: (1) kockázat (bizonytalanság) kereső magatartás (kockázatvállalás, stimuláció, nyitottság a változásra értékdimenziók), és a (2) kockázatos helyzetekben inkább másoknak való segítségnyújtás (altruizmus). Megállapítható tehát, hogy mind a szignifikánsan nagyobb, mind a szignifikánsan kisebb értékű elemek megfelelnek a nagykockázatú szervezetre vonatkozó elvárásoknak, azonban fontos megjegyezni, hogy a kérdőívet kizárólag a teljes biztonsági igazgatóság töltötte ki, tehát a hierarchia többi szintjén (legfelső vezetés, „bürokraták”, „melósok”) a válaszok nem ismeretesek, ami befolyásolhatja az egyenszilárdság és foltosság jellemzőit.

Multinacionális kereskedelmi és a többi vállalat összehasonlítása

Az eredmény jelentős átfedést mutat a HRO szervezet válaszaival (szignifikánsan nagyobb értékek: KE, LE, T faktorok), ugyanakkor a válaszok között olyan kijelentés is szerepel, amely szignifikánsan kisebb volt a HRO esetében (hedonizmus, kockázatvállalás értékdimenziók). Emellett szignifikánsan nagyobb értékeket kaptak az önállóság, altruizmus, kooperáció, innováció, nyitottság a változásra értékdimenziók (ezek a Nagyvállalat vs. KKV kategória változók összehasonlításakor a KKV-k jellemzői voltak a kvantitatív eredmények alapján) [41], ill. a szabályok „vakon” történő betartása és az egyenlő bánásmód, ami az állami nagyvállalat estében szintén szignifikánsan nagyobb értékkel szerepel. Ezek

az eredmények megfelelnek a vállalaton belül működő védelmi profilú munkavállalók attitűdjeinek és a KKV-kra jellemző individuális kultúra elemeknek. Ugyanakkor a nagykereskedelmi vállalat kapcsán is meg kell jegyezni, hogy a külföldi hátterű szervezeten belül a biztonság /védelem területén dolgozók és a biztonsági vezető vettek részt a felmérésben (a külföldi és magyar felső vezetők, kereskedelmi profilú munkavállalók, menedzserek nem töltötték ki a kérdőívet), tehát az egyenszilárdság szintjére a vállalat egészét tekintve, ezekből az adatokból szintén nem lehet következtetni.

Állami közlekedési és a többi vállalat összehasonlítása

A közlekedési vállalat biztonsági kultúra elemei jelentősen különböznek az előző két szervezettel összehasonlítva. Szignifikánsan nagyobb értékeket kapott az értékprioritások kapcsán (1) a pénz, mint motivátor szemben a biztonság elsődlegességével, valamint (2) a szervezeten belüli nagy hatalmi távolság negatív hatása a biztonságra és (3) a szervezeten kívüli tényezők biztonságra gyakorolt befolyásának észlelése (pl. társadalom, gazdaság, közélet stb.) Ugyancsak szignifikánsan nagyobb értéket adtak a válaszadók arra, hogy (4) a hibázás hátterében folyamat problémák és a munkahelyi körülmények állnak, hogy (5) a szabályokat „vakon" kell betartani, valamint az, hogy (6) a szerénység, visszafogottság fontos a biztonság megteremtésében. Ezeknek az attitűdöknek, értékpreferenciáknak mélyebb vizsgálata a kultúra rendszerbe helyezése, mély megértése szempontjából további vizsgálatokat igényel. Jelen kutatásban a vezetői interjúk részben magyarázatot adtak a felsorolt jellemzőkre. Ugyancsak további kérdéseket vetnek fel és a gyenge pontokra utalnak a szignifikánsan kisebb értékű elemek is. A válaszadók percepciói alapján ide sorolhatók, hogy (1) a szervezet biztonságpolitikáját kevéssé ismerik, nem alkalmazzák a napi munkában, (2) a biztonság kisebb értéket képvisel, (3) a standardok, dokumentumok, nem állnak összhangban a technológiával, (ez fakadhat abból is, hogy a munkavállalók nem ismerik), (3) egyéni szinten a felelős, tanuló, proaktív, tudatos, segítségnyújtó, innovatív, elkötelezett attitűd kisebb mértékben jellemző, (4) a környezetvédelem nem kap hangsúlyt, (5) az igazságos, tanuló kultúra kevéssé érzékelhető, (6) az egyes személyiség jellemzőket, az önállóságot, felkészültséget és a motivációt nem kapcsolják össze a biztonság kérdésével, (7) a hatalmi távolság kapcsán (HT faktor) kevéssé érzik úgy, hogy a menedzsment megtesz mindent a biztonság érdekében, valamint (8) az egyenlő bánásmódot is kevéssé tartják fontosnak.

Mindezek alapján megállapítható, hogy a kvalitatív kutatásban részt vett három szervezet közül a közlekedési vállalat jelentősen különbözik a biztonsági kultúra elemeit tekintve, míg a HRO és a nagykereskedelmi vállalat biztonsági / védelmi profilú egysége több ponton is egyezéseket mutat. A továbbiakban arra a kérdésre kerestem a választ, hogy mi jellemzi és magyarázza az egyes kultúra elemek vállalatspecifikus működését.

A kvalitatív kutatás eredményei

A biztonsági vezetőkkel és szakértőkkel végzett strukturált interjú a következő kérdésekből állt:

1. Hogyan értékelik az eredmény?
2. Milyen tényezőkkel magyarázzák az eredményeket?
3. Mit érdemes még vizsgálni, kutatni a jövőben?
4. Az eredmények tükrében, milyen szükséges lépéseket ismertek fel?

Az 1. és 2. kérdésre homogén válaszokat adtak: az eredményeket az adott pillanatot reálisan tükröző helyzetképnek értékelték (biztonsági klíma), melyet fő vonalakban az erős kultúra jellemzőivel magyaráztak. (Pl. „Erős struktúra, erős cég, az alkalmazottak fegyelmezettek, egy csapat vagyunk, egy irányba megyünk, egységes elvárások, egyformán gondolkodunk, a fiatalabb és idősebb kollégák tudnak egymástól tanulni, képesek a változásra, kemény elemek hatása a biztonságra”.)

A 3. és 4. kérdéskör mindhárom vállalat esetében egyedi működési jellemzőket eredményezett, ezeket a tartalom elemzést követően 3 témakörben csoportosítottam: (1) észlelt problémák a szervezeti működésben, (2) szakértői felismerések, vezetők reflexiói, a szervezeti valóság személyes észlelése (interpretációk vezetői szinten), (3) javasolt kutatási témák az elemzések tanulságai alapján.

Az alábbi összefoglaló táblázat a kvalitatív vizsgálatok eredményét három szinten mutatja be: (1) szignifikánsan nagyobb értékű kultúra elemek (t-próbák), (2) vállalatspecifikus jellemzők (interjú, tartalom elemzés), (3) a szervezeti valóság percepciói / interpretációi egyéni szinten.

	Szervezet 1 **HRO/energia szektor** Nagyvállalat (Zrt.)	**Szervezet 2** **Tömegközlekedési szektor** Állami nagyvállalat, (Zrt.)	**Szervezet 3** **Nagykereskedelmi szektor**, KKV, német tulajdonosi háttér
Résztvevők	a biztonsági igazgatóság vezetője, 3 főosztályvezetője, munka- és tűzvédelmi osztályvezetője, információbiztonsági vezetője, műszaki főszakértője, főtechnológusa	biztonsági vezető	biztonsági igazgató
Kultúra elemek (szignifikánsan nagyobb)	fejlődő, tanulni képes, igazságos, jelentő, kemény elemek (utasítások, standardok, dokumentumok és technológia összhangja)	**állami, magyar –** (1) erős biztonsági kultúra, (a vállalat kellő mértékben költ a biztonság növelésére, a munkavállalók ellenőrzés nélkül is betartják az előírásokat)„ (2) bürokratikus, (3) fejlődő, (4) konformitás és megőrzés értékdimenziók, (5) magas bizonytalanságkerülés (elvárás, hogy a szabályokat „vakon” tartsák be), (5) információ megosztás, (6) hatalmi távolság percepció (külső hatások befolyása), **nagyvállalat** -- a kockázatok csökkentését a (1) biztonságos szervezeti körülmények, (2) a felelős,	segítő, támogató, együttműködő magatartás (jóakarat, altruizmus, önmeghaladás, önállóság, nyitottság a változásra értékdimenziók)

		elkötelezett magatartás és (3) a biztonságos működési szabályok határozzák meg.	
Kvalitatív eredmények (vállalatspecifikus jellemzők)	**(1)** a bizalom és a „meggyőződés" kialakításához hiányoznak a megfelelően képzett humán szakemberek (T, LE), (2) a „melósok", „bürokraták" után „rés" van a hierarchiában (minden hazai nagyvállalatra ez jellemző) (HT, KE), (3) hiányzik a legfőbb beszállítók bevonása a biztonsági kultúra felmérésekbe (egyenszilárdság) (T), (4) a jelentő kultúra motivációs rendszere hiányos, (5) információhiány a biztonsági költségek kapcsán (KE), (6) lassú a haladás a kérdező magatartásra szocializálásban és a folyamatszemléletben (T, LE), (7) a formális képzésben sok az ismétlődés (T).	**(1)** rugalmatlan, nem reziliens (flexibilitás), (2) kevés egyéni döntéshozatal, inkább csoportos vagy hatósági (LE, HT), (3) rövid képzési idő és nincs számonkérés (T), (4) a munkavállalók nem látják át az egész szervezetet biztonsági szempontból, (5) nem hatékony átszervezések (KE), (6) szükségtelenül magas munkavállói létszám (KE), (7) alacsony a biztonsági kultúra felmérések kiterjesztése, (8) a műszaki „vezér" leterheltsége óriási.	**(1)** a hierarchiában a biztonsági igazgatóság nincs egy szinten a felsővezetéssel (nagy HT, KE), (2) nem elég erős a bizalom, a felelősségteljes és tanuló attitűd (LE, T), (3) inkonzisztencia a biztonsági kultúrában (foltosság, egyenszilárdság)
Interszubjektív eredmények (A szervezeti valóság személyes észlelése, interpretációk)	*- a magyar kultúrában az „őszinteség" faktor alacsony, a „kiskapuk keresése" faktor magas* *- a biztonsági kultúra nagyon lényeges eleme a kérdező magatartás, azonban további kérdés, „hogyan neveljük rá az embereket* *- a folyamat szemlélet alacsony színvonalon van általában Magyarországon* *- képzünk, de vajon számon is kérünk? „itt szokott lenni a luk."*, *hatótényező a képzések hatékonysága* *- a biztonsági kultúra nem mindenkinek „kedves" téma, de adott szint alá nem szabad menni* *- még senki sem ismerte el, hogy ő maga hibázott* *- a biztonsági kultúrából a kultúra fontosabb*	*- túl nagy cég, a dolgozók figyelmezettek* - a szabályokat figyelembe véve, *„ugyanaz jár mindenkinek",* - nemzetközi biztonsági fórumok kapcsán: *„figyeljük a világot, az eseményekből tanulunk"* *- nagy a cég, mindenki várja, hogy mi lesz: főváros, kormány, ellenzéki szerep – nehéz kitörni* *- minden évben új szabályozók jönnek, politikailag új preferenciák* *- a felettes szervezet rendeli meg a tevékenységet, büntetni tud, jelentős a politikai hátszél* *- 10-15%-kal többen dolgoznak, lehet, hogy „túllőttünk" ezen* *- 5 évente átszervezzük a struktúrát, de „másképp egyforma marad"* *- a bekövetkezett események mindig sokat változtatnak a biztonsági kultúrában*	*- ha ott áll mögöttem a CEO, ellehetetleníti a munkát, amiért dolgozunk* *- mindig a költségekkel jönnek elő* *- most marketing is kell a biztonsághoz* - jól *érzik magukat, bár nyafognak, lehet, hogy nem mernek őszinték lenni?* *- ahogy cserélődnek az emberek, már az elejétől úgy kell orientálni, hogy a biztonság fontos*

3.táblázat: A vizsgált három vállalat biztonsági kultúra jellemzőinek összefoglalása

ÉSZLELT PROBLÉMÁK ÉS JELLEMZŐK A SZERVEZETI MŰKÖDÉSBEN

Szervezet 1 (HRO)

A nagykockázatú szervezetben a biztonsági kultúra felméréseket jogszabály és nemzetközi standard írja elő, két évente kötelező végrehajtani, azonban az egyik legszembetűnőbb tendencia, hogy **a** kitöltési hajlandóság folyamatosan csökken. Ennek következtében vannak olyan szervezeti kockázati tényezők, amelyek nem derülnek ki, tehát a biztonságtudatosság szintje és a szervezetre jellemző biztonsági attitűdök feltáratlanul maradnak. A vezetők tapasztalatai azt mutatják, hogy a megfelelő számú biztonsági kultúra kérdőívek elemzésével meg lehet találni a vállalati működés „gyenge pontjait", de ha ennek pontos meghatározása nem lehetséges, akkor az adott témára épített fókuszcsoportos megbeszélés sem éri el a célját. A kitöltési arány növeléséhez, a vezetők véleménye szerint, elsődleges tényező a bizalom megszerzése. A bizalom mellett a legnehezebb kultúrára ható jellemző a „meggyőződés" kialakítása, amelyhez hiányoznak a megfelelően képzett humán szakemberek, valamint nagy szükség van a legfőbb beszállítók bevonására is a biztonsági kultúra felmérések kapcsán: fontos lenne a saját cégükben is elvégezni ugyanazt a felmérést, így megbízható képet kaphatnának az egyenszilárdság állapotáról. Az elmondottak alapján, ugyancsak a bizalom támájával függ össze, hogy a „melósok", „bürokraták" után „rés" van a hierarchiában, más szóval a felső vezetők és az alsóbb szintek között nagy a hatalmi távolság, eseteként hiányos a kapcsolat. *(„A nagyvállalatoknál mindenhol ez a jellemző.")* Ez a jelenség hátrányosan befolyásolhatja a biztonságot is, mert ha nincs bizalom, akkor többek között akadályokba ütközik a kommunikáció és nem érvényesül a jelentő, igazságos, tanuló, ill. hiba kultúra [2], ez pedig fokozza a kockázatokat, bizonytalanságot, valamint az emberi hibázást. Egybehangzó vezetői és szakértői vélemény, hogy a biztonsági kultúrával nem mérnököknek kellene foglalkozni, hanem humán szakembereknek, közös álláspontjuk az volt, hogy „a biztonsági kultúrából a kultúra fontosabb", mert *„a biztonságot megoldja a technológia".*

A vezetők megállapításai alapján, a társadalmi kultúrába való beágyazottság is fontos hatótényező, jól felismerhető jellemzői megjelennek a szervezeti magatartásban és befolyásolják a nagykockázatú szervezetekben elvárható megfelelő szocializációt, ill. biztonsági attitűdöket. Például a vezetők által beazonosított (detektált) kockázati tényező, hogy *a magyar kultúrában az „őszinteség" faktor alacsony, a „kiskapuk keresése" faktor magas.* Ez egy HRO vállalat esetében, ahol a szabályok, standardok, irányelvek szigorú betartása és alkalmazása elengedhetetlen a biztonságos működéshez, kockázatos értékpreferencia, megváltoztatása pedig rendkívül összetett.

Mindezek mellett a vezetők konkrét problémának látják, hogy a jelentő kultúra motivációs rendszerét finomítani kell. Ha például valaki problémát, hibát észlel, jelenti (biztonságtudatosság, jelentő kultúra), akkor a káresemény megelőzését jutalmazzák (igazságos kultúra). Azonban a gyakorlatban a problémákat főleg vezetők veszik észre, szervezeti szinten kommunikálják (elkötelezettség, tanuló kultúra**),** *„de még senki sem ismerte el, hogy ő maga hibázott"* (hibakultúra alacsony szintje).

Összegzésként megállapítható tehát, hogy a statisztikai eredmények alapján beazonosított kultúra elemek, pl. fejlődő [3], tanulni képes, igazságos, jelentő, KE faktor (utasítások, standardok, dokumentumok és technológia összhangja) meghatározó jellemzők a

HRO szervezet esetében, azonban javításuk érdekében sok a tennivaló, a problémák megoldása, kezelése pedig összetett társadalmi és vállalati feladat.

Szervezet 2 (Közlekedés)

Az állami magyar nagyvállalat biztonsági vezetője úgy látja, hogy a szervezet „piramis és jól olajozott gépezet" [42] egyszerre. Az egyik legfontosabb probléma és szempont, hogy folyamatosan alkalmazkodni kell a külső környezethez, ezért tervezni és fokozni kell a szervezet flexibilitási képességét és a rezilienciát. Ez nemcsak a gazdasági és társadalmi változásokra való gyorsabb reagálást jelenti, hanem a közélet alakulására adandó válaszokat is. Vezetői tapasztalat például, hogy minden évben új szabályozók kerülnek bevezetésre, politikailag új preferenciák, ami szükségessé teszi az alkalmazkodást, azonban ez megnehezíti a szervezeti működést, ami kihat a biztonságra is. A vezetői interjú alapján, a nagy hatalmi távolság percepció ebben a szervezetben is jellemző: a felettes szervezet rendeli meg a tevékenységet, *„büntetni tud"* és *„jelentős a politikai hátszéllel rendelkezik"*, ami nem kedvez a biztonsági kultúra állapotának, fejlődésének.

A legmegosztóbb kijelentés a kérdőívben a „dönthet önállóan" volt, erre a vezetői magyarázat az, hogy a döntéshozatalban kevés az egyéni, inkább a csoportos, vagy hatósági döntés jellemző. Az „egyenlő bánásmódot" és a „törődik mások biztonságával" jellemzők kapcsán a magyarázat az interjú alapján, hogy *„túl nagy cég, a dolgozók fegyelmezettek"* és a szabályokat figyelembe véve, *„ugyanaz jár mindenkinek",* valamint erős a szakszervezet háttér támogatása.

Az interjú tehát megerősítette és magyarázatot adott a kvantitatív kutatás eredményeire az olyan kultúra elemek esetében, mint pl. bürokratikus, konformitás és megőrzés értékdimenziók, [7], magas bizonytalanságkerülés (elvárás, hogy a szabályokat „vakon" tartsák be), valamint a hatalmi távolság [42], percepció (külső, belső hatások befolyása).

Szervezet 3 (Nagykereskedelem)

A multinacionális nagykereskedelmi vállalat biztonsági igazgatójával készített interjú alapján szintén a nagy hatalmi távolság hatása jelenti az egyik problémát a szervezet működésében. Vezetői percepció, hogy a hierarchiában a munkáltatói jogkör gyakorlója *„magasabb rendűnek érzi magát"*, mint egy funkcionális, más szóval a biztonsági igazgatóság nem egyenrangú partnere a felsővezetésnek. A vezető álláspontja az, hogy biztonsági szempontból hasznos lenne, ha például a biztonsági igazgató (interjú alany) is rendelkezne munkáltatói jogkörrel, valamint nagyobb hatáskörrel a pénzügyek területén, mert a biztonságra érdemes többet költeni. A szignifikánsan nagyobb kultúra elemek közül tehát a kvalitatív vizsgálat megerősítette az önállóság és a nyitottság a változásra értékdimenziókat. Annak ellenére, hogy a hatalmi távolság percepció nem szerepel szignifikánsan magasabb értékkel a statisztikai eredmények között, a vezető mégis az egyik legfőbb problémának nevezte meg.

VEZETŐK FELISMERÉSEI, REFLEXIÓI

Szervezet 1 (HRO)

A vezetők tapasztalatai alapján a biztonsági kultúra felmérése azért fontos, mert „az eredmények kapcsán meg lehet fogalmazni, alá lehet támasztani a szükségességét, ill. a fejlesztés érdekében lényeges szempont az erősségek-gyengeségek meghatározása". Ez a

szemlélet megegyezik azzal a koncepcióval, hogy a biztonsági kultúra egy folyamatos kutatás – tanulás – javítás folyamat eredménye.

A KE faktor vonatkozásában vezetői felismerés, hogy nem lehet tudni, hogy kellő mértékben költ-e a szervezet a biztonság növelésére: „még a vezető sem tudja pontosan**,** kevesen látnak rá", valamint „összességében elmondható, hogy senki sem költ szívesen a biztonságra". Ez a kérdéskör mélyebb elemzést igényel, azonban jelen kutatás nem terjedt ki a jelenség hátterének vizsgálatára, magyarázatára.

A fókusz csoportos interjú hangsúlyos témája volt, hogy ebben a nagykockázatú szervezetben is az előírások betartása szigorú, azonban mégsem várják el, hogy a szabályokat „vakon" tartsák be a munkavállalók, mert a biztonsági kultúra nagyon lényeges eleme a kérdező magatartás, azonban további kérdés, „hogyan neveljük rá az embereket".

Azzal kapcsolatban, hogy a hibázás hátterében szervezeti folyamatproblémák állnak-e a következő magyarázat született: a folyamat szemlélet alacsony színvonalon van általában Magyarországon, nehezen gondolkodnak folyamatokban a cégek, kérdés, hogyan szervezhető, ennél a vállalatnál például 4-5 év óta tanulják, de lassú a haladás.

A tanuló kultúra értékelése kapcsán az interjú megerősítette: logikus, hogy a biztonsági képzés hozzájárul a szervezet biztonsági céljainak eléréséhez, azonban a tapasztalatok alapján további kérdés, hogy „képzünk, de vajon számon is kérünk? „itt szokott lenni a luk. Hatótényező a képzések hatékonysága." Tehát a tanuló szervezet evidencia, azonban a formális oktatásban sok az ismétlődés.

Szervezet 2 (Közlekedés)

A magyar nagyvállalat esetében a tanuló elem kapcsán a vezető a következő jellemzőket sorolta fel: (1) az oktatás területén a biztonsági munkakörben dolgozók kapnak továbbképzést, 3-4 nap kellene az ismeretek alapos elsajátításához, azonban a több napos képzés nem életszerű. A képzési idő rövidsége mellett az is problémát okoz, hogy (2) nincs számonkérés. Mindezek következménye, hogy (3) a munkatársak csak kisebb területet ismernek, nem látják át az egész szervezetet biztonsági szempontból. Ugyanakkor a szervezeti tanulást segíti, hogy a biztonsági igazgatóság 1-2 évente nemzetközi szakmai fórumokon vesz részt, melynek célja a tapasztalatcsere. *(„figyeljük a világot", „az eseményekből tanulunk")*

A vezetővel készített interjú vállalati struktúrára irányuló magyarázata (KE faktor), rávilágított arra is, hogy a vállalat átszervezése öt évenként valósul meg, de minden alkalommal *„másképp egyforma marad"*, valamint a munkavállók létszáma 10-15%-kal több, mint ami a hatékonysághoz szükséges és ezt a költséget a biztonságra is lehetne fordítani.

Szervezet 3 (Nagykereskedelem)

A statisztikai elemzések kapcsán a biztonsági vezető felismerte, el kell gondolkodni, hogyan érhetnének el jobb eredményt: *„lehet, hogy csak egy worshop is elég".* Szintén felismerés, hogy *„a rutin kevés",* ma évről-évre magasabb az elvárás és fontos a folyamatos tudásfrissítés a biztonság területén is. Ugyancsak vezetői felismerés, hogy a válaszok alapján a mélyebb okokat is fel kell tárni a jövőben, (pl. lehet, hogy *„a közvetlen felettese elnyomja a munkavállalót",* ezért a biztonsági igazgatóságnak kellene kivizsgálni, mint „független" szakértők stb.) Emellett hamarabb kellene biztonsági szemléletre és gondolkodásmódra szocializálni az új munkatársakat. *(„ahogy cserélődnek az emberek, már az elejétől úgy kell orientálni, hogy a biztonság fontos")*

A külső és belső hatótényezők a biztonságra témakör kapcsán további vezetői reflexió, hogy az összefonódások növelik a kockázatot és a korrupció veszélyeztetheti az üzleti folyamatok hatékonyságát. Bár a vezető megítélése szerint a kérdőív eredményei megfelelően tükrözik a szervezeti valóságot, megmutatják, amit reálisan „éreznek" a munkavállalók, a bizalmat tovább kell erősíteni, valamint jó lenne, ha a dolgozók akkor is betartanák a biztonsági eljárásokat, ha felettesük nem tudja ellenőrizni. Új szempont annak felismerése is, hogy a biztonság területét érdemes lenne csökkenteni az „elszigeteltség érzést", erősíteni a biztonságért „mindenki felelős" szemléletet és a „a hibázásból tanulni kell" attitűdöt (krízis események, pl. pandémia)**.** Emellett a vezetői percepciók között szerepelt a *„befásulás"* kezelése, annak érdekében, hogy „*ne legyen unalmas a biztonság téma"*.

Az interjú során a vezetőt visszatérően foglalkoztatta, hogy közelebb kellene kerülni a leadership-hez kérdése, mert a biztonság, több, mint védelem, valamint, ha nincs függetlenség, nincs felhatalmazás, akkor nehéz döntéseket hozni. *(„bizalom nélkül, hogy dolgozzak?")* Megállapítást nyert az is, hogy a security (védelem) területén jellemzően alul vannak fizetve a dolgozók és ez kockázat más védelmi cégnél is, ennek ellenére a pénz nem lehet fő motiváció.

JAVASOLT KUTATÁSI TÉMÁK, TOVÁBBI VIZSGÁLATOK

Szervezet 1 (HRO)

A kvalitatív kutatás eredményeként a probléma területek, új kutatási fókuszok az alábbiakban foglalhatók össze a HRO vállalatnál készített fókuszcsoportos interjú alapján:

- Hogyan tudjuk befolyásolni a kultúrát, vagy hogyan érjük el, hogy az egyes jellemzők (kultúra elemek) a részévé váljanak? Lehet-e a biztonsági kultúrát alakítani?
- Hogyan változott dinamikájában a kultúra? Milyen különbségek vannak az egyes generációk között? (Ez más vállalatoknál is időszerű kérdés.)
- Milyen eszközöket lehet bevetni a biztonság érdekében a digitális korszakban?
- Kényelem kontra biztonság: a biztonság *„kényelmet gátló eszköz"?* (IT szempont) A biztonsági rendszerek megoldják a biztonsági problémákat, de hogyan lehet a tudatosságot, készenléti állapotot fenntartani, az „overfamiliarity" jelenségét kiküszöbölni?
- Befolyásolja a szervezeti magatartást és ezáltal a működést, hogy ki, hova van beágyazódva „*a normál társadalomba"*? Hogyan lehet elérni, hogy belépve a céghez a „biztonság tudatos vagyok" attitűd legyen a prioritás? Miként lehet rávenni a munkavállalókat, hogy „*itt más*", az értékek, normák különböznek a társadalmi szinten tapasztaltaktól, tehát ki kell zárni a külvilágot, mert itt mások az értékpreferenciák. *„Hogyan érhető el, hogy a kapun kívül hagyja azokat a szokásokat, viselkedésformákat, attitűdöket, amik itt kockázatosak?"* (pl. szabálykerülés, vs. szabálykövetés „rábólintás" vs. kérdező magatartás, „megoldjuk okosban" vs. eljárásrendek, szabványok szigorú betartása, közömbösség vs. éberség, tudatosság stb.)
- Mennyire jó a kiszervezett cégmodell? Nem mindegy a kontraktor minősége**,** az egyenszilárdságot folyamatosan mérni, monitorozni kell a biztonság érdekében.
- A biztonságnak van ára? Mi a kapcsolat a pénz és a biztonságtudatosság között?

Szervezet 2 (Közlekedés)

- A felső vezetőket is be kell vonni a biztonsági kultúra felmérésekbe, **„***bár csak hibátlan, elvárt válaszokat adtak volna”***,** azt, hogy minden OK, *„nem mondhatnak mást, csak, ami a szabályokban le van írva”.*
- A legfelsőbb vezetés (12 fő), ismeri a szervezeti valóságot, azonban a műszaki „vezérnek” nincs ideje erre, mert óriási a leterheltség.

Összességében tehát a nem biztonsággal foglalkozó területek vezetőinek, valamint az alvállalkozók biztonsági kultúra attitűdjeit is kutatni kell ahhoz, hogy az egyenszilárdság megvalósuljon.

Szervezet 3 (Nagykereskedelem)

A biztonsági igazgatóval készített interjú alapján a következőképpen foglalhatók össze a további kutatási témák.

- A kérdőív „jól össze van rakva, minden benne volt, kerek”, megmutatja a szervezeti biztonsági klímát, ebben nincs javaslat, azonban a szervezeten kívüli befolyásoló tényezők kérdése lényeges kutatási terület lehet (pl. politika, társadalmi összefüggések), annak ellenére, hogy a vállalat „semleges oldalt” képvisel. Emellett mélyebben meg kell vizsgálni a biztonsági igazgató és a munkavállalók közti bizalom kérdését.
- A vezető tapasztalata az, hogy „fő motivációs tényező a bér” *(„folyton nyafognak, de a kérdőívből nem jött fel”)*, azért is érdemes foglalkozni vele, mert ebben a kérdésben a tapasztalt valóság és a kitöltött kérdőív nincs összhangban, *„lehet, hogy nem mertek őszinték lenni”* a munkavállalók. Tehát a kérdőív válaszai alapján az alkalmazottak jól érzik magukat, a vezetői tapasztalat viszont azt mutatja, hogy rendszeresen panaszkodnak az alacsony bérekre.

KÖVETKEZTETÉSEK, SZAKMAI AJÁNLÁSOK

A fentiek alapján megállapítható tehát, hogy a kvalitatív eredmények megerősítették a szignifikáns különbségeket, ugyanakkor ezen túlmutatva, a vállalatok egyedi jellemzőit, mélyebb biztonsági kultúra rétegeinek vizsgálatában is eredményre vezettek. A triangulációnézőpontjai közül jelen tanulmányban a kvalitatív szakaszra helyeztem a hangsúlyt, melynek eredménye az ismertetett módszerek által kinyert információk, adatok magyarázó erejének bizonyítása, az egyes jelenségek hátterének mélyebb megértése, valamint az új kutatási fókuszok megtalálása. Emellett további tanulság, hogy az ebben a szakaszban szerzett kutatói tapasztalatok és eredmények megerősítették, hogy a jövőben a kvalitatív módszertanokat érdemes tovább bővíteni a biztonsági kultúra elemeinek mélyebb vizsgálatában.

A kutatás eredményei alapján a következő ajánlások fogalmazhatók meg a biztonsági kultúra kapcsán szervezeti szinten és tágabb összefüggésben.

Vezetői, szervezeti szint:

- nagyon sok a tennivaló a jelentő és igazságos kultúra területén, ehhez meg kell teremteni az alapokat: bizalom, nyílt kommunikáció, kérdező magatartás, kooperáció, stigmatizáló mentes hibakultúra, ösztönzés, a retorzióktól való félelem kiküszöbölése,

- a magyar vállalatoknak fejleszteni kell a szervezet flexibilitását és erősíteni a folyamatszemléletet,
- a biztonsági standardok, szabályzatok és a szervezetben alkalmazott technológia összhangjának, illeszkedésének vizsgálata további kutatást igényel,
- a felső vezetés és a nem biztonság területén dolgozó top menedzserek eltérő súllyal kezelik a biztonságot és sok esetben még mindig a termelést helyezik előtérbe a biztonság rovására, ezen a szemléleten változtatni kell,
- a biztonsági vezetők elkötelezettsége, profizmusa, szakértelme magas szintű, azonban a törvényi megfelelésen túl, bár határozottan képviselik, de nehezen érvényesítik elképzeléseiket a felső vezetés felé (pl. biztonsági kultúra felmérések, költségek stb.), ezért erősíteni kell a vállalton belül a hierarchia szintjei között a kommunikációt a biztonság kapcsán,
- a biztonsággal foglalkozó vezetők és menedzserek értékprioritásai (transzparencia, őszinteség, bizalom, környezetvédelem, fenntarthatóság, hiba és kérdezés kultúra), egyezést mutatnak (erős szakma kultúra), ugyanakkor a felső vezetés biztonsági paradigmája sok ponton eltérő szemléletet tükröz, ezért a szakmai párbeszédet erősíteni kell a szervezeti hierarchia különböző szintjei között,
- a szervezeten belüli és kívüli hatalmi különbségek növelhetik a kockázatokat, azonban vállalat specifikusan a mélyebb okok, ill. a társadalmi és vállalati kultúra biztonság fókuszú kapcsolatának vizsgálatára is szükség van,
- a felsővezetők „félnek" a „melósok" lekérdezésétől, annak ellenére, hogy a biztonsági vezetők szorgalmazzák az egyenszilárdsági kockázat kiküszöbölése érdekében, az okok mélyebb vizsgálatára nincs lehetőség, pedig kulcsténvező lehet a kockázatok csökkentésében (pl. a kontraktorok biztonsági kultúra felmérését is szorgalmazni kell),
- a biztonsági igazgatók és szakértők egyöntetű álláspontja, hogy a „melósokon" kívül a felső vezetők biztonsági attitűdjeit is ajánlott megvizsgálni, ezen a téren nagy az információ hiány,
- a hierarchiában „vákuum", „gap" van a felső vezetők és a biztonsági menedzsment között, melynek egyik következménye a hiányos kommunikáció, ami növelheti a kockázatokat,
- a tanuló kultúra mindenhol jelen van és nagyra értékelt, azonban a Reason féle négy kultúra elem együttesen nem érvényesült (tanuló, jelentő, igazságos, rugalmas kultúra), ezért a modell alkalmazhatóságát ki kell dolgozni és tudatosítását szorgalmazni kell,
- a szervezeti tanulás terén túl sok az ismétlődés a formális biztonsági oktatásban és még a nagykockázatú szervezetek esetében is kérdés, hogy elég hatékony-e a számonkérés, ezért a képzések minőségén, módszerein, ellenőrzésén, számonkérésén javítani kell,
- a fiatal generáció értékprioritásait, biztonsági attitűdjeit és ezek illeszkedését az adott vállalathoz a biztonsági kultúra kapcsán is ajánlott megvizsgálni,
- a nukleáris iparban, valamint a nagykockázatú szocio-technikai rendszerek esetében kötelező, a nemzetközi szervezetek által hivatalos ajánlásokban megfogalmazott biztonsági kultúra felmérés elvégzése ajánlott más gazdasági szektorokban, iparágakban is,

- a biztonsági kultúra egyik ága a védelmi (security) kultúra, ez Magyarországon jellemzően alulfizetett terület, amelyet a cégek alvállalkozói rendszerben működtetnek, azonban a „belsős" biztonsági vezetők mind az alacsony béreket, mind a kiszervezést kockázati tényezőnek értékelik,
- a biztonságot a vállalatok műszaki területként kezelik, és jellemzően csak a biztonsági vezetők szorgalmazzák, hogy speciálisan képzett humán szakemberek nélkül a biztonsági kultúrát nem lehet megváltoztatni, ezért tudomány és- szakmaközi együttműködésre és szemléletváltásra is szükség van.

Társadalmi szint, tágabb összefüggések:

- a társadalmi kultúrából fakadó, egyéni szocializáció során kialakult értékpreferenciák, motivációk, attitűdök nem mindig illeszkednek a szervezeten belüli biztonsági kultúra prioritásaival és az ebből fakadó elvárásokkal, tehát a biztonsági kultúra kapcsán társadalmi szintű kutatásra is szükség lenne a változáshoz,
- a hatalom, a hatalmi távolság (mennyire fogadják el az emberek a nagy hatalmi különbségeket) és a hatalom gyakorlása, szerepe, valamint a biztonság közötti kapcsolatot szervezeti és társadalmi szinten is vizsgálni kell,
- ha a döntéshozók annak érdekében, hogy a büntetést elkerüljék kizárólag a standardok, szabályok, előírások, betartatásával törődnek, vagy inkább kifizetik a pénzbírságot, ahelyett, hogy a biztonsági szakrendszerekbe fektetnének, ill. a szervezeti biztonságot nem együtt kezelik a fenntarthatóság kérdéseivel, fennáll a környezeti és társadalmi katasztrófák kockázata, tehát a biztonság kérdését komplexen ajánlott kezelni,
- a jelentő kultúrában erőteljes visszaesés tapasztalható, amit a biztonsági vezetők pl. a társadalmi hatásokkal magyaráznak: csökkent a bizalom, az őszinteség, a kérdezés kultúra, a „túlságosan tiszteletteljes", „tekintélyelvű" (munka)környezet aláássa a bizalmat, ezzel növeli a kockázatot, ezért a nagy hatalmi távolság index és hatásának, következményeinek további vizsgálata szükséges.

ÖSSZEGZÉS

A fentiek alapján bizonyítottam, hogy az ismertetett kvalitatív módszerekkel mélyebben határozhatók meg adott szervezet egyedi biztonsági kultúra jellemzői, azok kontextusa, az egyes kultúra elemek vállalatspecifikus magyarázata. Az ismertetett eredmények túlmutatnak a komplementer jellegen [43] [44][45] azáltal, hogy új fókuszokat tárnak fel a javítás érdekében alkalmazható szakmai ajánlásokhoz, valamint a jövőbeli vizsgálatokhoz. A kutatás folyamatában a statisztikai eredményekből kiindulva, az adott vállalat biztonsági kultúra jellemzői megmutatják, hogy a vezetők melyik típusú szervezetben szocializálódtak, majd ezeket a jellemzőket tovább mélyítették az interjúk. Az interszubjektív megközelítés a biztonsági kultúra elemeivel összefüggő szervezeti valóság személyes észlelése a további vállalat specifikus jellemzők és azok okainak beazonosítását is lehetővé tette.

A kutatás során megismert 41 szervezet, a kérdőíves vizsgálatokban résztvevő 8 vállalat és a kvalitatív kutatási fázisban közreműködő 3 szervezet nem reprezentálja a sokaságot, így azokról csak a konkrét esetekre vonatkozó megállapítások tehetők. A szervezeti „gyökérproblémák" biztonsági fókuszú vizsgálata hosszú folyamat és rendkívül szen-

zitív terület, azonban a kinyert adatok és vizsgálati eredmények rávilágítanak a hazai szervezeti biztonsági kultúra számos közös pontjára, fejlesztendő területeire, valamint segítenek a további kutatási irányok meghatározásában.

Mindezeken túl, kutatói munkámra reflektálva és a kutatás menetét más nézőpontba helyezve, maga a folyamat instrumentális esettanulmánynak is tekinthető (instrumental case study) [46], melynek lényege, hogy a konkrét eset egy másik cél elérését segíti, például egy jelenség megértését vagy az elméletépítést. Jelen munkában azt, hogy miként ragadható meg a biztonsági kultúra, hogyan jellemezhető az egyes szervezetekben, mi a kapcsolat a különböző vizsgálati módszerek között, illetve hogyan, milyen kutatásokkal építhető tovább a biztonságtudomány, mint önálló diszciplína. Ebben az értelemben a kutatás egy instrumentális esettanulmányként is definiálható.

Összességében kutatásom pilot jellegű, amely egy komplex kérdéskör tanulmányozása érdekében, meghatározott mintán, illetve egy lehatároltabb, de állandó résztvevői kör bevonásával történt. Mivel jelen kutatás szemléletét és módszereit tekintve a hazai biztonságtudományban előzmény nélküli, ezért a kutatási módszerek kidolgozásához, kikísérletezéséhez egy elmélet alapú, saját kérdőívet alkalmaztam, melyre kvalitatív vizsgálatokat építettem. Jelen tanulmány ez utóbbit mutatta be részletesen.

FELHASZNÁLT IRODALOM

[1] Reason, J. (2016), MANAGING THE RISKS OF ORGANIZATIONAL ACCIDENTS 2016 Taylor & Francis, New York USA,
[2] Reason, J. (1998). Achieving a safe culture: Theory and practice. Work & Stress, 12(3)
[3] Westrum, R. A (2005) Typology of Organisational Cultures, Quality and Safety in Health Care 13 Suppl
[4] Peters, T., & Waterman, R. (1982). In search of excellence. New York: Harper & Row Publishers.
[5] Kumar, S., (2019), The McKinsey 7S Model helps in Strategy implementation: A Theoretical Foundation, Tecnia Journal of Management Studies Vol. 14 No. 1
[6] Schwartz, S. H. (2003). A proposal for measuring value orientations across nations. Questionnaire Package of the European Social Survey, 259, 290
[7] Schwartz, S. H. (2011). Studying values: Personal adventure, future directions. Journal of Cross-Cultural Psychology, 42,
[8] Prazsák, G., (2014), Generációk és értékrendszerek: a tudás új útjai". *Információs Társadalom* XIV, 2. szám
[9] FICHTINGER Gy. (ed., director general): A biztonsági kultúra felmérése és az eredmények hasznosítása nukleáris létesítményeknél (Assessment of Safety Culture and Results Utilization in Nuclear Facilities), 2.18. sz. útmutató; OAH (Országos Atomenergiai Hivatal, National Nuclear Energy Office), Budapest, 2015.
[10] RAJNAI Z.; PUSKAS B.: Requirements of the Installation of the Critical Informational Infrastructure and Its Management; Interdisciplinary Description of Complex Systems, Vol. 13, No. 1, 2015, pp. 48–56.
[11] INSAG: Safety Culture. Safety Series No 75-INSAG-4, International Atomic Energy Agency, Vienna, 1991.

[12] SOLYMOSI M.: Új eljárások a nukleáris biztonsági és védettségi kultúra felmérésére és fejlesztésére. Doktori (PhD) értekezés, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, Budapest, 2018.
[13] ROCHLIN, G.I., LA PORTE, T., ROBERTS, K.: The self-designing high reliability organization. Naval War College Review, Autumn, 1987
[14] WEICK, K.E., SUTCLIFFE, K.M.: Managing the Unexpected: Assuring High Performance in an Age of Complexity. University of Michigan Business School Press, 2001.
[15] WEICK, K.E., SUTCLIFFE, K.M.: Managing the Unexpected: Resilient Performance in an Age of Uncertainty. 2nd ed., Jossey-Bass, San Francisco, 2007.
[16] WILPERT, B., ITOIGAWA, N.: Safety Culture in Nuclear Power Operations. Taylor & Francis, London, 2001.
[17] GORDON, G.G.: Industry determinants of organisational culture. Academy of Management Review, 16(2), 396-415, 1991
[18] BEREK Lajos - BEREK László - RAJNAI Zoltán: Tudományos kutatás folyamata és módszerei; 2022, ÓE-BGK 3073, ISBN 978-963-449-071-5.
[19] Babbie, E. 2008. A társadalomtudományi kutatás gyakorlata. Budapest: Balassi Kiadó.
[20] Cooper, M D, (2000), Towards a model of safety culture, 2000, Safety Science, (36)
[21] JUHÁSZ, M. – VASVÁRI, F. (2022): A BIZTONSÁGTUDATOS VEZETŐI ATTITŰD VIZSGÁLATA LEADERSHIP ATTITUDE IN CREATING A SAFETY CULTURE, VEZETÉSTUDOMÁNY / BUDAPEST MANAGEMENT REVIEW LI I. ÉVF. 2022. 1. SZÁM
[22] RICHTER, A., KOCH, C.: Integration, differentiation and ambiguity in safety cultures. Safety Science, 42, 2004.
[23] Lazányi, K. (2016). A biztonsági kultúra szerepe a vezetői döntések támogatásában. TAYLOR, 8(1), 143-50.
[24] Lazányi, K. (2015): Mire jó a biztonsági kultúra? TAYLOR. Gazdálkodás- és szervezéstudományi folyóirat. A Virtuális Intézet Közép-Európa Kutatására Közleményei, Szeged
[25] Kertai-Kiss I. (2024), Eltérő kultúrák biztonsági és nem biztonsági profilú vállalatoknál, Biztonságtudományi Szemle, VI. évf. 4. szám, ISSN 2676-9042
[26] Naevetsad, T. O., (2009), Mapping Research on Culture and Safety in High-Risk Organizations: Arguments for a Sociotechnical Understanding of Safety Culture, Journal of Contingencies and Crisis Management 17(2)
[27] Reason, P. (1994): Three approaches to participative inquiry, In: Denzin, N. K., Lincoln, Y. S.: Handbook of qualitative research, Sage, Thousand Oaks
[28] Gelei, A. (2002): A szervezeti tanulás interpretatív megközelítése: a szervezetfejlesztés esete, PhD értekezés, Budapest
[29] Le Cose (2019), How safety culture can make us think, in: Safety Science, 218
[30] Schein E. H., (1987), The Clinical Perspective in Fieldwork, SAGE Publications, Inc. Series: Qualitative Research Methods
[31] Schein, E. H., & Schein, P. A. (2021). Humble inquiry. San Diego, CA: Berrett Kohler.
[32] Schein, E. H., & Schein, P. A. (2023). Humble leadership (2nd ed.). San Diego, CA: Berrett Kohler.

[33] ADERAMO, A.T.; OLISAKWE, H.C.; ADEBAYO, Y.A.; ESIRI, A. E.: Behavioral Safety Programs in High-Risk Industries: A Conceptual Approach to Incident Reduction; Comprehensive Research and Reviews in Engineering and Technology, Vol. 02, No. 01, 2024.
[34] Denzin, N. K., (2017), Qualitative Inquiry Under Fire Toward a New Paradigm Dialogue First Published 2009, eBook Published 2017 New York Routledge
[35] Coghlan, D. (2024): Edgar H. Schein: The Artistry of a Reflexive Organizational Scholar-Practitioner, Routledge Studies in Organizational Change & Development, Routledge, London
[36] Brewerton, Millward L. J., (2001) Organizational Research Methods, SAGE
[37] Flick U., (2014), The SAGE Handbook of Qualitative Data Analysis, SAGE
[38] Sántha K. (2017), A TRIANGULÁCIÓ-TIPOLÓGIÁK ÉS A MAXQDA KAPCSOLATA A KVALITATÍV VIZSGÁLATBAN, VEZETÉSTUDOMÁNY / BUDAPEST MANAGEMENT REVIEW XLVIII. ÉVF. 2017. 12. SZÁM
[39] Sántha, K:, (2009), Bevezetés a kvalitatív pedagógiai kutatás módszertanába**,** Bevezetés a kvalitatív pedagógiai kutatás módszertanába, Eötvös József Könyv- és Lapkiadó Bt., Budapest, **ISBN:** 978-963-7338-99-1
[40] Gadamer, H.G. (2003): Igazság és módszer. Egy filozófiai hermeneutika vázlata., Budapest, Osiris
[41] Kertai-Kiss, I. (2024), A biztonsági kultúra elemeinek különbségei hazai nagyvállalatok és KKV esetében, ÓE Társadalom, Informatika és Gazdaság Kutatócsoport, TIG-KONF 2024 Szikora Péter (szerk), ISBN 978-963-449-370-9
[42] HOFSTEDE, G., HOFSTEDE, G.J., MINKOV, M.: Cultures and Organizations: Software of the Mind. 2nd ed., McGraw-Hill, New York, 2005.
[43] Ausabha, R., Woelfel, M. L. (2003). Qualitative vs quantitative methods: Two opposites that make a perfect match. Journal of the American Diedetic Association, 103(5), 566–569.
[44] Balázs, K., Hőgye-Nagy, Á., (2015), Kevert módszerű pszichológiai kutatás: A kvalitatív és a kvantitatív kutatási módszer integrációja., In: Pszichológiai Módszertani Tanulmányok (pp.9-28), Debreceni Egyetemi Kiadó, Editors: Balázs Katalin, Kovács Judit, Münnich Ákos
[45] *Koltai Júlia – Sik Endre – Simonovits Bori* (2015): A kvali-kvanti áldilemmán túl. Szociológiai Szemle, 25 (2): p. 31-49.
[46] Stake, R. E., (2011), Standards-Based & Responsive Evaluation (Methods: Evaluation, Program evaluation, Observational research) , Publication year: 2004 Online pub date: January 01, 2011, SAGE

DOI: https://doi.org/10.12700/btsz.2025.7.4.79

ASSESSMENT OF POTENTIAL WAR-RELATED ENVIRONMENTAL DAMAGE TO METEORITE CRATERS IN UKRAINE

AZ UKRAJNAI METEORITKRÁTEREK ESETLEGES HÁBORÚS KÖRNYEZETKÁROSÍTÁSÁNAK VIZSGÁLATA

REZSABEK Nándor[1]

Abstract

This study examines the potential war-related impacts on the natural and built environments of 8 meteorite craters in Ukraine. The research aimed to determine whether environmental damage could be detected based on available primary and secondary data sources. Meteorite databases, scientific literature, and mapped satellite and aerial imagery were analyzed to compare pre-war and wartime conditions. The results indicate that the craters have remained intact, with no evidence of war-related environmental harm. Although not necessarily the result of deliberate action, the findings align with the ethical considerations of environmental protection discussed in the theory of just war, which holds that military operations should avoid unjustified or disproportionate destruction of natural values. Due to the ongoing conflict and the country's infrastructural conditions, on-site investigations are unlikely in the future, and further research will primarily rely on remote analyses.

Keywords

impact crater, Ukraine, Russian-Ukrainian war, just war, environmental damage

Absztrakt

A tanulmány az Ukrajnában található 8 meteoritkráter természeti és művi környezetének esetleges háborús károsodását vizsgálja. A kutatás célja volt feltárni, hogy a rendelkezésre álló primer és szekunder adatforrások alapján kimutatható-e környezetkárosítás. A vizsgálat során meteoritikai adatbázisokat, szakirodalmi forrásokat, valamint térképes műhold- és légifelvételeket elemeztek a konfliktus előtti és alatti állapot összehasonlítására. Az eredmények azt mutatják, hogy a kráterek eddig sértetlenek maradtak, háborús környezetkárosításra utaló jelek nem azonosíthatók. Ha nem is tudatos cselekvés folytán, de a vizsgálat eredményei összhangban állnak az igazságos háború elméletében tárgyalt környezeti károkozás etikai megfontolásaival, amelyek szerint a katonai cselekményeknek kerülniük kell a természeti értékek indokolatlan, aránytalan pusztítását. A jövőben a háborús következmények és az ország infrastrukturális állapota miatt helyszíni vizsgálatok nem valószínűek, ezért a további kutatások is elsősorban távoli elemzésekre támaszkodnak.

Kulcsszavak

impakt kráter, Ukrajna, orosz–ukrán háború, igazságos háború, környezetkárosítás

[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

A téma bemutatása

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 ukrajnai meteoritkráterek esetleges háborús környezetkárosítását.

Tágabb értelemben tematikája a környezeti károkozással összefüggésben kapcsolódik az igazságos háború elméletéhez. Rámutatva és hangsúlyozva, hogy ezek a képződmények a természeti környezethez, sőt, az emberi élethez hasonlóan, nem csupán egy-egy hadviselő ország, hanem abszolút értelemben az emberiség számára is értéket jelentenek.

Szűkebb fókusza az ukrajnai meteoritkráterek esetleges háborús behatásainak vizsgálata. Kitér számosságukra, klasszifikációjuk ellentmondásaira, főbb földrajzi és földtani paraméterükre. Vizsgálat tárgyává teszi, hogy kimutatható-e bármilyen bekövetkezett változásuk, és történhetett-e esetlegesen környezetkárosításuk. A *Biztonságtudományi Szemle* mostani számában ennek eredményeit foglalja össze.

A témaválasztás indoklása

A 45 m átmérőjű egyiptomi Kamil impakt krátert [8] 2020 és 2023 között [5] vasmeteorit-zsákmány reményében meteoritvadászok pusztították el [3] (1. Ábra). A meteoritok felkutatására földmunkagépeket használtak [5], a pusztítás jelentős mértéke és helyrehozhatatlan környezetkárosítása főként ennek köszönhető. Mivel a Kamil alig több, mint 500 m-re húzódik a szudáni határtól (az ottani földrajzi távolságokat figyelembe véve Líbia is mindössze 110 km-re fekszik), elpusztításában informális híresztelések szerint komoly szerepe lehetett a meteoritvadászok által korrumpált határőrizetet ellátó egyiptomi hadsereg állományának is.

1. Ábra: A környezetkárosítás során 2020–2023 között elpusztított egyiptomi Kamil impakt kráter, https://lunarmeteoritehunters.blogspot.com/2024/10/kamil-crater-egypt-strip-mined-and.html

Ukrajnában az Oroszországgal vívott háborút megelőzően merült fel a 2017-ben természetvédelmi oltalom alá helyezett [6] Ilyinets kráter turisztikai hasznosítása. 2020-ban geohelyszínként való megjelenítésére részletes szakmai tervjavaslat készült [2 pp. 664–671.]. A konfliktus földrajzi eszkalálódásával joggal merül fel, hogy az igazságos háború elmélete elviekben szorosan összefügg a környezetkárosítás okozásának korlátozásával [1 p. 123.]. Ugyanakkor meg kell állapítani, hogy az eddigi háborús szembenállások során az

igazságos háború teoretikusai és a háború filozófusai kevés figyelmet fordítottak a környezeti katonai etikára [7 p. 399.]. Éppen ezért igényelnek kiemelt figyelmet az ukrajnai természeti képződmények, így a becsapódási kráterek is.

A téma lehatárolása

A téma időbeli lehatárolásának kezdete értelemszerűen megelőzi az Oroszország Ukrajna elleni inváziójának 2022. február 22-i megindítását. Ez az időközben már történelmi/hadtörténeti jelentőségűvé vált esemény emberi időskálán értelmezett. A vizsgálatba bevont impakt kráterek léte ugyanakkor földtörténeti távlatokban mérhető, de természetvédelmi aspektusban a hadműveletek előtti állapotukra alapoz. A szakmai dolgozat időbeli végét a kutatás befejezésének, illetve jelen cikk kéziratának 2025. november 11-i lezárása jelenti.

Földrajzi viszonylatban a vizsgálat kereteit az Ukrajna hivatalos államhatárain belül található 8 becsapódási kráter természeti és (infrastruktúrákkal települt) művi környezete jelenti.

AZ UKRAJNAI METEORITKRÁTEREK ESETLEGES HÁBORÚS KÖRNYEZETKÁROSÍTÁSÁNAK VIZSGÁLATA

Tudományos probléma, elérendő célok, alkalmazott módszerek

A témaválasztás indoklásában említett globális déli Egyiptomban bekövetkezett esemény felveti annak a lehetőségét, hogy a háborúval sújtott (európai dimenziójú elmaradottsága ellenére a globális északhoz sorolt) Ukrajna területén ugyancsak veszélyeztetettek ezek a meteoritikus eredetű természeti formációk. Mivel szomszédunk világszintű összehasonlításban is az egyik legtöbb kráterrel rendelkező ország, így az itt folyó harcok okán a környezetkárosítás esélye valós tudományos probléma.

A vizsgálatok célkitűzése kettős. Elsőként meg kell állapítani, hogy a kráterek pusztulására vonatkozóan a megadott adatforrásokból kinyerhetők-e egyáltalán információk. Amennyiben igen, akkor második körben ezek mértékének meghatározása és dokumentálása a célkitűzés.

A kutatás során alkalmazott módszerek a következők voltak: Meteoritikai adatbázisok primer adatainak áttekintése. Szekunder meteoritikai szakirodalmi vonatkozások keresése. A Mapy.com, a Google Earth Pro és a Google Térkép állományainak elemzése. Ennek során megkutatásra kerül, hogy van-e olyan térképszelvény, illetve ezekbe integrált fotódokumentáció, amelynél egyaránt megtalálható háború alatti, illetve a háborút megelőző műholdfelvétel, illetve in situ készített fénykép.

Alapfogalmak

- 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.

- 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.
- Krátermező: Kisbolygó- / meteoritbecsapódás során az égitest darabjai által egyidejűleg létrehozott kráterek csoportja.
- Környezetkárosítás: Tevékenység vagy mulasztás, amely a környezetben vagy annak valamely elemében közvetlenül vagy közvetve mérhető, jelentős kedvezőtlen változást idéz elő.
- Igazságos háború: Erkölcsileg elfogadható hadviselés, melyet jogtalan agresszió ellenében, vagy jogos okból, a béke helyreállítása érdekében, az erkölcsi korlátokat betartva vívnak.

Vizsgálatba bevont objektumok

A meteoritkrátereknek a nemzetközi szakmai közösség által egyöntetűen elfogadott nyilvántartását jelentő Earth Impact Database adatai szerint Ukrajna területén 8 asztroblém található (1. Táblázat). Ezzel a számossággal szomszédunk a Föld azon 8 országa között szerepel, ahol a legtöbb asztroblém található (2. Táblázat).

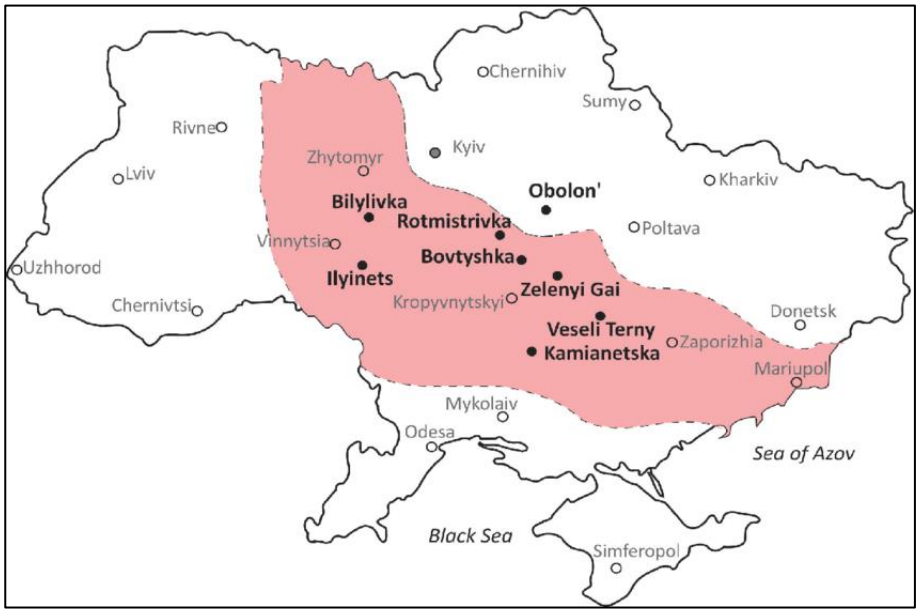
Impakt kráter neve [8]	**Földrajzi szélesség**	**Földrajzi hosszúság**	**Átmérő (km)** [8]	**Eltemetett** [8]
Boltysh	é. sz. 48° 45’ [8] é. sz. 48° 54’ [6]	k. h. 32° 10’ [8] k. h. 32° 15’ [6]	24	igen
Ilyinets	é. sz. 49° 7’ [8]	k. h. 29° 6’ [8]	8,5	igen
Kamenetsk	é. sz. 47° 46’ [8] é. sz. 47° 46’ [4]	k. h. 32° 21’ [8] k. h. 32° 21’ [4]	1,2	igen
Obolon’	é. sz. 49° 35’ [8] é. sz. 49° 35’ [6]	k. h. 32° 55’ [8] k. h. 32° 55’ [6]	20	igen
Rotmistrovka	é. sz. 49° 0’ [8] é. sz. 49° 8’ 50” [6]	k. h. 32° 0’ [8] k. h. 31° 42’ 30” [6]	2,7	igen
Ternovka	é. sz. 48° 8’ [8] é. sz. 48° 8’ [6]	k. h. 33° 31’ [8] k. h. 33° 31’ [6]	11	igen
Zapadnaya	é. sz. 49° 44’ [8] é. sz. 49° 40’ 8” [6]	k. h. 29° 0’ [8] k. h. 29° 0’ 49” [6]	3,2	igen
Zeleny Gai	é. sz. 48° 4’ [8] é. sz. 48° 53’ [6]	k. h. 32° 45’ [8] k. h. 32° 48’ [6]	3,5	igen

1. Táblázat: Az ukrán meteoritkráterek listája fontosabb paramétereikkel az Earth Impact Database adatai, valamint helyi források alapján (2025.11.04-ig), [4;6; 8] – saját szerkesztés

Ország neve	Impakt kráterek száma (db)
Kanada	31
Ausztrália	30
Egyesült Államok	30
Oroszország	19
Finnország	12
Brazília	8
Svédország	8
Ukrajna	**8**

2. Táblázat: A legtöbb impakt kráterrel rendelkező országok az Earth Impact Database adatai alapján (2025.11.02-ig), [8] – saját szerkesztés

Az országon belül a kráterek szinte kivétel nélkül a hatalmas kiterjedésű ősföld, az Ukrán-pajzs területére esnek. A nagyságrendileg 200 000 km^2-es ősmasszívum őrizte meg a földtörténeti múlt impakt eseményeinek lenyomatát (2–3. Ábra). Ennek megfelelően kőzetanyaguk vagy kristályos, vagy a kristályos aljzat feletti üledékes [8].



2. Ábra: Az ukrán impakt kráterek országon belüli földrajzi elhelyezkedése – rózsaszínnel jelölve az Ukrán-pajzs kiterjedése, [2 p. 659]

3. Ábra: Ukrajna földtani felépítése – sárgával jelölve az Ukrán-pajzs, Alex Tora, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

Mivel a mértékadó források is ellentmondásosak, az ukrajnai kráterek klasszifikációja és pontos száma kérdéseket is felvet. Az Earth Impact Database egész Földre kiterjedő listája 8 objektumot közöl [8] (2. Táblázat). Az adatbázis külön európai listája azonban csak 7-et ismer – ebből a Kamenetsk hiányzik. Feltételezhetően azért, mert ezt ismerték fel legutoljára: 2004-ben fedezték fel azt a negatív gravitációs anomáliát, amit 2006-ban végül becsapódási kráterként írtak le és publikáltak [4 p. 2461]. Vélhetően hibás adatrögzítés miatt a Kamenets az Ázsia és Oroszország közös adatbázisrészben található [8] – függetlenül attól, hogy az asztroblém földrajzilag nem az orosz megszállás alatt levő területre esik. Az impakt kráter felfedezésének friss volta lehet a magyarázata, hogy az Earth Impact Database adatait is integráló, a földi meteoritok paramétereit hivatalosan összefoglaló Meteoritical Bulletin Database a becsapódási kráterekre való szűrésre (szintén a Kamenetsk kihagyásával) ugyancsak 7 ukrán asztroblémet listáz [12].

Problémát jelent a vizsgálatba bevont objektumok kutatásában, hogy nemcsak az ismeretterjesztő, de a szakmai forrásokban, valamint a térképi állományokban is a kráterek hivatalos elnevezésétől gyakorta eltérnek. Ennek fő oka a cirill betűk használata, valamint az önálló ukrán nyelvhasználatra való törekvés.

A földrajzi koordináták a mértékadó adatbázisokban mindössze ívperces pontossággal vannak megadva, ezért a térképszelvények áttekintése fokozott figyelmet igényel. Ukrajnai források szolgálnak egyes esetekben pontosabb, ívmásodperces bontású adatokkal. Ennek további aspektusa, hogy a földrajzi koordináták esetén nem evidens, hogy az a kráter középpontjára vonatkoztatott-e, vagy sem.

Azonosításukat megnehezíti az is, hogy meteoritikai szakirodalmi adatok alapján az ukrán asztroblémek eltemetettek [8], struktúrájuk zöme (kráterperem, központi csúcs stb.) a földfelszín alatt helyezkedik el.

Adatforrások elemzése, értékelése

A Boltysh meteoritkráter:

A jelentős kiterjedésű, 24 km átmérőjű becsapódási kráter eltemetett [8]. A felszínen létezésére depresszió utal. A kráter középpontjában, Bovtyshka faluban horgásztavak találhatók [6]. A jelen vizsgálat ezekre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2020. augusztus 18-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

4. Ábra: A Boltysh meteoritkráter háború időszakára eső, 2024 májusi állapota, https://maps.app.goo.gl/LMvFngJfxyAeRKyt7 [Letöltés: 2025.11.09.]

A Google Térkép [10] fotói és videói között a legfrissebb 2024 májusi, a háború időszakára eső (4. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy a Boltysh meteoritkráter eddig az időpontig sértetlen.

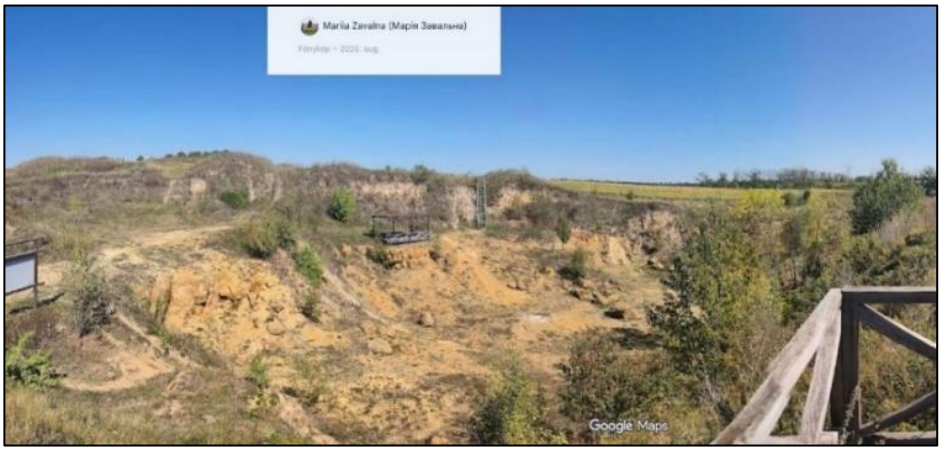
A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

Az Ilyinets meteoritkráter:

A jelentős kiterjedésű, 8,5 km átmérőjű becsapódási kráter eltemetett [8]. A természetes erózió és korábbi antropogén hatások révén kihantolt szegmensei Luhova községben tanulmányozhatók a felszínen [6]. A jelen vizsgálat ezekre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. október 19-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

5. Ábra: Az Ilyinets meteoritkráter háborút megelőző, 2021 októberi állapota, https://maps.app.goo.gl/NwYnC2dwSvKQpiPj9 [Letöltés: 2025.11.07.]



6. Ábra: Az Ilyinets meteoritkráter háború időszakára eső, 2025 augusztusi állapota, https://maps.app.goo.gl/iT5KhD1oh3WLwE3HA [Letöltés: 2025.11.07.]

A Google Térkép [10] fotói és videói között a legfrissebb 2025 augusztusi, a háború időszakára eső (5–6. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy az Ilyinets meteoritkráter eddig az időpontig sértetlen.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Kamenetsk meteoritkráter:

Az 1,2 km átmérőjű becsapódási kráter eltemetett [8]. A kráter Kam'yane falu mellett található. A jelen vizsgálat erre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. április 5-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

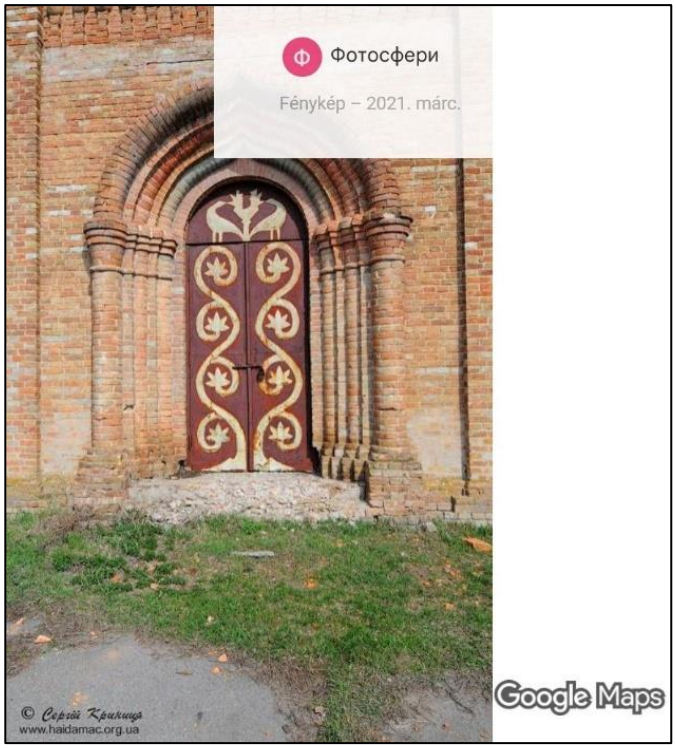
A Google Térkép [10] nem közöl a területről fotót vagy videót. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

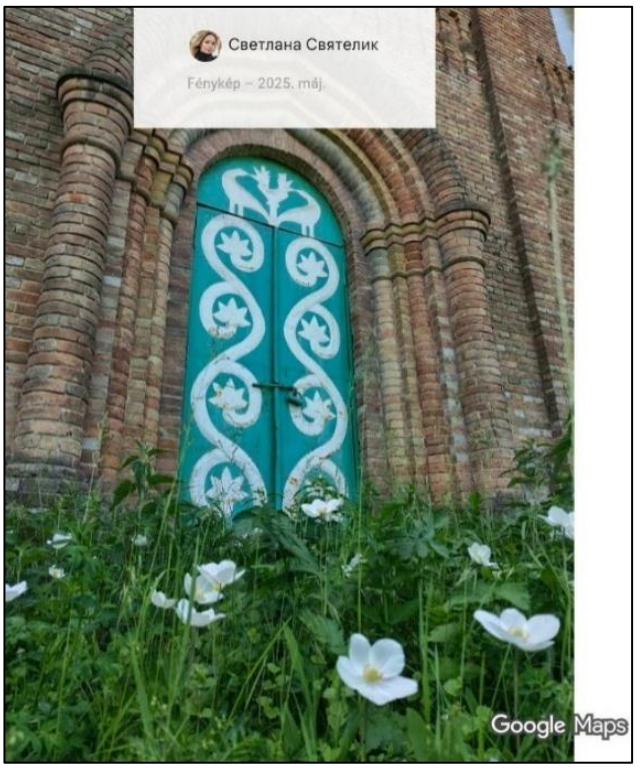
Az Obolon' meteoritkráter:

A jelentős kiterjedésű, 20 km átmérőjű becsapódási kráter eltemetett [8]. A kráter középpontjában a Hrakove vadrezervátum található. A kráter területén, Obolon' községben, valamint a környező településeken kórház, bevásárlóközpont, élelmiszerbolt, étterem, autószervíz, posta, sportpálya, kulturális központ és szakrális civil infrastruktúrák települnek. A jelen vizsgálat ezekre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. november 23-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.



7. Ábra: Az Obolon' meteoritkráterben található civil infrastuktúra háborút megelőző, 2021 márciusi állapota, https://maps.app.goo.gl/yUA4XHur72KzfqL36 [Letöltés: 2025.11.09.]



8. Ábra: Az Obolon' meteoritkráterben található civil infrastuktúra háború időszakára eső, 2025 májusi állapota, https://maps.app.goo.gl/BeizJ8wUf2iuuRYm8 [Letöltés: 2025.11.09.]

A Google Térkép [10] fotói és videói között a legfrissebb 2025 májusi, a háború időszakára eső (7–8. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy az Obolon' meteoritkráter eddig az időpontig ebben a tekintetben sértetlen.

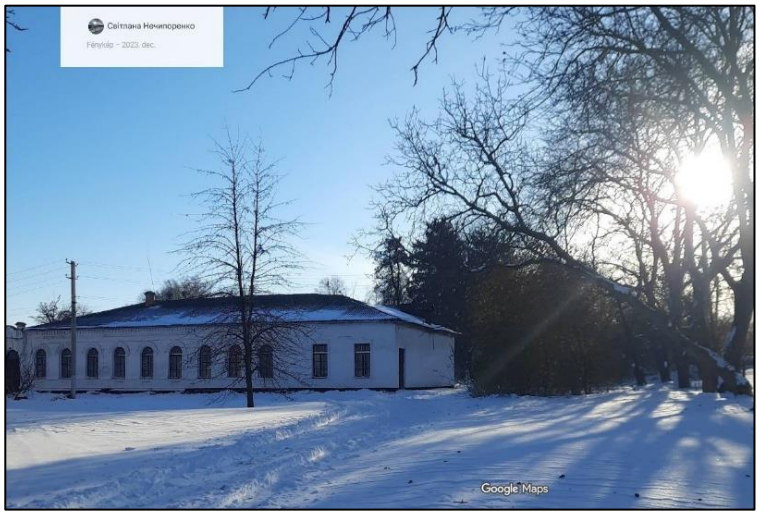
A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Rotmistrovka meteoritkráter

A 2,7 km átmérőjű becsapódási kráter eltemetett [8]. A felszínen létezésére depresszió utal [6]. A kráter középpontjában/területén, Rotmistrivka községben kisgépes repülőtér, élelmiszerbolt, autóalkatrész-bolt, posta, általános- és középiskola, zeneiskola civil infrastruktúrák településnek. A jelen vizsgálat ezekre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. október 8-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

9. Ábra: Az Rotmistrovka meteoritkráterben található civil infrastuktúra háborút megelőző, 2021 decemberi állapota, https://maps.app.goo.gl/RAjzM1Z6jSnP6XaT8 [Letöltés: 2025.11.09.]



10. Ábra: Az Rotmistrovka meteoritkráterben található civil infrastuktúra háború időszakára eső, 2023 decemberi állapota, https://maps.app.goo.gl/nmRmTQQUMTbeFEMF8 [Letöltés: 2025.11.09.]

A Google Térkép [10] fotói és videói között a legfrissebb 2024 októberi, a háború időszakára eső (mivel ezen magánszemélyek is látszanak, ezért itt egy 2023 decemberi felvétel szerepel) (9–10. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy az Rotmistrovka meteoritkráter eddig az időpontig ebben a tekintetben sértetlen.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumokról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Ternovka meteoritkráter

A jelentős kiterjedésű, 11 km átmérőjű becsapódási kráter eltemetett [8]. A kráter szinte teljes területén, Krivij Rih város Terny településrészén vasércbánya civil infrastruktúra települ [6]. A jelen vizsgálat erre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. július 5-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

11. Ábra: A Ternovka meteoritkráterben található civil infrastuktúra háborút megelőző, 2021 márciusi állapota (jelentős mértékű bányászati környezetkárosítással), https://maps.app.goo.gl/QSc76q7LbR1YEdwN9 [Letöltés: 2025.11.09.]

12. Ábra: A Ternovka meteoritkráterben található civil infrastuktúra háború időszakára eső, 2025 augusztusi állapota (jelentős mértékű bányászati környezetkárosítással), https://maps.app.goo.gl/sMobAjNkE2Cy5uHy8 [Letöltés: 2025.11.09.]

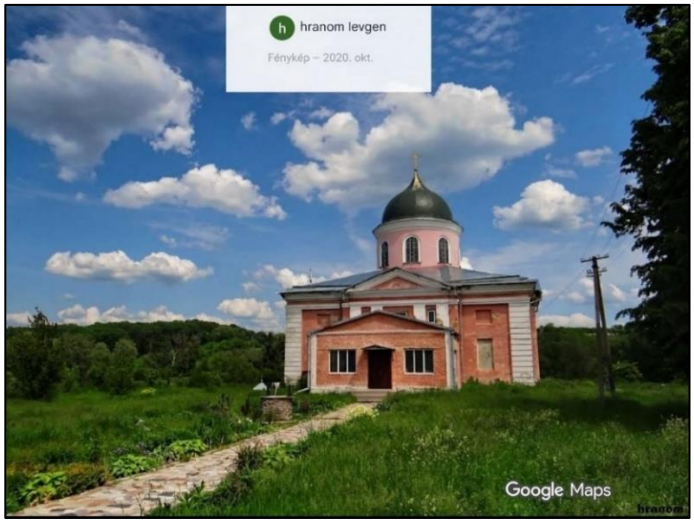
A Google Térkép [10] fotói és videói között a legfrissebb 2025 augusztusi, a háború időszakára eső (11–12. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy a Ternovka meteoritkráter eddig az időpontig ebben a tekintetben sértetlen. Ugyanakkor a jelentős volumenű külszíni bányászati kitermelés miatt negatív környezeti hatás.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumokról. A környezetkárosítás vizsgálata nem lehetséges.

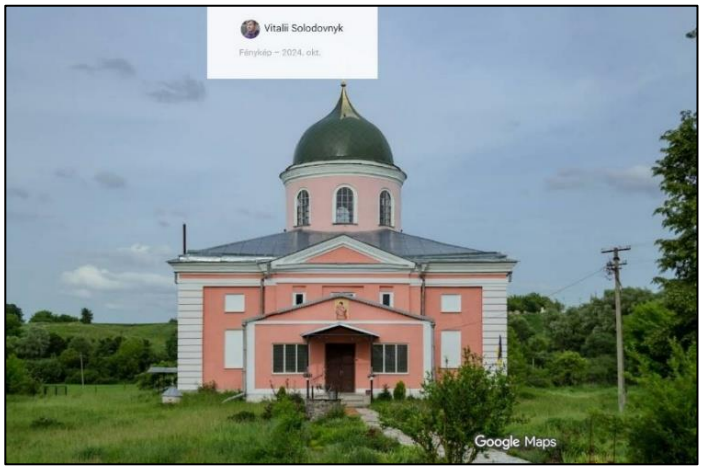
A Zapadnaya meteoritkráter

A 3,2 km átmérőjű becsapódási kráter eltemetett [8]. A kráter középpontjában, a Rostavytsia-folyó mellett erdős terület található. A kráter területén, Bilyvlika faluban élelmiszerbolt, posta, óvoda és szakrális civil infrastruktúrák településnek. A jelen vizsgálat ezekre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2019. október 19-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.



13. Ábra: A Zapadnaya meteoritkráterben található civil infrastuktúra háborút megelőző, 2020 októberi állapota, https://maps.app.goo.gl/9FWMc52B1Szk2JZq5 [Letöltés: 2025.11.09.]



14. Ábra: A Zapadnaya meteoritkráterben található civil infrastuktúra háború időszakára eső, 2024 júniusi állapota, https://maps.app.goo.gl/vskuQMrhAFwBRZnD7 [Letöltés: 2025.11.09.]

A Google Térkép [10] fotói és videói között a legfrissebb 2025 júniusi, a háború időszakára eső (13–14. Ábra). Háborús eredetű környezetkárosításra utaló képi információt nem tartalmaz; megállapítható, hogy az Zapadnaya meteoritkráter eddig az időpontig ebben a tekintetben sértetlen.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Zeleny Gai meteoritkráter

A 3,5 km átmérőjű becsapódási kráter eltemetett [8]. A Zeleny Gai esetében a szakirodalmi források a nagyobbik objektum mellett említést tesznek egy kisebb, 800 m-es ikerasztroblémről is, így valójában egy krátermezőről beszélhetünk [6]. A jelen vizsgálat erre terjedt ki.

A Google Earth Pro [9] optimális áttekintést nyújtó, 1 km szemmagasságú műholdas felvételei közül a legutolsó állomány 2017. május 2-i, a háborút megelőző. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Google Térkép [10] nem közöl a területről fotót vagy videót. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

A Mapy.com [11] légi- és műholdas felvételeinek készítési időpontjára vonatkozóan nincs adat, valamint nem közöl fotót az objektumról. Háborús eredetű környezetkárosítás vizsgálata nem lehetséges.

ÖSSZEFOGLALÁS

Összegzett következtetések

Az ukrajnai meteoritkráterek esetleges háborús behatásait felmérve szomszédunk hivatalos államhatárain belül 8 becsapódási kráter természeti és művi környezetének vizsgálata történt meg. Megállapítható, hogy a primer és szekunder adatforrásokból zömében kinyerhetők voltak a keresett információk. A vonatkozó meteoritikai adatbázisok (főképp a Earth Impact Database), valamint a témában feltárt szakcikkek kellő alapot biztosítottak mindehhez.

A vonatkozó műholdas és légifelvételeken nyugvó térképes állományok vizsgálata során pedig megállapítható volt, hogy a Google Earth Pro térséget lefedő felvételei a háború kezdete óta nem frissültek. Ugyanakkor a Google Térkép fotógyűjteménye lehetőséget biztosított ugyanazon földrajzi/infrastrukturális egység orosz–ukrán konfliktus előtti, majd háborús időszaki összehasonlítására.

A becsapódási kráterek döntő többségénél megtörténhetett ez a vizsgálat. Megállapítható, hogy háborús eredetű környezetkárosításra utaló eset nem történt. Ugyanakkor ebben nem az igazságos háború elméletének egyik alapvetése, a környezeti katonai etika érvényesülése játszotta a főszerepet, hanem az, hogy a hadműveletek szerencsés módon elkerülték ezeket az extraterresztrikus hatásra képződött, a teljes Földet figyelembe véve is ritka, tudományos szempontból kiemelkedő fontosságú objektumokat. A vizsgálatok ilyen vonatkozásban rámutattak arra is, hogy az erőforrásigényeket kielégítő bányászat jelentős negatív környezeti terhelést jelent még békeidőben is.

A további kutatás tervezett irányai

Az ukrajnai impakt kráterekre vonatkozó helyszíni vizsgálatokat a jelenlegi háború kapcsán fennálló gyakorlati nehézségek, valamint a biztonság hiánya lehetetleníti el. A várt békemegállapodást követő rövid időintervallumon belül sem valószínű, hogy a leromlott infrastruktúrájú országban az in situ terepi munka lehetővé válik. Éppen ezért kiemelten fontos, mind a releváns szakirodalom nyomon követése, mind az időről időre frissülő műholdas és légi térképi adatok, valamint fotódokumentációk vizsgálata.

Az idézett egyiptomi kráter esete mutatja, hogy lakott területektől távol ennek segítségével is tetten érhető a környezetkárosítás. Ennek eredményeképp egy hasonló jellegű jövőbeni ukrajnai antropogén károkozás esetén tájékoztatható a szakterület közössége, valamint riaszthatók a környezet- és természetvédelemért felelős helyi, országos, továbbá nemzetközi hatóságok és szervezetek.

FELHASZNÁLT IRODALOM

[1] Boda M., Az igazságos háború elmélete és a teremtésvédelem: az igazságos háború elméletének története a középkortól a 20. századig a teremtésvédelem szempontjából, *Hadtudományi Szemle*, 16, 4, 2023, pp. 123–137.

[2] Derevska, K. et al., The Ilyinets meteorite crater – unique geological structure in Europe and a promising destination for international tourism, *Journal of Geology Geography and Geoecology*, 29, 2020, pp. 656–672.

[3] Folta, A., Destruction of the Gebel Kamil Crater: A Loss for Science and Collectors, *Meteorite Club*, 2024. [Online]. Elérhető: https://meteoriteclub.com/meteorite-news/destruction-of-the-gebel-kamil-crater-a-loss-for-science-and-collectors/ [Letöltés: 2025.11.02.]

[4] Gurov, E. et al., Kamenetsk – A new impact structure in the Ukrainian Shield, *Meteoritics & Planetary Science*, 52, 12, 2017, pp. 2461–2469.

[5] Heinrich, P.V., Kamil Crater, Egypt, „Strip-mined" and Destroyed by Meteorite Criminals, *The Latest Worldwide Meteor/Meteorite News*, 2024. [Online]. Elérhető: https://lunarmeteoritehunters.blogspot.com/2024/10/kamil-crater-egypt-strip-mined-and.html [Letöltés: 2025.11.02.]

[6] Khymera, B., Catastrophe remnants: Where meteorite craters are preserved in Ukraine, *Universe Space Tech*, 2024. [Online]. Elérhető: https://universemagazine.com/en/catastrophe-remnants-where-meteorite-craters-are-preserved-in-ukraine [Letöltés: 2025.11.03.]

[7] Meisels, T., Environmental Ethics of War: Jus ad Bellum, Jus in Bello, and the Natural Environment, *Conatus*, 8, 2, 2023, pp. 399–429.

[8] *Earth Impact Database*, Planetary and Space Science Centre, 2025. [Online]. Elérhető: http://www.passc.net/EarthImpactDatabase/New%20website_05-2018/Index.html [Letöltés: 2025.11.02.]

[9] *Google Earth Pro*, Google, 2025. [Letöltés: 2025.11.07.]

[10] *Google Térkép*, Google, 2025. [Online]. Elérhető: https://www.google.hu/maps [Letöltés: 2025.11.07.]

[11] *Mapy.com*, Seznam.cz, a.s., 2025. [Online]. Elérhető: https://mapy.com [Letöltés: 2025.11.07.]

[12] *Meteoritical Bulletin Database*, The Meteoritical Society, 2025. [Online]. Elérhető: https://www.lpi.usra.edu/meteor/ [Letöltés: 2025.11.02.]

DOI: https://doi.org/10.12700/btsz.2025.7.4.95

STEGANOGRAPHIC MODELS AND TECHNICAL APPROACHES TO ENCRYPTING DATA EMBEDDED IN IMAGES

SZTEGANOGRÁFIAI MODELLEK, KÉPBE INTEGRÁLT ADATOK TITKOSÍTÁSA ÉS TECHNIKAI MEGKÖZELÍTÉSE

OLÁH Róbert[1] – LŐCSEI Anikó[2]

Abstract

The review of image encryption techniques aims to examine the computer-based analysis of digital images, as well as the theoretical and practical implementation of procedural methods. Image encryption methods are explored with regard to automated image analysis, noise reduction techniques, edge detection, and image classification. The presentation of imaging models related to these methods is interpreted through the analysis of image processing algorithms. The primary research focus is on the depiction of applied code snippets and models that contribute to the practical understanding of the presented methods. The functionality of encrypting data within images is demonstrated through various algorithms, which illustrate not only traditional techniques but also modern machine learning-based approaches. The objective of the research is to demonstrate, based on steganographic image encryption methods, how image processing algorithms facilitate the encryption of information within images, and to contribute to the future development of encryption techniques by introducing the latest research topics.

Keywords

steganography, image encryption, digital image processing, edge detection, noise reduction

Absztrakt

A képtitkosítási technikák vizsgálata a digitális képek számítógépes elemzését, az eljárási technikák elméleti és gyakorlati megvalósításának bemutatását célozza. A képtitkosítási módszerek az automatizált képelemzést, zajszűrési technikákat, a kép éleinek detektálását és képosztályozási technikák elemzését ismertetik. A módszerekhez kapcsolódó képalkotó modellek bemutatása a képfeldolgozó algoritmusok elemzésével értelmezhető. Az elsődleges kutatási szempontok azok az alkalmazott kódrészletek, illetve modellek ábrázolása, amelyek a bemutatott módszerek gyakorlati értelmezéséhez járulnak hozzá. A képben szereplő adatok titkosításának működőképességét szemléltetik a különféle algoritmusok, amelyek, a hagyományos módszerekkel szemléltetik a modern gépi tanuláson alapuló megközelítéseket is. A kutatás célja a szteganográfiai képtitkosítási módszerek alapján bemutatni, hogy a képfeldolgozó algoritmusok alkalmazásával hogyan válik lehetővé a képben lévő információk titkosítása, legújabb kutatási témák ismertetésével hozzájáruljon a titkosítási eljárások jövőbeli fejlesztéséhez.

Kulcsszavak

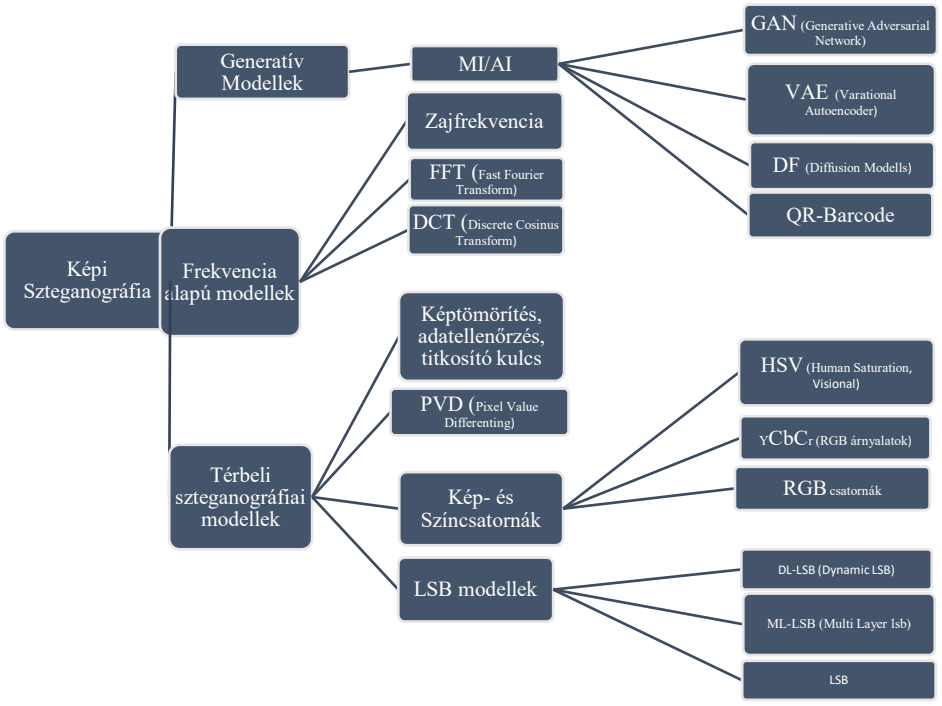
szteganográfia, képtitkosítás, digitális képfeldolgozás, élkiemelés, zajcsökkentés

[1] olah.robert@eotvostechnikum.hu | ORCID: 0009-0007-9134-9521 | IT teacher, Educational Center of Érd | Informatika oktató, Érdi Tankerületi Központ

[2] locsei.aniko@bparchiv.hu | ORCID: 0009-0005-7070-1982 | chief archivist, Budapest City Archives | főlevéltáros, Budapest Főváros Levéltára

BEVEZETÉS

A kezdetlegesen alkalmazott, de jelen időben már generatív technikával is rendelkező képtitkosítási eljárás a digitális adatvédelem és biztonsági során is jelentős szerepet kap. Az adatbiztonság fontosságával a képek titkosítási technikái és a digitális információk védelmének kutatási területei folyamatosan frissülnek. A technológiai területeken megvalósuló fejlődés lehetővé teszi a folyamatosan fejlődő gépi tanulás alkalmazásával szükségessé vált hagyományos és a kortárs képtitkosítási technológiák időrendszerű vizsgálatát. A képi információk titkosítási módszereinek áttekintésével lehetővé válik a modellek elméleti és gyakorlati megközelíthetősége és a képek biztonságos adatkezelése. A képek információbiztonsági szerepe és a digitális adatvédelem hozzájárul a szteganográfiai modellek új fejlesztéséhez és technológiai megoldásához. A mellékelt ábra alapszintektől a felső szintekig ismerteti a képi rejtési technikákat és a hierarchia felső szintjén lévő Mesterséges Intelligencia generatív modelljeit, ahol az intelligens adatbeágyazású MI/AI képbe integrált információk beágyazását ismertetjük. A térbeli módszerek során a Least Significant Bit (LSB), annak továbbfejlesztett rétegelt, multi layer ML-LSB és az adatptív dinamikus LSB modellek elemezzük. A térbeli modelleket kiegészítjük a kép-és színcsatornák váltakozási, a képpont módosítási eljárással a Pixel Value Differencing-gel (PVD). A frekvenciaalapú technikák alkalmazása mellett a koszinusz-függvény alapú Discrete Cosine Transform (DCT) és a Fourier alapú transzformációs modellek zaj- és frekvencia alapú megközelítését és a mindennapok során használt QR-Barcode képen belüli adatok vonalkód, vagy leolvasási technikát is bemutatjuk.



1. Ábra: a tanulmányban szereplő modellek folyamatábrája LSB legalsó szintjeitől a Generatív-AI modellekig, saját szerkesztés

A SZTEGANOGRÁFIA EREDETE FELHASZNÁLÁSI TERÜLETEI

A képi információk elrejtésének korai technikái és fejlődése

A szteganográfia szó elsődleges források szerint görög eredetű *s*tegein *„**στεγεῖν**”* igéből származik, melynek jelentése, hogy "fedni, rejteni", míg a szintén görög eredetű graphē *„γραφή”* szó a leíró tudományok általános neve, és azt jelenti, hogy "írni"[1]. Hérodotosz, görög történetíró nyomán feljegyzett történet a fogvatartott Demaratosz, spártai király nevéhez köthető. A perzsák általi hadműveletről, nyílt üzenetet nem küldhetett. Xerxész, perzsa király általi támadás hírét egy fatáblára vésve juttatta el, amelyet viasszal fedett le. A táblán lévő üzenet a hő hatására lett látható[2]. A kommunikáció fejlődésével új lehetőségek nyíltak meg az adatok képi titkosításához. A papiruszt felváltó pergamen új távlatokat jelentett a steganogramok elrejtéséhez, amely a szteganográfiai algoritmusok létrejövetelét eredményezte. A Kínában feltalált vízjelezett papírt, amely egyfajta eredet-hitelesítési és hamisítás elleni védelmi szerepet töltött be, Európa céhes iparágaiban és kereskedelmi forgalomban vagy okleveleken használták. A középkori módszerek közé tartozott az akrosztichon, a rejtett üzeneteket sorok vagy fejezetek kezdőbetűi tartalmazták. Az ipari forradalom idején újabb kommunikációs formák, az újságok töltötték be a titkos adathordozók szerepét, újságkódok nyomán lyukasztással emelték ki a betűket. A 20. század háborús időszakában a szteganográfia jelentős változáson ment keresztül. Az első világháború során az ún. láthatatlan tinták használata jelentette képi titkosítást, amelyek speciális vegyszerek, fényforrás segítségével váltak olvashatóvá. A második világháború során továbbfejlesztették a módszert mikrofilmek és azok mikro pontjainak használatával, amelyeken kisméretű üzeneteket rejtettek el. Katonai hírszerzés eszközeként szabad szemmel nem voltak láthatók az információk.[3] A szteganográfiát leginkább katonai parancsok, diplomáciai információk és kémkedési adatok elrejtéséhez használták információbiztonsági alapon, a szembenálló fél megtévesztéséhez. Az alábbi műszerek a képi információ kezelésének és vizualizációjának történeti előzményeit szemléltetik, a képi információk mechanikai adatfeldolgozásától a digitális grafikus rendszerekig.

2. Ábra: Lyukkártya és leolvasókészülék (IBM, 1950-1960):A képi információ kódolásának korai formája, ahol az adat mintázatban jelent meg, MKKM Műszaki Tanulmánytár, saját kép

3. Ábra: Telesis grafikus munkaállomás (Angliai modell Elektronikus Mérőkészülékek Gyára, 1985): A munkaállomás (1980) a CAD-CAM szoftverek és a digitális plotterek segítségével precízen kezelte a képi adatokat, lehetővé téve azok manipulálását, hogy az információk rejtett módon kerüljenek beágyazásra a digitális képekbe, MKKM Műszaki Tanulmánytár, saját kép

A képi adatok titkosítása és a mesterséges intelligencia (MI/AI- generatív modellek)

A létező szteganográfiai rendszerek a szöveg (PDF), a hang (visszhang alapú módszer), illetve a hálózati (IP fejlécekben rejtett információ) alapú eljárások közül jelen tanulmányban a képi szteganográfiai modelleket ismertetjük. A képi szteganográfia módszere eltérő a szintén rejtett információátadási technikával, a kriptográfiával, amely az üzenet értelmezhetőségét védi, annak visszafejtése egy megfelelő kulccsal lehetséges. A szteganográfia egy látható képen belül magát az üzenetet rejti el, legfőbb célja, hogy az információt semmilyen eszközzel ne lehessen azonosítani. A folyamat hatékonyságát az alábbi tényezők alapján korábbi kutatások és a mai gyakorlat is figyelembe vesz:

- **láthatósági intenzitás** (PER), amely a rejtett adat észlelhetőségét jelzi, túl sok adat beágyazásánál a kép minősége romlik
- **felfedhetőség** (DET), amely a képben titkosított adatok észlelhetőségét jelenti
- **erősségi faktor** alapján (STR), amely a képek feldolgozása során való sértetlenségét és tartósságát biztosítja
- **kompatibilitás** (COMP) és a **fájlformátum-függőség** (DEP) olyan tényezők, amelyek a titkosítás módszereinek alkalmazhatóságát és a képi formátumok közötti eltéréseket is figyelembe veszik
- **domain típus** (DOM) meghatározza, hogy az információk a képen térbeli vagy transzformációs tartományban kerülnek elrejtésre, ami különböző biztonsági szintet biztosít

A képbe ágyazott információ a kivonási folyamat során visszaállíthatjuk megfelelő kulcs, vagy algoritmusok alkalmazásával. Bizonyos rendszerek automatikus titkosítási módszert alkalmaznak, így az üzenet is titkosítottá, illetve visszafejthetővé válik.[4]

A mesterséges intelligencia képi alkotások algoritmusa

A mesterséges intelligencia napjaink egyik legfontosabb fejlődési területe. A mesterséges intelligencia alkalmazások már részben az életünk részévé vált. Ebben a publikációban azokat az algoritmusokat tárgyaljuk, amely alkalmazható a digitális képfeldolgozásra, amely hatással van a képi objektumok felismerésére is, az adott kép információ elrejtésében és visszafejtésében.

A diffúziós modellek (*Stable Diffusion*, *DALL·E 3*, *Midjourney)*

A diffúz modellek (különösen a Stable Diffusion) alkalmasak a képfelismerésre, osztályozásra, képelemzésre, és az adott objektum beazonosítására, többféle modellt vizsgáltunk meg.

Generatív modell:

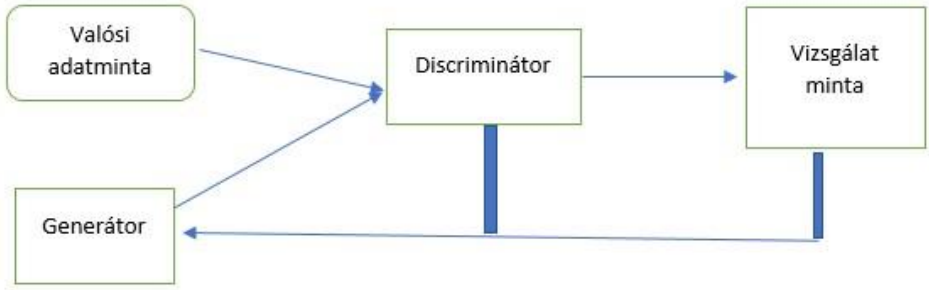
- GAN (Generative Adversarial Network)
- VAE (Variational Autoencoder)
- Diffusion modellek (pl. *Stable Diffusion*, *DALL·E 3*, *Midjourney*)

A generatív modell alkalmas új képek létrehozására és az adott képnek az elemzésére. A GAN modell egy neurális hálózati rendszer, amely alkalmas képgenerálásra és képfelismerésre. A GAN működése egy véletlenszerű rajzból egy valósághoz hasonló képet próbál létrehozni. A diszkriminátor szerepe pedig annak eldöntése, hogy kép valós vagy hamis a képosztályzás segítségével. A GAN a neurális hálózatoknak van egy olyan osztálya, amelyet a felügyelet nélküli tanulásra használnak.

Működése:

- Generatív: Ez valószínűségi modell felhasználásával írja le az adatok generálásának módját
- Adverzális: Itt történik a modell betanítása
- Neurális hálózat: Az MI algoritmusok használata

A Generative Adversarial Network tartalmaz generátort és egy diszkriminátort. A generátor mintákat generál, ami lehet a képi információ, ami lehet igazi vagy hamis.



4. Ábra: Generative Adversarial Network, saját szerkesztés

A diszkriminátor a fenti ábra alapján ez a Generative Adversarial Network versenyalapon működik. Az adatok elosztása rögzítve van, betanított állapotban célja az, hogy a diszkriminátor hibázásának a valószínűségét maximálisan növelje.

Ezzel szemben a dikszkriminátor becsléssel azt vizsgálja, hogy a kapott adatok tanulóadatok-e, és az adatok származását elemzi, hogy azokat honnan kapta. Megállapítottuk, hogy mindkét modell versenyalapon működik mert egymás jutalmát próbálják minimalizálni, de a modellek a saját jutalmukat pedig maximalizálni kívánják.[5]

TÉRBELI SZTEGANOGRÁFIAI MODELLEK

Képi információk titkosítása bit szintű képmódosítás alapján; Least Signification Bit

A képi szteganográfia legelterjedtebb adatrejtési technikája a LSB módszer, amely újabb fejlesztések nyomán egy másik algoritmussal párosítva hatékonyabb eredményeket közvetít. A kutatás során vizsgáltuk, hogy a hagyományos LSB-t a F4 (Filtering szűrési) algoritmussal, egy fejlettebb technikával párosították, amely titkosított adatokat a kép minőségének megőrzése mellett biztosította. Ennek eredményeképpen a LSB-ben (a kép legkisebb információegysége), az adatrejtés a több színcsatornából (RGB) álló látható fedőkép térbeli tartományának, vagyis képszínek manipulációjával valósul meg. A titkosított adatok úgy ágyazódnak be, hogy a képen látható változás minimális marad.

A LSB módosításakor az adatrejtés során a kép pixeleiben használt bitek számát a K-érték határozza meg. Ha a K-érték nő, akkor a bitek is jobban váltakoznak, így rejthető el nagyobb mennyiségű adat, változhat meg jobban egy kép minősége és válhat könnyebbé a titkosított adat észlelhetősége is. K = 1 (csak az egyes pixel, az LSB módosítása történik meg) K = 2 (az LSB és a 2. legkisebb bit is változik, így nagyobb mennyiségű adat rejthető el, de a kép minősége torzulhat.

- Az elrejtendő információ K-bites egységei meghatározott sorrendben kerülnek beágyazásra a kiválasztott fedőkép pixeleinek legkisebb helyiértékű bitjeibe.
- A fedőkép a RGB színmodell három csatornából épül fel, ahol mindegyik csatorna meghatározott (6, vagy 8) bites értékkel jellemzi a színintenzitást; ezek legkisebb bitjei használhatók az adatrejtésre.
- A LSB helyettesítése egy algoritmus alapján történik, ahol az elrejtendő üzenet bitekre bontva kerül titkosításra, így az összes képpont legkisebb helyiértékű bitje a titkos üzenet egy-egy bitjével kerül helyettesítésre. Bináris formátumú kódolás esetén a számítógép adatként, pl. képpont-értékként kezel és értelmez, a kép vizuálisan nem változik, de az információ rejtve marad.
- A visszafejtés során a LSB-bitek kiolvasásával az üzenet visszaállíthatóvá válik; a módszer előnye, hogy a módosított kép azonos marad az eredetivel.[6]

Többrétegű bitrejtési módszer értékelése, Multi Layer LSB (ML-LSB)

A képi titkosítás hatékonyságát és adatbiztonsági funkcióját a Friedrich-modellel, három kritérium alapján szemléltethetjük: a megfelelő kapacitás, robusztusság és a vizuális észlelhetőségi faktor alacsony szinten tartásával. A robusztusság (ellenállóság): a képben lévő titkos adat sértetlenségét külső manipulációk (tömörítés, átméretezés, zajok hozzáadása), a kapacitás pedig a biztonságosan elrejthető adatok mennyiségét határozza meg. LSB esetén: csak az utolsó bitet használja, egy rétegben 1 bit/pixel kapacitást biztosít (512×512 kép esetén kb. 32 KB), míg a ML- LSB több réteg alsó bitet használ, így nagyobb adat rejthető el (64 KB), de a kép torzulása is növekszik. Az észlelhetőség: a rejtett információ láthatósága LSB esetén kevesebb bit módosul, nehezen észlelhető, míg a MLSB több

réteg bitet változtat, a felismerhetőség kockázata nő, a változás sima képeken könnyebben, míg zajos részletgazdag képeken nehezen észlelhető. A többrétegű LSB több LSB réteget alkalmaz az adat elrejtéséhez, hogy növelje a hordozó biztonságát és adatkapacitását (10 KB helyett 12 KB). A többrétegű LSB-t matematikai modellel ábrázolhatjuk *s* és *k* rétegek számításával:

Változók	Rétegek mutatói	eredmény s=1	eredmény s=2
s	beágyazódási szintek	s=1	s=2
b	pixel színmélység értéke	b=24 bit	b=24 bit
a	bitek/pixel száma	a=1	a=2
m	sorok száma	512 pixel	512 pixel
n	oszlopok száma	512 pixel	512 pixel
k	rétegek száma	1 db	1 db
C'	C' (egyrétegű kapacitás)	32 KB	64 KB
C	C (többrétegű kapacitás)	32 KB	192 KB
K%	K% (kapacitás növekedés)	0%	200%
r	r (adat arány)	4.17%	25 % adat

1. Táblázat: Egy 512x512 színes, 24 bites kép egyenletek alapján számolt értékei, forrás: "Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach", saját szerkesztés

- Beágyazási szintek **s**: egy adott kép titkosításához szükséges rétegek száma, figyelembe véve a kép méretét, a használt beágyazott biteket „a" és a pixelbitek „b" számát adja meg, M a képméret, N az adatmennyiség, k a rétegek száma, alapján:

$$s = log_b^a\ (M, Nk)$$

- Többrétegű módszer c: a képletben **c** az elrejtett adat teljes mennyisége, **s** a titkosítási rétegek száma és az előzőekben említett paraméterek összeadása alapján, a kapacitás növekményét mutatja a titkosítási rétegek számának növelésével:

$$c = \sum_{n=1}^{s} \left(MNk \left(\frac{b}{a}\right)^n \right)$$

- Az egyrétegű titkosítás(C'): a fedőadat kapacitása mutatja, a beágyazható adat mennyiségét mutatja egy egyrétegű módszer alkalmazása esetén:

$$C' = MNk \left(\frac{b}{a}\right)$$

- Kapacitásnövekedés mértéke-K% aránya: a kapacitás növekedését mutatja meg, amit az ML-LSB módszer alkalmazásával érhetünk el az alap LSB módszerhez képest:

$$K = \frac{C - C'}{C'}\ x100$$

- Rejtett adat aránya: a képlet a rejtett adat arányát mutatja meg a teljes fedőadathoz képest:

$$r = \frac{C}{MNK} x100$$

A képi adatstruktúrához kötött értelmezést az egyenletben szereplő változók segítik az egy és többrétegű LSB leírásánál.[7]

Képi titkosítás adaptív pixel értékekkel-Dinamikus LSB (D-LSB)

A LSB továbbfejlesztett, adaptív változata a D-LSB, amellyel a kép a vizuális minőséget őrizhetjük meg, míg a rejtett adat mennyiségét maximalizálhatjuk. A dinamikát a kép egyes részeibe rejtett adatok bitjeinek cseréje jelenti LSB legkisebb utolsó bitjei helyett. A LSB dinamikája a pixel kontrasztjában keresendő, amelyben nem társul minden adott pixelhez ugyanannyi bit, ezért alacsony kontrasztnál több, magasabb esetén kevesebb kép vizuális minőségét befolyásoló bit változik. A D-LSB módszert összehasonlítottuk a LSB alapú Binary Image Text-tel (BITS), adattitkosítási módszerrel, melyben az elrejtett információt a kép különböző részein helyezi el. A D-LSB mellőzi a statikus szabályszerűséget, a BITS fix elhelyezési mintát követ, ahol az elrejtési módszer nem adaptív, meghatározott struktúrát követ. A D-LSB módszerekben az elrejtett információ helye nem fix, a titkos üzenet jellemzői vagy a képpontok tulajdonságai alapján változik. A BITS technikában az információ a kép különböző részein helyezkedik el, az éles átmenetek nem látszanak, a detektálhatóság csökkentett mértékű, de az elrejthető adatmennyiség növelhetővé válik. A szakértők a módszert a Wavelet Obtained Weights (WOW) szteganográfiai algoritmusokkal fejlesztették tovább, amely intelligensen alkalmazkodik a kép helyi kontrasztjához, ezáltal megőrizve vizuális minőségét és biztosítva a beágyazott információk integritását. Mindenre kiterjedő, alapos tesztelést követően a csúcsjelzés-zaj arány (PSNR), a strukturális hasonlósági index mérés (SSIM), a bit hibaarány (BER) és az átlagos négyzet alakú hibamérés során (MSE) – 87 %-os megközelítést ért el a stego-kép az eredeti képhez való viszonyításkor.[8]

LSB típusa	Tulajdonság	Előny	Hátrány
LSBT	üzenet bitek legkevésbé jelentős bitekbe kerülnek	egyszerű, gyors	Kevés adat rejthető el, könnyen kimutatható.
ML-LSB	üzenetbitek több rétegben helyezkednek el a képpontokban	több adat rejthető el	képminőség romlása láthatóbb
D-LSB	üzenetbitek dinamikusan, adattípusnak megfelelően helyezkednek el (adaptív rendszere miatt hatékonyabb)	több adatrejtés, jobb minőség	bonyolult, lassabb művelet

2. Táblázat: A képi szteganográfia térbeli LSB modellek összehasonlításáról, saját szerkesztés

Kép- és színcsatornák váltakozása (HVS, YCbCr, RGB)

Vizsgálatunk a képi szteganográfia legfontosabb alapjaira, a kép élességére és az abban elrejtett információ láthatatlanságára összpontosít. A kép a színcsatornák váltakozása és manipulációja révén a humán vizuális rendszer (HVS) érzékenységéhez igazodik. A HSV modell kis méretű képeknél jobb vizuális eredményt ad, mint a YCbCr, mert a módosítás

kevésbé torzítja a minőséget. A fényerő (Value) különválik a színektől (Hue Saturation), így a rejtett információ kevésbé torzítja a képet. A YCbCr modellben Y – luminancia, fényerősség, Cb (Blue Chroma –kék, illetve Cr –Red Chroma- vörös színárnyalatok, amelyek a fényerőt és a színárnyalatokat külön kezelik. A modell hatékony az információ elrejtésére, de a színcsatornák energiaszintje érzékeny, kisebb színinformációkal rendelkező képeknél torzításokat okoz. Az RGB modell nagyobb formátumú képek esetében energiahatékonyabb és stabilabb.[9] A különböző színmodellek a beágyazás során módosult változatokat mutatnak. A RGB – minden csatornája (vörös, zöld, kék) egyenlő szerepet kap a nagyobb képeken stabilabb teljesítményű, minimális torzulási eredménnyel. A három csatornás módszerben az egyik csatorna utolsó két LSB-je jelzi, hogy a további két csatorna tartalmaz-e adatot. A csatornák sorrendje minden 3. pixelnél ismétlődően változik. A módszer hátránya, hogy a kapacitás a jelzőbit értékétől, átlagosan 3 bit/pixel értéktől függ.

Pixel sorszáma	R-csatorna	G-csatorna	B-csatorna
1	I	adattároló 1.	adattároló 2.
2	adattároló 1.	I	adattároló 2.
3	adattároló 1.	adattároló 2.	I

3. Táblázat: RGB csatornák beosztása pixelindikátorok szerint. I = Indikátor csatorna, adattároló 1, 2 = a pixel azon csatornái, ahol a titkosított adat el van rejtve, saját szerkesztés

A módszer továbbfejlesztett változata a Triple-A algoritmus, amely az AES szimmetrikus titkosítást és pszeudorandom számgenerátort (PSNG) használja a színcsatornák véletlenszerű kiválasztásával. Két véletlenszám (Seed1, Seed2) határozza meg a beágyazás helyét és a beilleszthető bitek számát, így a biztonság és kapacitás egyaránt növekszik.[10]

PVD (Pixel Value Differencing), a képpont alapú értékkülönbségek a szteganográfiában

A ML-LSB és DLSB módszerek utáni leghatékonyabb eljárás az adatelrejtést és a kép minőségének megőrzését illetően a PVD. Módosított változataival a képek pixelértékein belüli hatékony dinamikus adatrejtést tehetjük lehetővé. Fejlesztett változata a hibrid PVD és az LSB technikák kombinációja, így a bitek szélterületeinek kihasználásával a beágyazási kapacitás is hatékonyabbá vált. A TPVD (három-pixel érték technikájú alkalmazás) a meglévő értékek különbségéttől teszi függővé a beágyazás minőségét. A hagyományos PVD statikus alapú módszer értékerősségét fokozta a PVD flexibilis változata a MFPVD (Modified Flexible PVD), amelynek legfőbb tulajdonsága a rugalmas paraméterek, a képi minőség és színpontosság megőrzése. A fejlesztési eredmények ellenállók a képbe integrált adatok megfejtésekor a RS (Regular Sampling) rendszerességen alapuló elemzés során. A PVD célja hogy a pixel értékeiben hatékonyan megőrizze a beágyazott információt, mert a hatékonyságot vizsgáló módszerek, például a Wavelet Steganalízis (WS) és a PDH (Pixel Differenciás Hisztogram) a képen belüli apró eltéréseket és a színek közötti eltérő mintákat ismerik fel. A kezdetleges PDH a pixelérték különbség sebezhetőségét méri. MatlabR2018 segítségével létrehozott kísérleti környezetben 1000-10000 véletlenszerű kép válogatásával a képosztályokat négy osztályra csoportosították, gyanús-stego kép, valódi-borítókép és ezek kevert változatai alapján.[11]

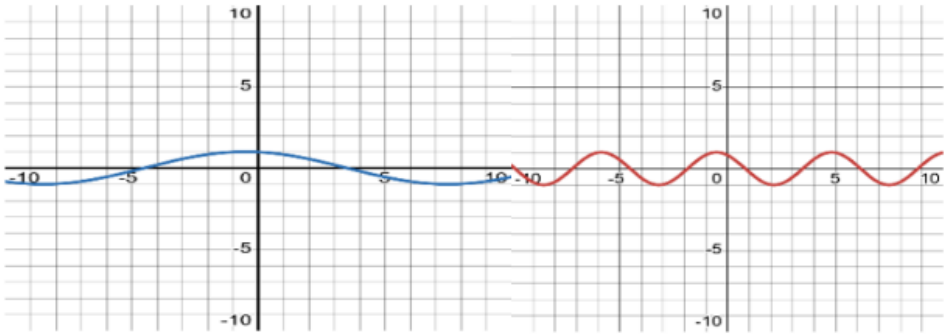
Az adatok biztonságos beágyazása a stego-kép magas vizuális minőségétől függ. Az adatok kinyerését egy indikátor pixeltől (IP), tehetjük függővé. Az IP egy kulcsjelző

pixel, ami megmutatja, hogy *honnan és hogyan* tudjuk az adatokat kinyerni. A borítóképbe való beágyazása előtt a titkos adatoknak megfelelő pixelek sorrendje módosul és átrendeződik. Adatbiztonsági szempontokat figyelembe véve a képpontok sorrendjét és beágyazás szempontjából fontos paramétereit egy Genetikai Algoritmussal (GA) optimalizáltan módosítjuk és rendezzük át. A folyamat célja a legalkalmasabb képi pixelpozíciók kiválasztódása. A legújabb fejlesztések algoritmusok és keresztezett PVD módszerek alapján, így a GA-IPVD egy, amely a beágyazott adatok biztonságos rejtésére összpontosít és garantálja a kép minőségét. A módszer a különböző stego-támadásokkal szemben ellenállást mutatott, beleértve a hisztogramot (PDH), valamint a rendszeres és egyedülálló (RS) elemzéseket.[12]

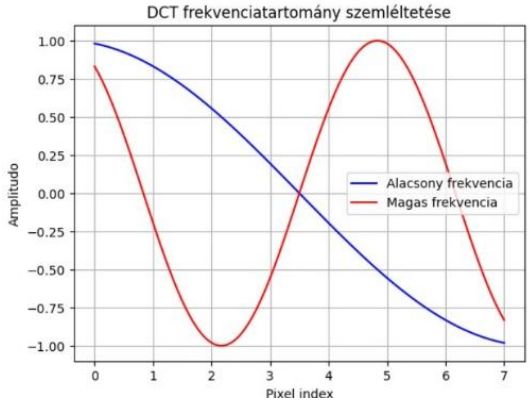
FREKVENCIA-ALAPÚ KÉPREJTÉSI MODELLEK

Diszkrét Cosinus Transzformáció, Fast Fourier Transzformáció, zajfrekvencia

Míg a PVD a képpontok intenzitáskülönbségeire épít, addig a transzformációs modellek frekvenciatartománybeli feldolgozással növelik a hatékonyságot, ahol az együtthatók viszonya és a referencia-minták biztosítják a stabil adatbeágyazást. A DCT az 1970-es évek végétől ismert képtömörítési eljárás. A szakértők a transzformációs technikát a 8x8 soros blokkokra alkalmazták, ahol a kiválasztott együtthatókat rendezett párokba csoportosították. Minden párba egyetlen vízjel-bitet kódoltak referenciaminták alapján: ha az első együttható nagyobb a másodiknál, 1 bitet, ha kisebb, 0 bitet jelöl, egy minta két együtthatója 1 és −1. Az együtthatók értéke a képpel összevetve jut eredményre, az előjelek mutatják, hogy az első együttható nagyobb-e a másodiknál. A Watson (David J. Watson) perceptuális modellje az észlelési kísérletben elsőként a referencia mintát alakítja át DCT-ben, ahol a kép ábra-komplexitás, színek, és fényerősség frekvenciájával optimalizál egy képet. A módosított komponensek szabályozzák, hogy hol tudjuk jobban elrejteni az adatot, amelyek a formált mintát a térbeli tartományba helyezik vissza, hogy azt a képbe ágyazhassák. Nem lineáris adatnyerési folyamat, így a Gauss-féle (harang-görbe) eloszlással a középtartományban lévő adatokban a kódolt bitek statisztikai módszerekkel könnyen kinyerhetők.[13] A DCT a kétirányú koszinusz függvények kombinációját használja a 8×8-as blokk frekvenciáinak bemutatására. Az ábrák a blokk komponenseit szemléltetik, az x- és y-irányú koszinuszokat külön hullámként:



5. Ábra: kétirányú függvények hullámábrázolása, a bal oldalon lágy, alacsony frekvenciájú, míg a jobb oldalon egy zajosabb, magasabb frekvenciájú hullámok különbsége a frekvencia növekedésében rejlik, amely a DCT alkalmazásával érzékelhető, desmos-graph: saját szerkesztés



6. Ábra: A mindkét irányban (x és y) ábrázolt koszinusz függvények mutatják, hogyan hatnak a különböző frekvenciák az 8×8-as blokk komponenseire a diszkrét koszinusz transzformáció során, jupyterlite.github.io/demo/lab/index- Python kernel backed by Pyodide: saját szerkesztés

A DCT-transzformáció az egyik legelterjedtebb frekvencia-alapú módszer a sztenográfiában, energia-tömörítési tulajdonságával a jel energiáját néhány jelentős együtthatóban koncentrálja. A jelentéktelenebb együtthatókat felhasználhatjuk a titkos adatok elrejtésére a jel minőségének romlása nélkül. A DCT a kép az alacsony frekvenciákat a térbeli tartományából a frekvenciatartományba, míg a nagyfrekvenciás összetevőket a kisebb és kevésbé érzékelhető értékekre állítja, így biztonságosan módosíthatjuk a titkos adatok beágyazására. A kép vizuális érzékeléséért felelős nagyfrekvenciás, rejtett adatokat tartalmazó együtthatók módosíthatók anélkül, hogy a változás észlelhető lenne. A következő képletek a DCT alkalmazását mutatják a jelek frekvenciakomponensekre bontásakor, a titkos információk különböző frekvenciákba való beágyazásánál. Elsőként egydimenziós DCT képletet használunk, a jel frekvenciakomponensekre való bontásához, egy sor vagy oszlop itt N a minták száma (azaz a jel hosszúsága), **k** az adott frekvenciaindex:

$$\mathrm{X}[k] = \sum_{n=0}^{N-1} x[n] \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right], \quad ahol\ k = 0,1,\dots,N=-1$$

A kétdimenziós DCT, amelyet képek esetén alkalmazunk, az alábbi módon számíthatjuk ki a képi frekvenciákat:

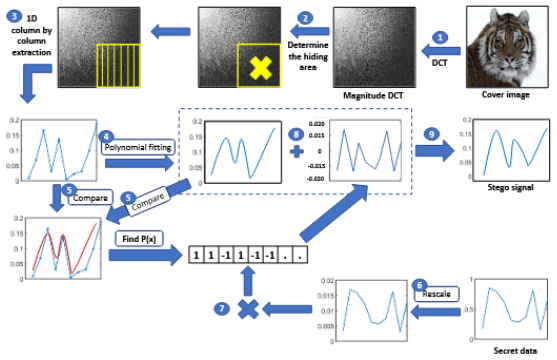
- M **és** N a bemeneti kép dimenziói:
- u**,** v a frekvenciaindexek
- x,y = eredeti kép képpontjainak értékei:

$$\mathrm{X}[\mathrm{u},\mathrm{v}] = \sum_{\mathrm{x}=0}^{\mathrm{M}-1}\sum_{\mathrm{y}=0}^{\mathrm{N}-1} \mathrm{x}\left[\mathrm{x},\mathrm{y}\right] \cos\left[\frac{\pi}{\mathrm{M}}\left(\mathrm{x}+\frac{1}{2}\right)\mathrm{u}\right] \cos\left[\frac{\pi}{\mathrm{N}}\left(\mathrm{y}+\frac{1}{2}\right)\mathrm{v}\right]$$

Az első summáció **x** indexe, a **x=0** értéktől **M-1**-ig terjed, a második **y** indexét használja, és **y=0** értéktől **N-1**-ig terjed, a summáció az alacsony frekvenciájú jellemzőket, hátteret, éleket mutatja, a koszinuszok a képen változó frekvenciákat.

A titkos adat beágyazásának folyamata oszloponként zajlik. Az algoritmus a 2D-DCT alkalmazásával először a fedő képből kinyeri a DCT koefficienseket, majd a titkos

jelet a polinomiális modellel kombinálja. Az inverz DCT -vel visszaállítja a stego képet, így a titkos információ rejtve marad:



7. Ábra: Az embedding algoritmus, oszlopról-oszlopra haladva. Rabie T.,Baziyad M., Kamel I.: High-Fidelity Steganography: A Covert Parity Bit Model-Based Approach, 9.pp

- 1-4 lépések: fedő kép és titkos információ behelyezése, polinomiális fok és skálázási tényezők megállapítása
- 5-9 lépések: a 2 Dimenziós DCT-t a fedő képre helyezik, majd a titkos képet lecsökkentik a skálázási tényezővel a DCT oszlopok kinyerése után minden oszlopon polinomiális modellezést alkalmaznak, amelyhez hozzáadják a titkos üzenetet
- 11-16 lépések: csoportosítják az oszlopokat és visszahelyezik őket, majd az inverz DCT-t alkalmazzák a stego kép előállításához.[14]

FFT (Fast Fourier Transform) alapú szteganográfia

Az FFT hasonlóan működik a DCT-hez, de a Fourier-transzformációt alkalmazza a képen. Az elrejtett adatokat a kép frekvenciatartományában található magas frekvenciájú komponensekben rejthetjük el, amelyek kevésbé észrevehetők a szem számára.

A Fourier-transzformáció egy olyan matematikai módszer, amely alapján az adott jel vagy függvényt át tudjuk transzformálni időtartományból frekvenciatartományba.

$$F(w) = \sum_{-8}^{8} f(t) e^{-iwt} dt$$

Ahol:

- f(t)f(t)f(t) az időbeli jel,
- F(ω)F(\omega)F(ω) a frekvenciatartományban lévő transzformált jel
- ω\omegaω a szögfrekvencia (ω=2πf)
- i az imaginárius egység.[15]

A képfeldolgozás igen fontos technika, mert többféle alkalmazási területe van, pl. a röntgenfelvételek képi információ vagy fényképezőgéppel elkészített kép képi információ feldolgozása. Vizsgálatunk az adott képi szűrők alkalmazására tér ki, hogy hogyan változik a kép, a jó minőségű megtartása mellett. A Fourier-transzformáció algoritmusai segíthetnek a hatékony képfeldolgozásban. Egy adott kép feldolgozása során többféle képi szűrő algoritmusát alkalmazhatjuk, amelynek keretében fontos a képminőség javulása pl.: a képélesítési algoritmussal és a zaj eltávolításával, ha van a képen. A képfeldolgozásban vizsgált frekvenciatér segít megérteni és megváltoztatni az adott kép frekvenciatartományát. Míg a

képeket a vizualitás szemszöge szempontjából a pixelek érétkei alapján vizsgáljuk, a Fourier transzformációs módszerrel a képet egy frekvencia terében értékelhetjük. Vannak alacsony frekvenciák, amelyeken az adott képet egy lassú és fokozatos átmenetek kísérik, míg ha a magas frekvenciát tekintjük, akkor a képi élek textúrák gyors változásai követhetjük nyomon.

A Fourier-transzformáció igen fontos szerepet játszik, különösen a Fast Fourier Transzformáció a digitális szteganográfiában, amely alapján egy adott frekvenciatartományban a jelet változtathatjuk is az információ elhelyezése vagy kinyerés mentén. A Fourier-transzformáció alkalmazása során a digitalizált kép vagy hang frekvenciakomponensekre bomlik. A frekvenciák lehetnek magas és alacsony szinten. Azt az információt, amit szeretnék elrejteni a magas frekvenciába ágyazzák be, tekintettel arra hogy ez biztonságosabb mert az emberi hallószerv, nem érzékeli megfelelően a változást. Megkülönböztetünk kép és hangalapú titkosítást. A Fourier transzformációnak köszönhetően megkülönböztethetünk képi és hangalapú szteganográfiát. A FAST Fourier Transzformáción alapúló változtatás során, a képi színintenzitások szempontjából kisebb változást tehetünk azokon a képi komponenseken amelyek, a magas interferencia tartományú értékeket képviselik. A kép tartalma nem változik, de a titkosítandó adat rejtve marad a képen. A hangsztenográfia esetében a magas frekvencia hangok változtatására fokuszálunk, van olyan hangminta, amely mint zaj, az emberi érzékszerv a fül nem érzékel, mert egy olyan frekvencia tartományba esik, amely nem hallható, és ott van az a pont, ahol az információ elrejtése valósul meg. Azonban mint mindennek vannak előnyei és hátrányai. Vizsgálva a Fourier algoritmust lehetőségünk van adatokat elrejteni torzulás nélkül, mivel a változások frekvenciatartományban történnek meg. A jelet nem szabad túlzottan módosítani, mert a rejtett adat sérülhet, és a kívánt információ visszanyerése nehezített lesz.

8. Ábra: eredeti kép, Gauss elmosás, gimp, saját szerkesztés

Itt az eredeti képet elsőször a frekvencia tartományba alakítottuk a diszkrét Fourier transzformációval DFT segítségével. A DFT és FFT összehasonlítva az FFT jobb hatékonyságot mutat, a számítási módban is. A Léna-képet (8. ábra) FFT alkalmazásával frekvenciatartományba alakítottuk egy felül áteresztő szűrőt alkalmazva, hogy az alacsony frekvencia összetevőket kiszűrjük, kiemelve az éleket és a képen látható finom részleteket. A képen a magas frekvencia a kép éleit és a zajaikat reprezentálják, a szűrő segítségével megtartunk alacsony frekvenciás képi információkat. A felül áteresztő szűrővel eltávolítottuk a mély

frekvenciákat, ennek köszönhetően a kép élesebb lett, de az alacsony frekvenciájú képi információk komponensei erősebb képi megjelenést adnak, miközben az alacsony frekvenciájú információk megmaradnak. Léna (8. ábra) képét gauss elmosás algoritmusát alkalmazva a képi pixel értékek egy elmosó megjelenést adtak, amely hatékony módszer a kép simítására, és amely a konvulució és a FFT kapcsolatára alapoz. A kép simítása során, a gauss-elmosás célja az, hogy csökkentsük a zaj és a Gauss függvénnyel való konvuluciót, de ez a konvulucios művelet szorzatként jelenik meg ezért hatékonyabb, ha a képet egy egyszerűbb frekvencia tartományba helyezzük, ott végezzük el az adott műveletet majd visszaalakítjuk.

A folyamat lépései:[15]

Fourier-transzformáció - Az adott képet, amit szeretnénk elmosni alkalmazva az FFT (FAST Fourier Transform) átalakítjuk egy frekvencia tartományba, így eredményképpen az adott kép frekvenciakomponenseit.

$$F(u,v)FFT(\{f(x,y)\}$$

A Gauss függvény segítségével megtartjuk a középső és alacsony képi frekvenciákat míg a magas frekvenciákat pedig lépésekben elnyomjuk.

$$H(u,v)=e-\frac{(u^2+v^2)}{2q^2}$$

Ezután a képnek a Fourier spektrumát szorozzuk a Gauss szűrővel

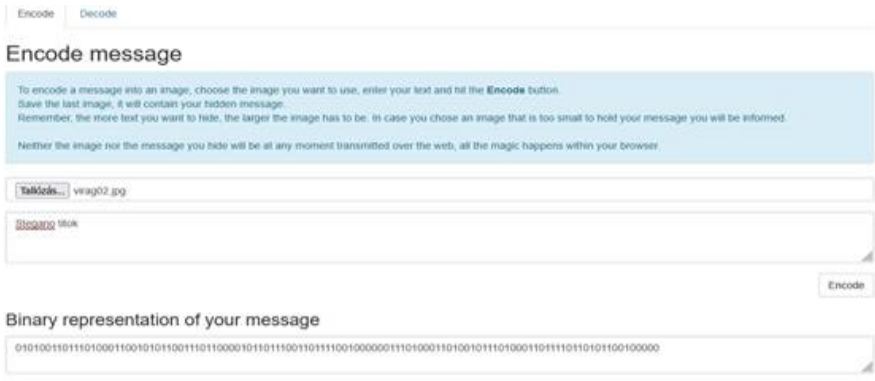
$$G(u,v)=F(u,v)\cdot H(u,v)$$

Végül a kapott eredményt segítségével visszaalakítjuk a képtartományba az úgynevezett inverz FFT segítségével.

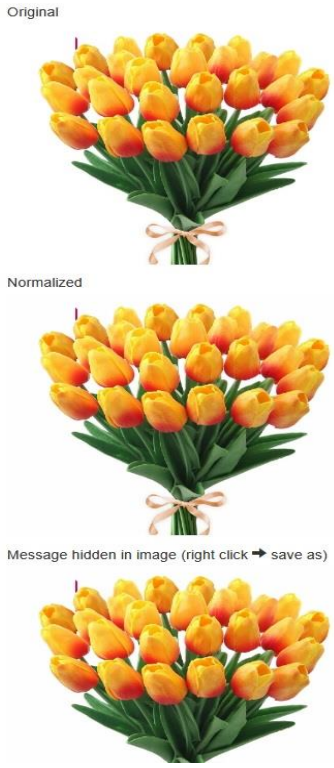
$$g(x,y)=Inverz\ FFT\ G\{(u,v)\}[15]$$

Az eredmény egy elmosott, lágyabb kép lesz, ahol a részletek csökkennek, de a fő struktúrák megmaradnak. A képekre többféle szűrőt, vagy open-cv könyvtárat alkalmazhatunk, amelyek segítségével az algoritmusok olvassák be az adott képet. A könyvtár számtalan algoritmust tartalmaz, amelyet a mémiára, ami lehet kép vagy hangfájl is használhatunk. Az adott képre nem csak szűrőt alkalmazhatunk, hanem információt is be tudunk ágyazni a gyors Fourier-transzformáció segítségével, amely egy digitális szteganográfiának felel meg, ahol a képre elrejteni kívánt információt a frekvencia tartományba rejtjük el. A módszer működhet kép és hangfájlokra is. A titok egyik nyitja az, hogy az FFT a média frekvencia komponenseit olyan mértékben módosítjuk, hogy az emberi érzékszervek pl. fül vagy, szem számára alig észrevehető legyen. Első körben a médiától függetlenül (kép vagy hang) a gyors Fourier transzformációval átalakítjuk, ebben az esetben a médiát (képet) ez a művelet felbontja, ahol az adott pont egy frekvenciát és egy fázist jelent. A következő lépésben az adatbeágyazását tesszük meg, azt az üzenetet, szövegrészt, amit szeretnénk titkosítani, egy középfrekvenciás komponensbe bitenként beágyazzuk. Ezután a Fourier transzformációnak vesszük az inverzét, így visszakaphatjuk a tértartománybeli képet. Az adott képen, hogy a titkosított információt kinyerjük, dekódolós eljárást végzünk és kiolvassuk a bitinformációkat. A beágyazási módszer jól paraméterezhető, a frekvenciasáv, a képen lévő beágyazás mélysége és a visszafejtési kulcs alapján. A módszer előnye abban tükrözik, hogy más módszerhez hasonlóan az információ rejtettebb lesz, hátránya, hogy számításigényes, mert az FFT inverzét is alkalmazni kell, továbbá ismernünk kell a frekvenciasávot, és a kulcsot.

A szteganográfia szempontjából a kép olyan részét használjuk fel, ami nem okoz szemmel látható torzulást. A kép pixelgrafika esetén pixelekből áll, minden egyes pixel adott képpontnak felel meg amely RGB numerikus színértéket képvisel. A szteganográfiai programok elő körben bekérik az eredeti képet, amire szeretnék a titkosítani kívánt információt elrejteni.



9. Ábra: információ kódolása, saját szerkesztés



10. Ábra: képi transzformációk, saját szerkesztés

A rejtett üzenet dekódolását láthatjuk, itt az üzenetet vagy egy szót dekódoltuk.

ASCII Bináris Kódtáblázat (Nagy- és Kisbetűk)

Karakter	ASCII (decimális)	Bináris
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001010
O	79	01001111
P	80	01010000
0	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010
a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101

Karakter	ASCII (decimális)	Bináris
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

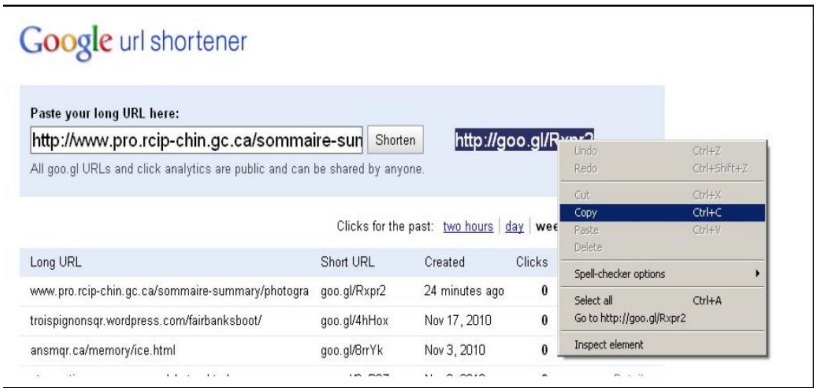
4. Táblázat: Ascii kódtáblázat, saját szerkesztés

ASCII kódtáblázat

A kódtáblázat segítségével történik a titkosítás, azonban a fő komponens a Fourier-transzformáció algoritmusa, amely az adatot átalakítja a frekvenciatartományba, így az adott eredeti jel, amely lehet hang vagy kép, komponensekre bontják. Az eltitkolni kívánt üzenetet elrejthetjük az adott jel frekvencia komponenseiben vagy a frekvencia spektrumánál tesszük meg a módosítást, de csak olyan mértékben, hogy ne legyen ismert. Egy kulcs segítségével végezzük el a frekvenciák módosítását, amely a titkosítani kívánt információt jelenti, csak az tudja visszafejteni, aki a kulcsot ismeri. Ezután vesszük a titkosított üzenetet, amely már el van rejtve a frekvenciák között, ezt az eredeti jelet visszaalakítjuk az időtartományba, és a Fourier-transzformáció inverzének segítségével, így már a kapott média tartalmazza a titkosított információt, amelynek dekódolásához ismerni kell a kulcsot. A Fourier transzformációt alkalmazzák a titkosítási módszereknél, mert lehetővé teszi az adott jel frekvenciatartományában megtehető módosításokat, amelynek köszönhetően el tudjuk rejteni a kívánt információt, amely a jel manipulatív eljárásán alapul.

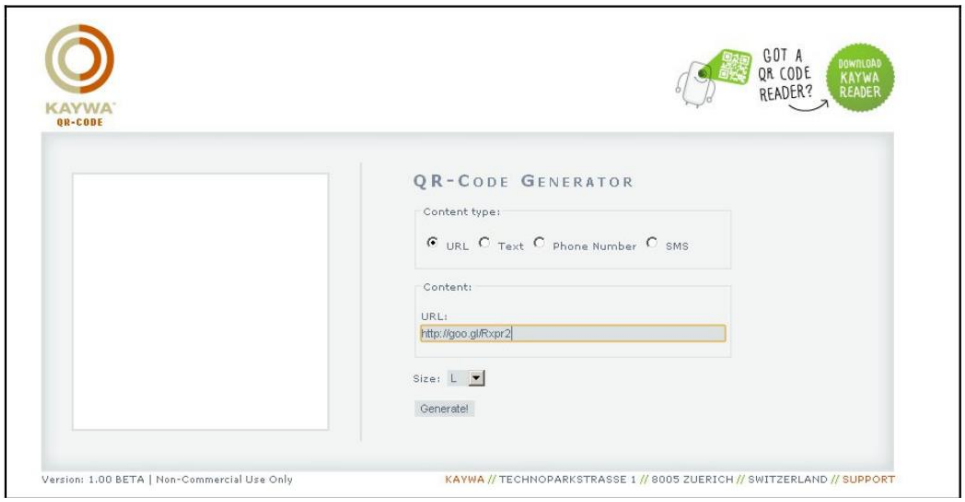
QR-kódok vagy Barcodes a képen belül

A QR-kód egy vonalkód típus, amelyben információt tudunk tárolni, pl.: a termék árát. A szkennerek segítségével tudjuk az információ dekódolni. Kezdetben a logisztikai területén alkalmazták. Bár ez nem egy hagyományos szteganográfiai módszer, a QR-kódok és vonalkódok is tartalmazhatnak titkos adatokat, amelyeket a képen belül rejtünk el. Ezt akkor alkalmazzák, ha a képen egy olyan mintázatot szeretnének elhelyezni, amelyet egy QR-kód vagy vonalkód olvasó képes dekódolni. A QR kód egy beágyazott weblinként működik. Biztonságot is adhat pl.: hogy csak a kódkiolvasás esetén lehet használni a számítógépet. A QR kódokat létre tudjuk hozni webes felületen, kutatásunk során a Kayw weboldallal találkoztunk, ahol a QR kód generátort alkalmazva, lehetőségünk van QR kódot generálni. Első körben a létrehozott tartalom mint információ rövid kódját másoljuk, a goole.gl webes felületen.[16]



11. Ábra: weboldal, forrás: URK weboldal

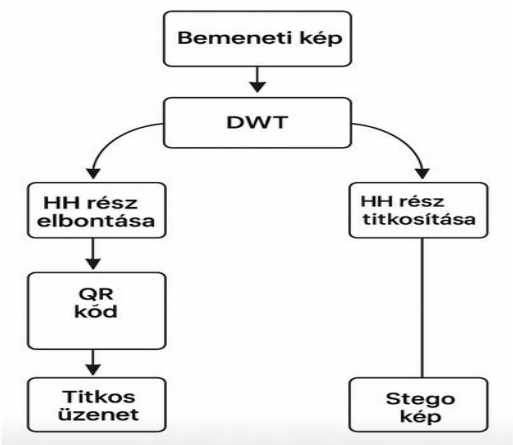
Beillesztjük az URL-t, a https://qrcode.kaywa.com/ weboldalon, kiválasztjuk a 12. ábra méretét, végül megjelenik a QR-kód.



12. Ábra: *QRkód Generátor, forrás: https://qrcode.kaywa.com/*

A fentieket tovább gondoljuk és alkalmazzuk a szteganográfia eljárást akkor a QR kód és a kriptográfiát is kombinálva lehetőségünk van biztonságos környezetű információ beágyazását az adott képbe, amely egy QR kód kép. Ezt a titkosított QR kódot a kép, DWT diszkrét hullámtranszformációs tartományba teszik, a tartományon belül az úgynevezett HH alrészlet legkisebb helyiértékű LSB bitjeibe ágyazzák. A HH Hullámtranszformáció több részre osztható (LL, LH, HL, HH). A HH alrésznek van egy LSB bit síkja és azt a részt módosítják, ennek köszönhetően szinte alig észrevehető lesz az rejtett információ. Hasonlóan a FFT (Fast Fourier Transformation) eljáráshoz, alkalmazzák a DWZ inverzét, visszakapjuk a stego-képet amelyben az információ rejlik.[17]

A titkosított üzenet visszanyerése fordított művelettel történik meg. A módszer a vizsgálat során igen jónak bizonyult, mert alig észrevehető a torzítás.[18] [19]



13. Ábra: folyamatábra, saját szerkesztés

Zaj hozzáadása

Az adatok beágyazása után kis mennyiségű zaj hozzáadása a képhez segíthet elrejteni a módosításokat. A zaj célja, hogy eltorzítsa az eredeti pixelek értékét úgy, hogy az adatok ne legyenek könnyen felismerhetők, de a titkosított üzenet még mindig visszanyerhető marad. A zaj hozzáadása csökkenti a titkosított üzenet minőségét, így érdemes a zaj mértékét gondosan szabályozni.

Degradációs modell

A képi degradációs folyamat egy **degradációs függvény** hatásán keresztül modellezhető, amely az eredeti képen, valamint egy **additív zajkomponensen** működik.

Formálisan a folyamat az alábbi összefüggéssel írható le:

$$g(x,y)=H\{f(x,y)\}+\eta(x,y)$$

- f(x,y) az eredeti (torzítatlan) kép**,**
- H{·} a degradációs operátor vagy átviteli függvény**,** amely jellemzi a torzító folyamatot (pl. elmosódás, mozgás, optikai hibák stb.),
- η(x,y)az additív zajkomponens, amely a képhez szuperponálódik,
- g(x,y) pedig a megfigyelt (degradált) kép[20]

14. Ábra: RGB zaj és Median filter kép, saját szerkesztés

f(x,y(median{g(s,t)}

A medián a **zaj csökkentéséhez** a véletlenszerű zajokat távolítja el, megőrizve a kép fontos részleteit:

- **g(s,t)**: ahol a függvény felvesz egy s és t változót, a kimeneti érték egy numerikus érték
- a **median{g(s,t)}**: a medián függvény a zaj csökkentéséért felel
- **f(x,y,median{g(s,t)})**: x és y azok a pixel pontok koordinátái, ahol a függvényt alkalmazzuk.

A zaj miatt a kép helyreállítása, degradációs függvény statisztikai jellemzőire tekintettel minél pontosabban becsüljük vissza az eredeti képet, ami f(x,y) lenne. Ez egy inverz feladat, amely alapján a degradációs függvény inverzét kell meghatározni, figyelembe véve a környezeti jellemzőket, mint a kép zajának mértéke és torzítása. a kutatásom alapján megállapítottam, hogy az egyik legjobb zajszűrő a medián filter alkalmazása az adott képre, amely a kép pixel intenzitás értékét, amely helyettesítve van a kép szürkeségi szintek mediánjával. Ez a módszer hatékonyan csökkenti a zajt.[21][22]

A median filter képszűrő alkalmazásával kiváló zajcsökkentési képesség érhető el, más filterhez képest arányosan kevesebb elmosodással. A kép vizsgálat alapján hatékonyság tapasztalható impulzuszaj bipoláris és unipoláris zaj esetén.[20]

FELHASZNÁLT IRODALOM

[1] D. Harper, „steganography”, *Online Etymology Dictionary*. [Online]. Elérhető: https://www.etymonline.com/word/steganography

[2] B. Thayer, *Herodotus: The Histories, Book VII, chapters 175–239*. [Online]. Elérhető: https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Herodotus/7d%2A.html

[3] D. Megías, W. Mazurczyk, és M. Kuribayashi, Szerk., *Data Hiding and Its Applications: Digital Watermarking and Steganography*. Basel: MDPI - Multidisciplinary Digital Publishing Institute, 2022.

[4] P. Sharma és S. Goyal, „Steganography Techniques, in: International Journal of Engineering Research & Technology (IJERT)”, köt. 02, 2013, doi: 10.17577/IJERTV2IS4812.

[5] V. Bok, *GANs in Action: Deep Learning with Generative Adversarial Networks*. New York: Manning Publications Co. LLC, 2019.

[6] H. Jaheel, Z. Beiji, és A. L. Jaheel, „Design and Implementation Steganography System by using Visible Image”, *International Journal on Smart Sensing and Intelligent Systems*, köt. 8, sz. 2, o. 1011–1030, jan. 2015, doi: 10.21307/ijssis-2017-793.

[7] A. Qasim Jabbar és D. Roshidi, „Capacity Performance of LSB Method On Multi-Layer Images in Steganography”, *International Journal of Engineering and Techniques*, sz. 5, o. 118–121, 0 2022.

[8] M. S. Abuali, C. B. M. Rashidi, R. A. A. Raof, K. N. F. Ku Azir, S. S. Hussein, és A. Q. Abd-Alhasan, „Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach”, *MMEP*, köt. 11, sz. 6, o. 1403–1416, jún. 2024, doi: 10.18280/mmep.110602.

[9] H. Sajedi, Szerk., *Recent Advances in Steganography*. InTech, 2012. doi: 10.5772/2501.

[10] G. Swain, „Classification of Image Steganography Techniques in Spatial Domain: A Study”, *IJCSET*, köt. 5, sz. 3, o. 219–232, 2014.
[11] W.-B. Lin, T.-H. Lai, és K.-C. Chang, „Statistical feature-based steganalysis for pixel-value differencing steganography”, *EURASIP J. Adv. Signal Process.*, köt. 2021, sz. 1, o. 1–18, dec. 2021, doi: 10.1186/s13634-021-00797-5.
[12] F. Akram, A. AbuEl-Atta, és M. M. Selim, „Image Steganography Based on PVD and Knight Tour Algorithm: A Combined Approach”, *BJAS*, köt. 9, sz. 5, o. 97–103, 2024.
[13] I. J. Cox, *Digital watermarking and steganography*, 2nd ed. in The Morgan Kaufmann series in multimedia information and systems. Amsterdam Boston: Morgan Kaufmann Publishers, 2008.
[14] T. Rabie, M. Baziyad, és I. Kamel, „High-Fidelity Steganography: A Covert Parity Bit Model-Based Approach”, *Algorithms*, köt. 17, sz. 8, o. 328, júl. 2024, doi: 10.3390/a17080328.
[15] V. A. Oppenheim és S. A. Wilsky, *Signals and Systems*, köt. Pearson Education. 1983.
[16] „Appendix D: Glossary Introduction, QR Code How-To Guide”. Prepared by the Association of Nova Scotia Museums For the Canadian Heritage Information Network’s (CHIN) Professional Exchange. [Online]. Elérhető: https://www.canada.ca/content/dam/chin-rcip/documents/services/web-interactive-mobile-technologies/codes_qr-qr_codes-eng.pdf
[17] A. Yahya, *Steganography Techniques for Digital Images*. Cham: Springer International Publishing, 2019. doi: 10.1007/978-3-319-78597-4.
[18] L. M. Marvel, C. G. Boncelet, és C. T. Retter, „Spread spectrum image steganography”, *IEEE Trans. on Image Process.*, köt. 8, sz. 8, o. 1075–1083, aug. 1999, doi: 10.1109/83.777088.
[19] C. Y. K, „A HDWT-based reversible data hiding method”, *Journal of Systems and Software*, sz. 82, o. 411–421, 2009.
[20] N. Subash és M. Sucharitha, *DIGITAL IMAGE PROCESSING*. 2021.
[21] V. Hajduk, M. Broda, O. Kovac, és D. Levicky, „Image steganography with using QR code and cryptography”, in *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, Kosice: IEEE, ápr. 2016, o. 350–353. doi: 10.1109/RADIOELEK.2016.7477370.
[22] R. C. Gonzalez és R. E. Wood, *Digital Image Processing*. in 4.

DOI: https://doi.org/10.12700/btsz.2025.7.4.117

FUNDAMENTALS OF THE ON-LINE HAZOP OPTION AND THE ACS-FORCE MODELL

A HAZOP ON-LINE LEHETŐSÉGÉNEK ALAPJAI ÉS AZ ACS-FORCE MODELL

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

Abstract

HAZOP is a qualitative method traditionally applied during the design phase. Our objective is to integrate HAZOP into on-line, industrial process control systems. Achieving this, however, requires a novel approach. While the integration of fuzzy logic has opened new dimensions in HAZOP analyses [8], its applicability remains limited due to inherent compromises. In our view, Takagi–Sugeno–Kang type fuzzy models may offer a breakthrough, enabling faster and more numerical risk estimation. To address the inherent weaknesses of TSK fuzzy systems, we employ metaheuristic optimization techniques. As part of our research, we have developed a new framework named: ACS-FORCE. Beyond its on-line data processing capabilities, ACS-FORCE provides high sensitivity, robustness, and scalability, thus elevating HAZOP-based risk assessment to a new level.

Keywords

HAZOP, fuzzy, on-line risk assessment, ant colony, industrial process control

Absztrakt

A HAZOP egy tervezési fázisban alkalmazott, kvalitatív, kockázatelemzési módszer. Célunk, hogy a HAZOP -ot, integráljuk az on-line, ipari üzemirányítási folyamatokba. Ehhez viszont új megközelítésre van szükség. A fuzzy logika integrálása új dimenziót nyitott a HAZOP elemzésekben [8], de csak kompromisszumok mellett alkalmazható. Meglátásunk szerint a Takagi–Sugeno–Kang típusú fuzzy modell alkalmazása áttörést jelenthet, mert így gyorsabb, numerikus kockázatbecslés valósítható meg. A TSK-fuzzy gyengeségeit, metaheurisztikus optimalizációval kompenzáljuk, kutatásunk során megalkottunk egy új keretrendszert, melynek az ACS-FORCE nevet adtuk. Az on-line, adatfeldolgozási képességen túl, az ACS-FORCE magas érzékenységet, robusztusságot és skálázhatóságot kínál, s új szintre emeli a HAZOP-alapú kockázatértékelést.

Kulcsszavak

HAZOP, fuzzy, online kockázatértékelés, hangyakolónia, ipari folyamatirányítás

[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 biztonságkritikus rendszerekben a kockázatelemzés kiemelkedő fontosságú, mivel ezeknek a rendszereknek a meghibásodása vagy helytelen működése súlyos biztonsági következményekkel járhat. A kockázatelemzés célja a kockázatok azonosítására és mélyebb megértésére irányul, ideértve azok lehetséges következményeit és bekövetkezési valószínűségét, használatával megelőzhetők az esetleges balesetek [1][2][3]. A kockázatelemzés területén az egyik legelterjedtebb és legszélesebb körben alkalmazott módszertan a HAZOP (Hazard and Operability Study), amely az 1960-as években a vegyipari biztonságtechnika igényeire válaszul került megalkotásra. Az eltelt évtizedek során a módszer de facto iparági szabvánnyá vált, különösen a nagy megbízhatóságú, veszélyes üzemeltetésű rendszerek körében [4], példaként említjük a petrolkémiát, gázipart és hidrogéntechnológiát. A HAZOP a tervezési fázisban alkalmazott, szisztematikus módszer, mely a komplex rendszerek veszélyeinek és működési anomáliáinak azonosítására alkalmas. Módszertani előnye, hogy strukturált. Az összetett rendszereket részfunkciókra (ún. „node-okra") bontja, majd irányított kulcsszavak (ún. „guide word") segítségével elemzi azokat. A folyamat során a cél, hogy az üzemszerű működéshez képesti eltéréseket, valamint a kockázatok lehetséges okait és következményeit is feltárja. A HAZOP további előnye, hogy kiterjedt szakirodalom és módszertani útmutatók támogatják [5][6]. Ugyanakkor jelentős emberi erőforrás-igényű és magas szubjektivitással terhelt módszer, amely a döntésekben nagymértékben a szakértők egyéni megítélésére támaszkodik, numerikus konklúzió nélkül [7][8]. A szubjektivitás csökkentésére fuzzy alapú kiterjesztéseket dolgoztak ki, amelyek közül leggyakrabban a Mamdani-fuzzy rendszert alkalmazták [8]. Ez ugyan javította a bizonytalanság kezelését, de továbbra is nyelvi kimeneteket ad, és a defuzzifikációs lépés miatt korlátozottan alkalmazható valós idejű, numerikus kockázatértékelésre. A kutatási rés: jelenleg nincs olyan numerikus, valós idejű és skálázható HAZOP-megoldás, amely ipari környezetben is hatékonyan alkalmazható lenne.

E hiány pótlására jelen kutatás egy Takagi–Sugeno–Kang (TSK) fuzzy modellt és Ant Colony System (ACS) optimalizációt integráló új módszertant mutat be. A TSK-fuzzy közvetlen numerikus kimenete és alacsony számítási igénye lehetővé teszi a valós idejű integrációt ipari folyamatirányító rendszerekbe. Az ACS-optimalizációval kombinált megközelítés csökkenti a szubjektivitást, mérsékeli a nyelvi változók dominanciáját, és pontos, reprodukálható kockázati értékelést biztosít biztonságkritikus környezetben.

KUTATÁSI FELADATUNK ÉS CÉLJAINK

A hidrogéngazdaság széles körű elterjedésének egyik meghatározó feltétele a biztonság fokozása. A hidrogén sajátos fizikai és kémiai tulajdonságai, valamint a történelmi katasztrófák nehezítik a technológia társadalmi és ipari elfogadását, ugyanakkor a környezetvédelmi és energetikai kihívások szükségessé teszik annak fejlesztését és terjedését. Kutatásunk a hidrogéntechnológiák integrációjára, ezen belül a biztonságtechnikai kockázatelemzés fejlesztésére fókuszál. Törekszünk arra, hogy az induktív kutatás szempontjainak a figyelembevételével, általános érvényű, interdiszciplináris modellalkotással járuljunk hozzá a hidrogénbiztonság, hidrogéntechnológia fejlesztéséhez.

Kutatásunk célja egy olyan rendszer alapjainak kidolgozása, amely empirikus, kvalitatív és kvantitatív elemzésekre [9][10][11] támaszkodva lehetővé teszi a már bizonyítottan hatékony HAZOP módszer, on-line adatfeldolgozással támogatott, folyamatos kockázatelemzési alkalmazását. Új szemlélettel kívánunk élni, eltérve a hagyományos, statikus megközelítéstől, mert a hidrogéntechnológiák kockázati sajátosságai szükségessé teszik, hogy a HAZOP dinamikusan integrálódhasson az üzemirányító rendszerek on-line döntéstámogatási moduljába, azonban ehhez új módszertani és számítási feltételek megteremtése szükséges, mert egy hidrogéngázt tartalmazó fizikai rendszerben a bizonytalanság kezelése kulcsfontosságú a megbízható működés és a biztonság fenntartása érdekében.

Hidrogénrendszerek esetében a bizonytalanság mértékét több tényező is növeli: a hidrogén rendkívül kis molekulamérete elősegíti a szivárgást és a diffúziót, a nagy nyomásértékek és gyors nyomásváltozások dinamikus terhelést jelentenek a berendezésekre és a rendszert alkotó elemekre, míg a magas térfogatáramok fokozzák a rendszer instabilitásának lehetőségét. A szenzoradatok zajossága, pontatlansága és időbeli késése további bizonytalansági forrást jelenthet, ami közvetlenül befolyásolja a kockázatértékelést és a valós idejű folyamatirányítást. Solukloei és munkatársai rámutatnak arra, hogy a fuzzy módszertan képes jól kezelni a bizonytalanságot, az általuk megalkotott szabályalapú modell viszont minden iterációnál idő- és erőforrásigényes [8].

Meglátásunk szerint, a probléma gyökere abban rejlik, hogy a Mamdani-fuzzy inference rendszerek (FIS - Fuzzy Inference System) teljesítménye drasztikusan romlik, ha a bemeneti dimenzió nő (pl.: szenzoradatok) vagy ha a szabályok száma megnő [14]. Kutatási célunk, hogy a HAZOP, egy már elkészül üzem esetén, ne csak a tervezési fázisban legyen elvégezve, hanem az üzemeltetés során is, valós idejű alkalmazásként futhasson a háttérben. Ehhez azonban a fuzzy rendszert optimalizálni kell, sőt újra kell értelmezni! Amíg a Mamdani-fuzzy rendszer kimenete „nyelvi” (pl. „közepes kockázat”), s ez defuzzifikációt igényel, addig a Takagi–Sugeno-Kang (TSK) fuzzy rendszer lineáris kimeneti függvényeket használ, így az jelentősen gyorsabb lehet. Ennek az az előnyös tulajdonsága, hogy közvetlenül implementálható a SCADA (Supervisory Control And Data Acquisition), IoT agy DCS (Distributed Control System) rendszerekbe és ezáltal a valós üzemi adatok alapján a biztonság szintje növelhető. Természetesen, ezesetben megoldást kell találnunk a szenzoradatok megbízhatósági elemzésére is.

Az on-line kockázatértékelő rendszerek alkalmazása során több kulcsfontosságú követelménynek kell teljesülnie:

- elengedhetetlen a numerikus kockázatértékelés lehetősége, amely kvantitatív alapot biztosít a döntéshozatalhoz,
- a rendszernek elegendően gyors adatfeldolgozási képességgel kell rendelkeznie az on-line működés fenntartása érdekében, miközben a kockázati becslések megfelelő pontossága is biztosított kell legyen,
- a rendszernek alkalmasnak kell lenni arra, hogy érzékelni tudja a bemeneti adatok megbízhatatlanságát, és ilyen esetekben figyelmeztetést kell küldjön az operátornak, jelezve a manuális beavatkozás vagy a rendszerellenőrzés szükségességét.

Megvizsgálva a fuzzy logika szakirodalmát, megállapítottuk, hogy a TSK-fuzzy rendszerek kiválóan alkalmasak numerikus kockázatbecslésre, ugyanakkor a TSK-szabály-

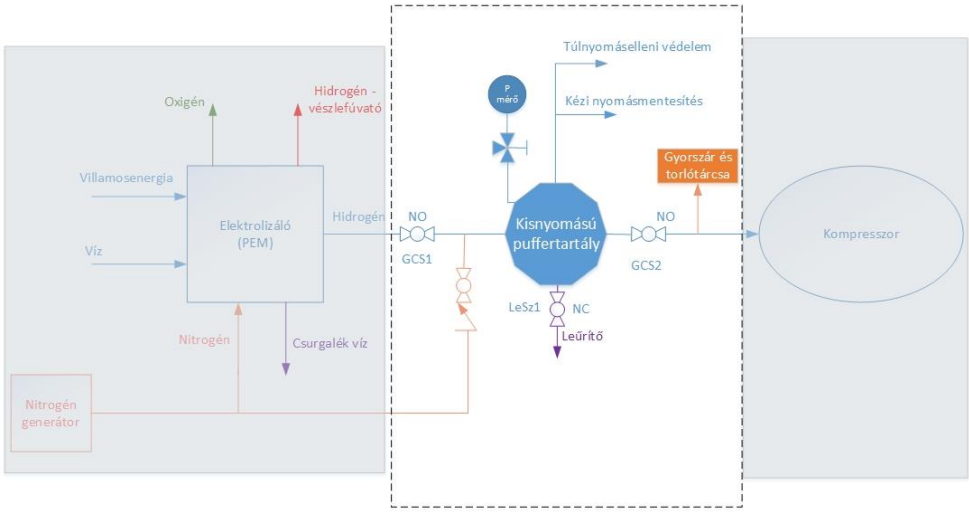
bázis optimalizálása, a paraméterek hangolása, illetve a bemeneti változókhoz tartozó tagfüggvények illesztése szintén jelentős számítási kapacitást és jól definiált keresési stratégiát igényel. E kihívások kezelésére hatékony megoldást kínál a hangyakolónia optimalizációs algoritmus (ACO - Ant Colony Optimization), amely bioinspirált keresési stratégiájával dinamikusan és adaptívan képes feltérképezni az optimális szabálybázist és paraméterkészletet. Feltételezésünk, hogy az ACO algoritmus segítségével a TSK-fuzzy rendszer tanulási folyamata felgyorsítható, mert az algoritmus egy olyan metaheurisztikus módszer, amely gyorsan képes jó megoldásokat keresni nagy keresési térben, így segíthet hatékonyabban megtalálni az optimális TSK paramétereket. Mindeközben növelhető a modell generalizációs képessége és prediktív pontossága is, ami a mi esetünkben annyit tesz, hogy a modell nemcsak a tanulóadatokra ad jó eredményt, hanem ismeretlen, új adatokon is jól teljesíthet, továbbá az előrejelzések pontossága jól közelít a valósághoz. Az iteratív kollektív keresés lehetővé teszi a konzisztens és robusztus szabályrendszerek kialakítását, különösen valós idejű, zajos vagy hiányos adatokkal rendelkező környezetben [12][13].

A feldolgozott szakirodalomban azt tapasztaltuk, hogy a Mamdani elvű fuzzy + HAZOP és ACS (Ant Colony System) kombinációja már kidolgozott eljárás, azonban ez a módszer csak offline körülmények között tesztelt. A valós idejű fuzzy rendszerek összehasonlító elemzése nagyon szűk körben vizsgált kutatási terület és a fuzzy + ACS + valós idejű rendszer alkalmazása a hidrogéninfrastruktúra biztonsági diagnosztikájában jelenleg nem létezik átfogóan kidolgozott, dokumentált, nyilvánosan elérhető formában.

Kidolgoztunk egy új módszert, aminek az ACS-FORCE nevet adtuk: Ant Colony System and Fuzzy Optimization for Real-time Critical Environments. módszerünkben, a fuzzy rendszert támogatja az ACS, ami a szabálystruktúrákat optimalizálja kolóniaviselkedés alapján. Az ACS és TSK kombinációt kifejezetten alkalmasnak találjuk a szabályhalmaz csökkentésére vagy a legveszélyesebb eseményláncok detektálására [13], Megközelítésünk további újdonsága, hogy az optimalizáció eredményként létrejött adathalmazból mi azonnali döntéseket kívánunk támogatni.

A HAGYOMÁNYOS HAZOP BEMUTATÁSA ÉS A TESZTMODELLÜNK

A HAZOP elemzés során egy multidiszciplináris szakértői team, lépésről lépésre elemzi a rendszer minden egyes részét (pl.: szelep nem működést, túlnyomást) és különböző "mi lenne, ha?" kérdéseket tesznek fel. Például: "Mi történne, ha a nyomás túl magas lenne?", "Mi történne, ha a szelep nem működne?". A folyamat szisztematikus és formális, szigorú szabályok mentén alkotott eljárás, melyet új létesítmények esetén szoktak elvégezni. A terjedelmi korlátok nem teszik lehetővé egy teljes HAZOP elemzés lefolytatását, hiszen egy komplex üzem esetén ez akár több ezer oldal terjedelmet is elérhet, ezért mi most egy egyszerűsített, de egy valóságban már megépült hidrogénipari objektum [15] részelemén mutatjuk be a HAZOP módszer gyakorlatát. A modellel szemléltetni kívánjuk a kockázatelemzés módszerét. A bemutatott részelem egy PEM (Polymer Electrolyte Membrane) elektrolízisen alapuló, hidrogén előállító üzem, kisnyomású puffertartályának vizsgálata. Az elemzés célja a lehetséges veszélyek és működési akadályok azonosítása a puffertartály működése során, különösen a nyomás, áramlás és a szelep műveletek vonatkozásában.



1. ábra: A számításokhoz és a szemléltetéshez használt tesztmodellünk, saját szerkesztés

Elemzési paraméterek: Nyomás (37-43 bar közötti normál tartomány), áramlás, szelepműveletek. Vezényszavak (guide words): magas/alacsony; túlzott/hiányos; megfelelő/nem megfelelő.

Paraméter	Lehetséges eltérés	Lehetséges okok	Lehetséges következmények	Meglévő védelmi intézkedések	Ajánlott intézkedések
Nyomás	Túl magas	Nyomásmentesítő szelep meghibásodása	Tartály túlnyomása, robbanás veszélye	Túlnyomás elleni védelem, nyomásmérő	Nyomásmentesítő szelep rendszeres tesztelése és karbantartása
Nyomás	Túl alacsony	Szivárgás a csatlakozásoknál (GCS1, GCS2), hibás leűrítés	Hidrogénvesztés, alacsony nyomás miatti folyamat megszakadása	Nyomásmérő, redundáns töltőrendszer	Szivárgásérzékelők telepítése, csatlakozások gyakori ellenőrzése
Áramlás	Túlzott áramlás	Node 1 hiba, Nod 9 hiba,	Túlnyomás, tartály túlterhelése, repedés, szivárgás, robbanás	Nyomásmérő, túlnyomás elleni védelem	Töltési folyamat felügyelete,elektorolizáló ellenőrzése, nitrogéngenerátor ellenőrzése
Áramlás	Hiányos áramlás	GCS2, GCS2 gömcsap vagy gyorszár hibás működése, szivárgás	Puffertartály leűrülése, nyomáshiány, kompresszor leállás, szivárgás, szúróláng vagy robbanás	Gyorszár és gömbcsapok ellenőrzése, Node 1 kilépő nyomás ellenőrzése	Gömcsapok és gyorszár karbantartása, kézi működtetés tesztelése, Nyomásmérők ellenőrzése a Nod 1 oldalon, majd a kisnyomású puffertartály oldalán
Szelepművelet	Nem megfelelő zárás	Gömcsapok (GCS1, GCS2) vagy gyorszár meghibásodása	Szivárgás, nyomásproblémák, Szúróláng, robbanás	Redundáns szelepek	Szelepek rendszeres karbantartása, működésük ellenőrzése
Szelepművelet	Nem megfelelő nyitás	Kézi nyomásmentesítő szelep elakadása	Nyomás felgyülemlése, túlnyomás	Túlnyomás elleni védelem	Kézi szelep rendszeres tesztelése

1. táblázat :A klasszikus HAZOP formája és struktúrája a tesztmodellre, saját szerkesztés

Ahogyan az 1. táblázatban is látható, a HAZOP egy kvalitatív módszer, amelynek eredményei szöveges leírások formájában jelennek meg. A rendszer számos előnnyel rendelkezik, ugyanakkor hátrányai közé tartozik, hogy nem kezeli a kombinált hibákat, jelentős idő- és erőforrásigénye van, valamint erősen függ a „guide word” (vezényszó) alapú megközelítéstől. Ennek következtében atipikus hibák rejtve maradhatnak, ha azok nem sorolha-

tók be egy tipikus vezényszó kategóriába. Továbbá, az emberi tényezők (például a tapasztalat, a kreativitás, a szubjektív torzítások és a csoportdinamika) szintén befolyásolhatják a feltárt veszélyek körét [4][5][16][17].

Az egyik ígéretes irány a fuzzy logika integrálása a HAZOP-ba. A szakirodalom számos eredménnyel igazolja a fuzzy logika hozzáadott értékét, így a hagyományos HAZOP bizonytalanságai jobban kezelhetők, és reálisabb kockázati szint besorolás érhető el [18][19][20][21]. Fontos kiemelni, hogy a fuzzy-HAZOP kiegészíti, nem helyettesíti a hagyományos HAZOP-ot. A elemzés alapjait továbbra is a guide word-alapú brainstorming adja, s ezt követően lép be a fuzzy logika, a számszerűsítés és értékelés fázisában. Így a két módszer ötvözése biztosítja, hogy ne vesszen el a HAZOP kreatív, feltáró jellege, viszont a kimenet jobban felhasználható legyen a kockázatkezelési döntésekhez.

Anomáliafigyelés és a Mamdani-fuzzy alkalmazása a tesztmodellen

Ebben az egyszerű modellben, három változót (nyomás, áramlás, szelepállapot) és 18 fuzzy-szabályt írhatunk fel, melyből egy szabály logikailag így írható fel: *IF nyomás IS magas AND áramlás IS alacsony AND GCS2 IS zárt THEN kockázat IS nagy*.

A National Renewable Energy Laboratory (NREL) és a Marylandi Egyetem közös kutatásában megállapították, hogy a hidrogénrendszerekben a szivárgás a leggyakoribb meghibásodási mód. A tanulmány hangsúlyozza, hogy a szivárgások gyakoriságának és mértékének bizonytalansága korlátozza a kockázatok pontos megértését és kezelését [22]. Az Oxford Energy Institute, 2024-es jelentése szerint a hidrogénellátási láncban, a legmagasabb szivárgási arányok a föld feletti tartálytárolás esetén fordulhatnak elő [23]. A hidrogénipari rendszereknél a szivárgás és annak detektálása kritikus fontosságú, mert a szivárgás következtében tűz és robbanás egyaránt kialakulhat. A szakirodalmi adatok szerint a nem észlelt szivárgások 25-40%-al csökkenthetik a biztonsági rendszerek megbízhatóságát a hidrogéninfrastruktúrában [24][25][26][27]. Tekintettel a hidrogénrendszer sajátosságaként (nehezen észlelhető, katasztrofális kimenetű szivárgás) megjelenő kockázatok növekedésére, a modellünket egy anomáliafigyelő ággal bővítettük, ami konkrétan azt jelenti, hogy ha a GCS2 szelep zárt állapotában áramlást érzékelünk, akkor a következő üzemszerű esetek fordulhatnak elő, melyeket a DCS rendszer érzékel:

- túlnyomás elleni védelem (PRV - Pressure Relief Valve) aktív, vagy
- kézi nyomásmentesítő szelep vagy a leürítő-szelep nyitva,

Viszont ha a DCS-ben nincs aktív jel, a fenti két állapotra és minden, tartályból „kivezető” szelep zárt állapotban, mégis van áramlási jel a bemeneti oldalon, akkor a rendszer valahol szivárog.

Annak érdekében, hogy az anomáliát detektálhassunk a Mamdani-fuzzy rendszerben, definiálni kell egy „mérhető” fuzzy kategóriát is az áramlási univerzumban (eddig volt: túlzott, normál, hiányos, most új változó: mérhető), ez viszont a szabályok számát növelné. A klasszikus fuzzy szabályterünk eddig 18 szabályt (3x3x2) tartalmazott, a bővített szabálytér 24 szabályra (3x4x2) növekedne, de annak érdekében, hogy az ilyen eseteket hatékonyan, nagyobb számítási kapacitás igénye nélkül kezelni tudjuk, logikai értéket állítunk be, s csak akkor figyeljük, ha egy feltétel (pl.: GCS2=0, vagyis zárt) igaz. Amennyiben így járunk el, ekkor nem növeljük meg a szabályrendszer komplexitását.

A modell validálása érdekében a MATLAB-ban (R2024b) a Fuzzy Logic Designer alkalmazás segítségével megterveztünk egy fuzzy következtetési rendszert (FIS) így a tesztelést is el tudtuk végezni, illetve hangolni tudtuk a modellünk viselkedését. A felhasznált validációs mutatók és értelmezésük:

Rövidítés	Jelentés	Értelmezés
N = Sample size	minta száma	A vizsgált minták (szenzoradatok, esetek) száma összesen
TP = True Positive	igaz pozitív	A modell helyesen riasztott, amikor tényleg volt kockázat
TN = True Negative	igaz negatív	A modell helyesen nem riasztott, mert nem volt veszély
FP = False Positive	hamis pozitív	A modell tévesen riasztott, pedig nem volt veszély
FN = False Negative	hamis negatív	A modell nem riasztott, pedig kellett volna

2. táblázat: A mutatók értelmezése, saját szerkesztés

Mutató neve	Jelentés	Képlet	Jelentőség
Találati arány (TPR)	A modell helyesen azonosította a valós kockázatos eseteket	$\frac{TP}{TP+FN}$	Mennyire érzékeny a modell
Fals pozitív arány (FPR)	A modell akkor is riasztott, amikor nem kellett volna	$\frac{FP}{FP+TN}$	Mennyire stabil, kerüli a vakriasztást
Fedezet (Coverage)	A modell hány mintát ítélt kritikusnak az összesből	$\frac{TP+FP}{N}$	Az érzékelési aktivitás mértéke
Biztonsági érzékenységi index (SSI)	A kockázatos minták hány százalékát azonosítja hatékonyan	$\frac{TP}{TP+FP+FN}$	Kombinált hatékonysági mutató

3. táblázat: Validációs mutatók számítása ás értelmezése, saját szerkesztés

Szimulációs eredményeink 1000 mintára

N - összes minta száma		1000
Összes pozitív minta - valóban veszélyes		344
Összes negatív minta - valóban biztonságos		656
TP	helyes riasztás, valódi veszély	330
TN	helyesen, nem riasztott	625
FP	téves riasztás, nem volt kockázat	31
FN	veszélyes esetek száma, a modell nem érzékelte	14
TPR	A valós veszélyek 96%-át detektálta a modell	0,959
FPR	A modell 10-szer tévesen riasztott	0,047
Coverage	Az esetek 36,1%-ra adott valamilyen riasztást.	0,361
SSI	A modell megbízhatóan és biztonságosan működik, a legtöbb valódi veszélyt képes volt azonosítani, kevés fals riasztással.	0,880

4. táblázat: MATLAB-szimulációs eredményeink, saját szerkesztés

Következtetések

- A riasztások nem túlérzékenyek: a rendszer nem riaszt minden magas nyomásra vagy nagy áramlásra.
- A fuzzy logika érzékeny a kombinációkra, különösen határérték közeli sávokra, ezáltal a modell:
    - korán jelzi a veszélyt, mielőtt a fizikai állapot kritikussá válna,
    - de nem túl gyakran, tehát nincs riasztási infláció.

A TSK-FUZZY ALKALMAZÁSA A TESZTMODELLEN

Egyszerű megoldás: IF Nyomás IS Magas AND Áramlás IS Alacsony AND GCS2 IS Zárt THEN Kockázat = a_1·Nyomás + a_2·Áramlás +a3·Szelepállapot + Konstans

Anomália detektálással: IF Nyomás IS Magas AND Áramlás IS Alacsony AND GCS2 IS Zárt THEN Kockázat = a_1·Nyomás + a_2·Áramlás +a3·Szelepállapot + a4· 1anomális + Konstans

Bemenetek

Az újdonság a Mamdani–fuzzyhoz képest, hogy itt megjelenik három bemeneti változó (x_1, x_2, x_3), majd a logikai blokk belsejében megtörténik a súlyokkal kombinált lineáris egyenlet kiszámítása. Az egyenlet eredménye pedig egy szám, szemben a Mamdani-fuzzy esetével, ahol egy szöveges eredmény van, amit ahhoz, hogy számot kapjunk még további műveletek (aggregáció és defuzzifikáció) szükségesek.

Bemenetek	Jellemző	Paraméter
x_1	Nyomás (bar)	normál (37-43)
x_2	Áramlás	hiányos/normál/túlzott
x_3	GCS2 - szelep	0: zárt, 1: nyitott

5. táblázat: A TSK-fuzzy paraméterei, saját szerkesztés

Súlyozás

A fuzzy logikán alapuló döntéstámogató rendszerek (különösen igaz ez a Takagi–Sugeno–Kang (TSK) típusú fuzzy modellekre) gyakorlati alkalmazása során a legnagyobb kihívást a súlyparaméterek meghatározása jelenti. Mivel minden fuzzy szabályhoz külön lineáris következmény-egyenlet tartozik, amelyben a bemeneti változókhoz súlyokat (pl.: a_1,a_2,…a_n) és egy konstans tagot (b) kell rendelni, a teljes modell paramétereinek száma drámaian megnő a bemeneti dimenziók számának növekedésével. Egy tíz bemenetet tartalmazó rendszer, három-három fuzzy taggal változónként, már több mint ötvenezer szabály kombinációját igényli, ami közel hétszázezer súlyérték manuális beállítását jelentené. Ez gyakorlati szempontból szinte kivitelezhetetlen, különösen valós ipari környezetben, ahol a rendszer működése nem tesz lehetővé azonnali visszacsatolást az egyes súlyok hatásáról, és a döntési következmények akár csak hónapokkal vagy évekkel később jelentkezhetnek.

Nehezíti a helyzetet, hogy a bemeneti változók közötti hatások nem lineárisak, azaz a nyomás súlya például az áramlás és a szelepállapot függvényében más és más módon befolyásolja a kockázati szintet. Ilyen esetekben a szakértői intuíció, bár hasznos a szabályrendszer alapvázának kidolgozásában, nem alkalmas nagy dimenziójú rendszerek súlyainak precíz és optimalizált meghatározására. Emellett az ipari alkalmazásokban gyakran több – egymással „versengő” célkitűzésnek kell egyidejűleg megfelelni (pl.: magas találati arány,

alacsony fals pozitív arány, nagy érzékenység és üzemi stabilitás), melyek kézi beállítással nem hozhatók egyensúlyba.

Kutatási modellünkben, a kezdeti súlyokat ember állíthatja be, mely korrigálható, finomhangolható, de távlati szinten ezt a feladatot egy gépitanulási-algoritmus tanítja be a rendszernek, egy olyan optimalizásós módszer segítségével, ami a predikciós hibára nézve végez el egy minimum-követelményű optimalizációt. A példa kedvéért mi most szemléltetjük a számítási folyamatot, az áramlás súlyának változtatásával, de a lenti táblázatban összszefoglaljuk a súlyok mértékét és azok hatását.

Jellemző	Súlyozás	Hatás
Nyomás	+0,7	A pozitív előjel, növeli a kockázatot, egységnyi nyomásnövekedés, 0,7 egységnyi kockázatnövekedést okoz
Áramlás	-1,8 (túlsúlyozott állapot)	Ez negatív súly: ha nő az áramlás, csökken a kockázat. Magas áramlás esetén valószínű, hogy nincs torlódás, ezért nem alakul ki túlnyomás. A szám abszolút értéke nagy, mert az áramlás gyorsan kompenzálhatja a nyomást.
Szelepállapot	+ 0,8·(1 – GCS2)	zárt= 0, nyitott= 1, Ha zárt: (1 – GCS2): 1-0 = 1 → növeli a kockázatot, Ha nyitott: (1-GCS2): 1-1= 0 → csökkenti a kockázatot
Szivárgás	+1,2	Szivárgás detektálva, anomália detektálás aktív
Konstans	+8	A modellben (kritikus biztonság) arra törekedtünk, hogy semmilyen körülmények között ne adjon teljes biztonsági visszajelzést, s erre a konstans választása egy ideális lehetőség.

6. táblázat: TSK súlyozás és annak magyarázata, saját szerkesztés

ACS alkalmazásának indoklása

IF Nyomás IS Magas AND Áramlás IS Alacsony AND GCS2 IS Zárt THEN Kockázat $= 0{,}7 \times x_1 - 1{,}8 \times x_2 + 0{,}8 \times (1 - x_3) + 1{,}2 \times 1 + 8$

Ha a nyomást (x_1=53,7 bar), az áramlást (x_2=22,1 kg/h) és a szelepértéket (x_3=0) egy random, fix értéken tartjuk, a konstans értéke +8, akkor az egyenletek súlyozása és annak hatása könnyedén számítható. Az áramlás súlyát három állapot szerint változtatjuk, lesz egy

- túlsúlyozott → Kockázat1
- normál → Kockázat2
- végül egy alulsúlyozott áramlási paraméterünk → Kockázat3

Kockázat1 $= 0{,}7 \times 53{,}7 \ - 1{,}8 \times 22{,}1 + 0{,}8 \times (1 - 0) + 1{,}2 \times 1 + 8 = 7{,}81$

Kockázat2 $= 0{,}7 \times 53{,}7 - 1 \times 22{,}1 + 0{,}8 \times (1 - 0) + 1{,}2 \times 1 + 8 = 25{,}49$

Kockázat3 $= 0{,}7 \times 53{,}7 - 0{,}2 \times 22{,}1 + 0{,}8 \times (1 - 0) + 1{,}2 \times 1 + 8 = 43{,}17$

Súlyozás	Kockázat értéke	Jelentés
Túlsúlyozott áramlás: a2=-1,8	7,81	Az áramlás negatív súlya nagyon erősen csökkenti a kockázati értéket → alacsony kockázat még veszélyes helyzetben is

Súlyozás	Kockázat értéke	Jelentés
Optimális súlyozású áramlás: a2=1	25,49	Az áramlás és nyomás kiegyensúlyozott → életszerű kockázati szint
Alulsúlyozott áramlás: a2=0,2	43,17	Az áramlás hatása túl gyenge → a modell túlságosan kockázatosnak ítél szinte minden helyzetet, túlérzékennyé válik.

7. táblázat: A súlyparaméterek megválasztásának hatása az eredményre, saját szerkesztés

Mindezek fényében belátható, hogy az ilyen fuzzy rendszerek hatékony és megbízható hangolásához automatizált optimalizálási módszerekre van szükség. Ilyen módszer például az ACS, amely képes valós vagy szintetikusan generált adatok alapján iteratív módon javítani a szabályok és a hozzájuk tartozó súlyok teljesítményét. Ezen megközelítés a klasszikus kézi hangolással szemben nemcsak skálázható, hanem objektíven értékelhető is a validációs mutatók (TP, FP, FN, TN) alapján, így megbízható és prediktív megoldást nyújtanak.

Mamdani-fuzzy számítási lépések	TSK-fuzzy számítási lépések
1A - Fuzzifikáció, a bemeneti tagsági függvényekkel $\mu_{Magas}^{Nyomás}(x_1) \in [0,1]$ $\mu_{Alacsony}^{Áramlás}(x_2) \in [0,1]$	1B - Fuzzifikáció $\mu_i^{(1)}(x_1), \quad \mu_j^{(2)}(x_2)$
2A - Szabály aktiválás – minimum operátorra $\mu_{akt} = min\left(\mu_{Magas}(x1), \mu_{Alacsony}(x2)\right)$	2B - Szabály aktiválás, szabály erőssége: $w_k = y_i^{(1)}(x1) \times y_j^{(2)}(x2)$
3A - Kimeneti szabály leképzése pl.: Nagy kockázat	3B - Szabály kimenetének számítása: $z_k = a_1^{(k)}(x1) + a_2^{(k)}(x2) + c^{(k)}$
4A - Aggregáció, itt több szabály eredményét egyesítjük $\mu_{outp(y)} = max(\mu_1(y1), \mu_2(y2) \dots)$	4B - Súlyozott átlag képzése: $y^* = \frac{\sum_{k=1}^{N} w_k \times z_k}{\sum_{k=1}^{N} w_k}$
5A - Defuzzifikáció, pl. súlyozott középpont. $y^* = \frac{\int y \times \mu_{outp(y)}\, dy}{\int \mu_{outp(y)}\, dy}$	

8. táblázat: Mamdani-fuzzy és TSK-fuzzy összehasonlítása, saját szerkesztés

SÚLYOK OPTIMALIZÁLÁSA AZ ON-LINE KOCKÁZATELEMZÉS

TSK-fuzzy fent bemutatott alkalmazása igényli a súlyparaméterek optimális megválasztását, ami lényegesen befolyásolja s a rendszer hatékonyságát és a megbízhatóságát. A korábbi példákban is láthattuk, hogy bár egyetlen szabály szerkezete numerikusan kezelhető, egy valós rendszerben akár több száz bemeneti kombináció, és ezzel együtt több ezer

paraméter is jelen lehet. A súlyok kézi beállítása nemcsak, hogy szubjektív és időigényes, hanem skálázhatatlan is, és nem biztosítja a szabályok közötti optimalizált együttműködést. Ez különösen igaz, amikor a rendszer célja nemcsak a helyes kockázati előrejelzés, hanem a riasztási logika optimalizálása is (pl.: a fals pozitív (FP) riasztások számának csökkentése mellett a biztonsági érzékenység növelése).

Az ilyen összetett szabálytér automatikus optimalizálására az Ant Colony Optimization (ACO) vagy annak célzottabb változata, az Ant Colony System (ACS) algoritmus kiváló eszköznek bizonyul, melyet Shokouhifar [12] és Solukloei [8] munkáikban már igazoltak. Az ACS egy olyan metaheurisztikus keresési módszer, amely természetes kolóniák viselkedését imitálva képes hatékonyan felfedezni a szabálytér legjobb „útjait" vagyis a legideálisabb súlykombinációit. A TSK-fuzzy rendszerek esetén ez a módszer nem csupán a szabályok súlyainak finomhangolására alkalmazható, hanem akár az egész szabályhalmaz redundanciamentesítésére is használható. A TSK-fuzzy és az ACS együttes, komplex alkalmazásával, eredményként egy egységes, prediktíven is pontos és iparilag is adaptálható fuzzy modell jön létre. Az ACS-alapú optimalizálással nemcsak a számítási hatékonyság javítható, hanem a biztonságtechnikai és az operátori szintű döntéstámogatás is egységes és reprodukálható keretrendszerbe foglalható. Ennek a keretrendszernek az ACS-FORCE - Ant Colony System and Fuzzy Optimization for Real-time Critical Environments) nevet adtuk.

A TSK-fuzzy szabályrendszerünk implementálása az ACS optimalizáláshoz

Az ACS valójában egy sztochasztikus keresési algoritmus, melyet jellemzően kombinatorikus optimalizálási problémák megoldására használunk, további előnye, hogy a mérnöki gyakorlatban jól ismert gráfként modellezhető. A legismertebb kapcsolódó matematika kérdések, a Hamilton-út, a Hamilton-kör vagy az utazó ügynök (TSP - Travelling Salesman Problem) problémája [13].

Szakirodalomkutatásra támaszkodva, bemutattuk, hogy az Ant Colony System (ACS) algoritmus hatékonyan alkalmazható a TSK-fuzzy súlyparaméterek optimalizálására [12], [8]. Az ACS algoritmus a természetes hangyakolónia táplálékszerző viselkedését modellezi. A folyamat lényege, hogy a megoldási tér elemei közötti átmeneteket **feromonnymok** és **heurisztikus információk** vezérlik, amelyeket a „hangyák" lépésről lépésre frissítenek a megoldásépítés során. Kutatásunkban az ACS-t a TSK-fuzzy szabályok konzekvens súlyvektorainak és tagfüggvény-paramétereinek optimalizálására alkalmazzuk. A keresési tér egy irányított gráffal reprezentálható. A későbbiekben ennek részletes matematikai és algoritmikus leírását megadjuk, kitérve a gráfmodell felépítésére, a hangyák útvonalépítési szabályára és a feromonfrissítés lépéseire.

Modellünk TSK szabálya

$$Kockázat = a_1 \cdot Nyomás + a_2 \cdot Áramlás + a_3 \cdot Szelepállapot + a_4 \cdot 1_{anomális} + Konstans$$
$$Kockázat = a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot (1-x_3) + a_4 \cdot anomália + b$$

$$y = \sum_{i=1}^{n} a_i x_i + b$$

$x_i - bemeneti\ változók\ (pl.: nyomás, áramlás, szelepállapot)$
$a_i \in \mathbb{R} -\ a\ tanulandó\ súly$
$b_i \in \mathbb{R} -\ a\ konstans\ tag$
$y -\ a\ rendszer\ által\ becsült\ súly$

$$W = \left\{ \vec{w}^{(r)} = \left[a_1^{(r)}, a_2^{(r)}, \dots, a_n^{(r)}, b^{(r)} \right] \right\}_{r=1}^{R}$$

$W - optimális\ súlyhalmaz, ami\ maximalizálja\ a\ fuzzy\ rendszerünk\ teljesítményét$
$\vec{w}^{(r)} - \ az\ r\ szabályhoz\ tartozó\ súlyvektor$
$a_i^{(r)} - \ az\ r szabályhoz\ tartozó, i\ bemenet\ súlya$
$b^{(r)} - \ az\ r szabályhoz\ tartozó, konstans\ tag$
R – a szabályok összes száma

Az ACS alkalmazásának kettő fontos célja van, az egyik a súlyvektorok optimalizálás, a másik az összes szabály kombinációjának szűkítése, végeredményben a gyors számítás lehetővé tételé.

- az összes szabályhoz tartozó súlyvektor és konstans (a1,a2,a3,a4,b) optimalizálása, így minden szabályhoz tartozik egy súlyvektor,

$$\vec{w}^{(r)} = \left[a_1{}^{(r)}, a_2{}^{(r)}, \dots, a_n{}^{(r)}, b^{(r)} \right] \in \mathbb{R}^{n+1}$$

  az összes szabály pedig együtt alkot egy teljes modell-leíró vektort, amely

$$W = \left[\vec{w}^{(1)}, \vec{w}^{(2)}, \dots, \vec{w}^{(R)} \right] \in \mathbb{R}^{n+1}$$

- az összes szabály kombinációjának szűkítése (redundáns, nem informatív szabályok kiszűrése, így a számítási folyamatok gyorsabbá tétele)

A teljes súlytér: $\Omega \subset \mathbb{R}^{R(n+1)}, \rightarrow \Omega \subset \mathbb{R}^{18(4+1)} = \mathbb{R}^{90}$

$\Omega - a\ megoldási\ tér$
$\mathbb{R} - a\ valós\ számok\ halmaza, tehát\ az\ optimalizálás\ folytonos$
R – a fuzzy szabályok száma a térben
n – a bemeneti változók száma (pl.: nyomás, áramlás, szelep)
+1 – a konstans tag

Ez azt jelenti, hogy egy hangya 90 paraméterből álló vektort épít, és ezt próbálja optimalizálni. A hangyák ebben a 90-dimenziós súlytérben mozognak, minden iterációban egy új súlykészletet generálnak, és a fuzzy modell ez alapján számolja a rendszerünk kockázat szintjét, majd a teljesítmény (pl. találati arány, hibaarány) visszacsatolásával a feromoneloszlás frissül.

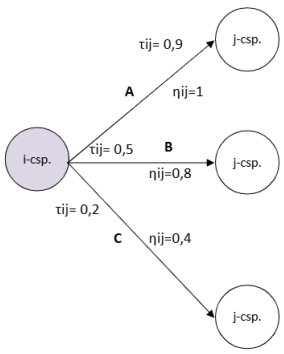
A hangyák mozgása az élen a valószínűségi döntési szabály alapján

$$P_{ij}^{k} = \begin{cases} \dfrac{[\tau_{ij}]^{\alpha} \times [\eta_{ij}]^{\beta}}{\sum_{l \in N_k} [\tau_{il}]^{\alpha} \times [\eta_{il}]^{\beta}} & ha\ j \in N_k \\ 0 & különben \end{cases}$$

$P_{ij}^{k} - a\ k - adik\ hangya\ valószínűsége\ arra, hogy\ i \rightarrow j\ lépést\ választ$
$i - \ a\ jelenlegi\ csomópont, ahol\ a\ hangya\ van$
$j - \ a\ célcsomópont, amelyre\ a\ hangya\ lépni\ szeretne$
$l \in N_i^k - \ az\ összes\ elérhető\ célcsomópont\ az\ i - ből\ kiindulva\ (a\ k - adik\ hangya\ számára)$
$\tau_{ij} - az\ adott\ paraméterértékhez\ tartozó\ feromonintenzitás$
$\eta_{ij} - heurisztikus\ érték, mennyire\ jó\ az\ i \rightarrow j\ él\ azonnali\ szempontból$

$$\eta_{ij} = \frac{1}{1 + hiba_{ij}}$$

$\alpha, \beta \in \mathbb{R}^{+} - súlyok\ a\ feromon\ és\ heurisztika\ között$
N_i^k – a még látogatható csomópontok a k-adik hangya számára



Példa egy hangya mozgására, melyen látható, hogy a magas feromonszint és a jó heurisztika kombinációja dominál a döntést.

$$P_{ij} = \frac{[\tau_{ij}]^{\alpha} \times [\eta_{ij}]^{\beta}}{\sum_l [\tau_{il}]^{\alpha} \times [\eta_{il}]^{\beta}}$$

Él	Feromon	Heurisztika (β)	Valószínűség
A	0,9	1	71,9%: legvonzóbb
B	0,5	0,8	25,6% közepes
C	0,2	0,4	2,6% alig választott

Ha a heurisztika súlyát (β) változtatjuk és fokozzuk az erősségét, akkor a rendszer egyre inkább a „legjobb" (leginkább illeszkedő) opció felé húz, és a többi lehetőséget szinte kizárja. Ha β túl nagy, a rendszer korai konvergenciára hajlamos (nem próbál ki új lehetőségeket – túl „biztos").
Feromon frissítés:

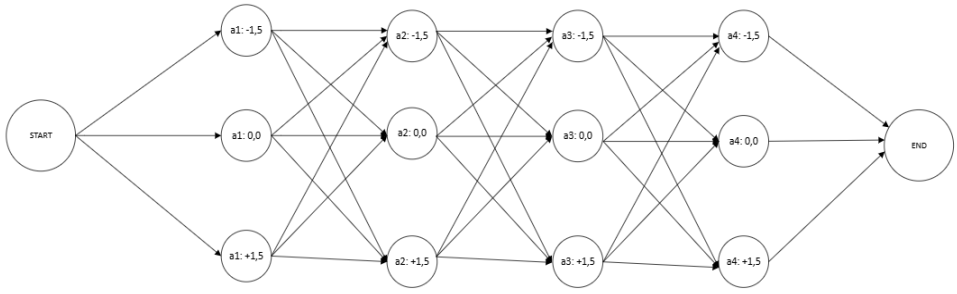
$$\boldsymbol{\tau_{ij} \leftarrow (1-\rho) \times \tau_{ij} + \rho \times \Delta\tau_{ij}^{best}}$$

$$\boldsymbol{\Delta\tau_{ij}^{best} = \frac{Q}{f_{(\vec{w})best}}}$$

$\rho - feromonpárolgási\ ráta\ \rho \in (0,1)$
$Q - konstans$
$az\ f_{best} - legjobb\ megoldás\ költsége\ (vagy\ fitness)$

A súlyparaméterek optimalizálását gráf-reprezentációval végezzük, ahol:

- A csomópontok a fuzzy szabályok egy-egy súlyparaméterének lehetséges értékeit jelentik (például: -1,5; 0.0, +1,5)
- Az élek a lehetséges átmeneteket jelölik két egymást követő súlykomponens értékei között.
- Egy „hangya" teljes útvonala egy súlyvektor felépítésének felel meg $\vec{w} = [a_1, a_2, a_3]$



2. ábra: ACS - súlyválasztási optimalizációt bemutató gráf, saját szerkesztés

Ez a megközelítés lehetővé teszi, hogy az ACS hatékonyan feltérképezze a súlyvektor teljes keresési terét, miközben a feromonfrissítés adaptívan a jobb szabálykonfigurációk felé tereli a keresést, ezáltal javítva a fuzzy rendszer teljesítményét és konvergenciáját.

Definiált célfüggvényünk

$$f_{(\vec{w})} = \alpha \times TPR - \beta \times FPR + \gamma \times Coverage + \delta \times SSI$$

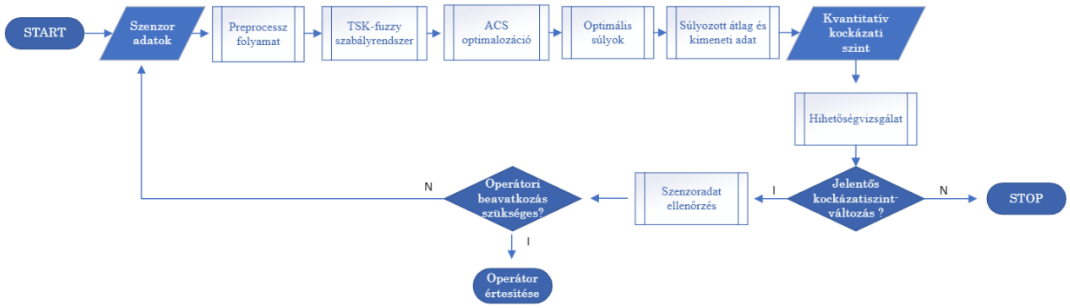
TPR, FPR, Coverage, SSI – a 3. táblázat alapján
$\alpha, \beta, \gamma, \delta \in \mathbb{R}^+ -$ *súlytényezők*

A legjobb súlykombinációkat tartalmazó szabályhalmaz az ACS-FORCE eredménye, így az prediktíven pontos, alacsony riasztási hibarátával rendelkezik, adaptív a bemeneti tér változására és alkalmas a valós idejű alkalmazásra is

$$\overrightarrow{w^*} = \underset{\vec{w} \in \Omega}{arg\,max\, f(\vec{w})}$$

$\overrightarrow{w^*} -$ *az optimális súlyvektor*
$arg\,max\, f(\vec{w}) -$ *maximalizálja az* $f(\vec{w})$*értékét*
$\vec{w} \in \Omega$ *- a keresési térben*

Az ACS-FORCE folyamatábrája



3. ábra: Az ACS-FORCE egyszerűsített folyamatábrája, saját szerkesztés

Ahogyan a 3. ábrán is látható, hogy az ACS-FORCE algoritmus elvégzi az automatikus szenzoradat-ellenőrzést, amennyiben a hihetőség vizsgálat jelentős eltérést talál. A visszacsatolással növelni tudjuk a modell megbízhatóságát.

Jellemző	csak TSK	ACS-FORCE eredmény
Találati arány (TPR)	0,959	0,96
Fals pozitív arány (FPR)	0,01	0,01
Fedezet (Coverage)	0,361	0,88
Biztonsági érzékenység (SSI)	0,88	0,91

9. táblázat: Szimulációs eredményeink, saját szerkesztés

Az ACS-FORCE automatikusan finomhangolta a szabályokhoz tartozó súlyvektorokat annak érdekében, hogy minimalizálja a fals riasztások arányát (FPR), miközben maximalizálja a predikciós érzékenységet (TPR) a valós lefedettség és az SSI értéket. Bár az önmagában használt TSK-fuzzy TPR és FPR szempontjából kiemelkedően pontos volt, a fedezet és az SSI alacsony értéken maradt, mely arra utal, hogy a modell a potenciálisan kockázatos állapotok jelentős részét nem aktiválja döntési szinten.

Ezzel szemben az ACS-FORCE képes a teljes bemeneti tér nagy részét lefedni. A szabályhalmaz több, eltérő fuzzy premisszát ölel fel, ezáltal a lefedett kockázati állapotok aránya drámaian megnő (88%), miközben a predikciós mutatók (TPR, FPR) is megtartják kiváló szintjüket.

Következtetések, javaslatok

A Mamdani-fuzzy rendszerek intuitív szabályformájuknak köszönhetően könnyen értelmezhetők, ugyanakkor gyakorlati korlátot jelent az aggregáció és a defuzzifikáció számítási összetettsége, különösen igaz ez nagyméretű szabályrendszerek esetén.

Megállapítottuk, hogy a Mamdani-fuzzy rendszerek nyelvi alapú kimeneteket generálnak, amelyeket defuzzifikációval kell numerikus értékké alakítani, ezzel szemben a TSK-fuzzy modellek lineáris vagy affin függvényeket alkalmaznak, így az egyes szabályok kimenete már eleve numerikus. Az aggregáció ebben az esetben egyszerű súlyozott átlagként számítható, a defuzzifikáció pedig a numerikus érték miatt teljes egészében szükségtelen. Ennek köszönhetően a TSK-fuzzy rendszerek lényegesen gyorsabban és alacsonyabb számítási igénnyel állítanak elő eredményeket (9. táblázat).

Mindezek alapján megállapítható, hogy a TSK-fuzzy modell egyértelműen előnyösebb választás a Mamdani-fuzzy modellel szemben olyan biztonságkritikus rendszerekben, ahol kvantitatív kockázatbecslésre és valós idejű prediktív döntéshozatalra van szükség. A valós idejű feldolgozás képessége lehetővé teszi a folyamatos és pontos kockázatszint-számítást online adatforrások felhasználásával (9. táblázat).

Tulajdonság	Mamdani-fuzzy	TSK-fuzzy
Szabálykimenet típusa	Nyelvi	Numerikus
Defuzzifikáció szükséges?	Igen	Nem
Kimeneti folytonosság	Diszkrét	Folytonos
A kimenet deriválható	Nem	Igen
Számítási idő (1000 minta)	1,2 másodperc	0,15 másodperc
Automatizálhatóság	Korlátozott	Teljes mértékben
Valós idejű alkalmazás	Korlátozott	Alkalmas

10. táblázat: Összefoglaló záblázat a Mamdani és TSK-fuzzy összehasonlítására

A TSK-fuzzy rendszer paraméterezhető súlystruktúrája lehetővé tette, hogy a modell érzékenyen reagáljon a bemeneti jellemzők változásaira, miközben fenntartotta az egyensúlyt a biztonsági érzékenység és a túlriasztási hajlam között. E tulajdonsága alkalmassá teszi olyan ipari környezetekben való alkalmazásra, ahol a sokváltozós, dinamikusan változó üzemi állapotok folyamatos figyelése és a kockázati szintek megbízható becslése kulcsfontosságú.

A TSK-fuzzy rendszer előnyösen integrálható prediktív modellekbe, különösen akkor, ha a szabályegyenletek súlyparamétereit Ant Colony System (ACS) optimalizációval hangoljuk. E megközelítés a tesztjeinkben növelte a prediktív pontosságot és robusztusságot, még zajos vagy részben hiányos bemeneti adatok esetén is. Szimulációs eredményeken keresztül igazoltuk a z ACS-FORCE létjogosultságát és számítási pontosságát (8. táblázat).

Az alacsony számítási igény és a gyorsan rendelkezésre álló numerikus eredmények révén az ACS-FORCE keretrendszer transzparenssé és auditálhatóvá teszi a kockázatértékelési folyamatot, ami kiemelten fontos biztonságkritikus ipari rendszerek esetén.

Terveink a kutatási perspektíva szempontjából:

- a rendszer teljesítményének validálása nagyobb mintaszámú és több bemeneti változót tartalmazó adathalmazon, valamint egy bővített modellverzió megvalósítása, mely lehetővé teszi, hogy statisztikai elemzéseket, többek között konfidenciaintervallum becslését és a szignifikanciavizsgálatot is elvégezzük, amely lehetővé teszi a modell tudományos megbízhatóságának növelését,
- célunk annak vizsgálata, hogy a szintetikus adathalmazon túl lehetőség nyílhat-e valós szenzoradatok felhasználására, annak érdekében, hogy modellünket valós üzemi körülmények között validálhassuk.

ÖSSZEFOGLALÁS

Tudományos szempontból vizsgálva a kérdést, a TSK-fuzzy rendszerek számos területen előnyösebb megoldást nyújtanak a biztonságkritikus rendszerek modellezésére, különösen akkor, ha valós idejű (on-line) adatfeldolgozás a cél. A Mamdani-fuzzy rendszerek alapvető előnye, az emberi gondolkodást utánzó, szabályalapú nyelvi leírás, a gyakorlati implementáció során hátrányba fordul, mivel a defuzzifikáció és az aggregáció műveletei numerikus értelemben számításigényesek, és nehezen skálázhatók többváltozós, gyorsan változó rendszerek esetén. Ezzel szemben a TSK-fuzzy modellek alacsony számítási komplexitásuk és folytonos, determinisztikus kimenetük révén lehetővé teszik, hogy a bemeneti adatok alapján közvetlenül numerikus kockázati szintet számítsunk, anélkül, hogy szükség lenne a klasszikus fuzzy rendszerekre jellemző defuzzifikációs lépésekre. Cikkünkben igazoltuk a TSK-fuzzyhoz kapcsolódóan az ACS szükségességét és a definiált validációs mutatók segítségével rámutattunk az ACS-FORCE algoritmusunk előnyös és hatékony működésére.

FELHASZNÁLT IRODALOM

[1] Dr. Galambos P. és Dr. Fekete I, Kockázatelemzés lépésről lépésre. ISBN:963 86905 0 X, ETK Szolgáltató Zrt., Budapest
[2] International Organization for Standardization, „ISO 31000:2018: Risk management — Guidelines, (Edition 2, 2018)”, 2018.
[3] International Organization for Standardization, "ISO/IEC 31010: Risk management – Risk assessment techniques", 2019.
[4] SafetyCulture, "HAZOP (Hazard and Operability Study", [Online]. Elérhető: https://safetyculture.com/topics/hazop/. [megtekintve: 2024.03.01.].
[5] International Electrotechnical Commission, "IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide", 2016.
[6] H. Zhang, B. Zhang, and D. Gao, “A new approach of integrating industry prior knowledge for HAZOP interaction,” Journal of Loss Prevention in the Process Industries, vol. 86, 2023, Art. no. 105005, doi: 10.1016/j.jlp.2023.105005.
[7] Z. Li and J. Zhao, “HAZOPCT: A HAZOP analysis completeness tool based on knowledge graph reasoning,” Process Safety and Environmental Protection, vol. 178, 2025, Art. no. 107025, doi: 10.1016/j.psep.2025.107025.
[8] H. R. J. Solukloei, S. Nematifard, A. Hesami, H. Mohammadi, and M. Kamalinia, “A fuzzy-HAZOP/ant colony system methodology to identify combined fire, explosion,

and toxic release risk in the process industries," Expert Systems with Applications, vol. 192, 2022, Art. no. 116418, doi: 10.1016/j.eswa.2021.116418.

[9] I. Szén, „Hidrogénbiztonság: Balesetek kvantitatív elemzése és biztonságközpontú, új tervezési módszerek fejlesztése" in XXXIX. Kandó Konferencia 2023, G. Molnár, Zs. Temesvári, and T. Wührl. Budapest, Hungary: Óbudai Egyetem, 2024, pp. 44–49.

[10] I. Szén, E. Rácz, and M. Bakosné Diószegi, „Hidrogénüzemek, új és komplex kockázatértékelési rendszere: Új tervezési irányelvek a hidrogénipari létesítmények biztonságának fokozása érdekében, in KVK Habilitációs és PhD Workshop Minikonferencia: Kiadvány kötet, T. Wührl, Ed. Budapest, Hungary: Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar, 2024, pp. 92–97.

[11] I. Szén, "Hidrogén-energetika 1. rész, Energiatárolási célok és lehetőségek, a hidrogén értéklánc," Elektrotechnika, vol. 116, no. 9–10, pp. 28–32, Magyar Elektrotechnikai Egyesület, Budapest, 2023.

[12] M. Shokouhifar „FH-ACO: Fuzzy heuristic-based ant colony optimization for joint virtual network function placement and routing" Applied Soft Computing, Volume 107, August 2021, 107401, doi.org/10.1016/j.asoc.2021.107401

[13] C. Blum, „Ant colony optimization: A bibliometric review" Physics of Life Reviews, Volume 51, December 2024, Pages 87-95, doi.org/10.1016/j.plrev.2024.09.014

[14] H. Belyadi, A. Haghighat, and T. A. Al-Quraishi, „*Machine Learning Guide for Oil and Gas Using Python: A Step-by-Step Breakdown with Data, Algorithms, Codes, and Applications*, Gulf Professional Publishing, 2021. doi: 10.1016/C2019-0-03617-5. (ISBN: 978-0-12-821929-4)

[15] Bükkábrányi Energiapark, *Bükkábrányi Energiapark*. [Online]. Elérhető: https://bukkabranyienergiapark.hu/ [megtekintés dátuma: 2025. ápr. 20.]

[16] J. Isimite and P. Rubini, "A dynamic HAZOP case study using the Texas City refinery explosion," *J. Loss Prev. Process Ind.*, vol. 40, pp. 496–501, Mar. 2016.

[17] S. Silvianita, M. F. Khamidi, I. Rochani, and D. Chamelia, "Hazard and Operability Analysis (HAZOP) of Mobile Mooring System," *Procedia Earth Planet. Sci.*, vol. 14, pp. 208–212, Dec. 2015. doi: 10.1016/j.proeps.2015.07.103.

[18] J. Ahn and D. Chang, "Fuzzy-based HAZOP study for process industry," *J. Hazard. Mater.*, vol. 317, pp. 303–311, 2016. doi: 10.1016/j.jhazmat.2016.05.096.

[19] J. L. Fuentes-Bargues, C. González-Gaya, C. González-Cruz, and V. Cabrelles-Ramírez, "Risk assessment of a compound feed process based on HAZOP analysis and linguistic terms," *J. Loss Prev. Process Ind.*, vol. 44, pp. 44–52, 2016. doi: 10.1016/j.jlp.2016.08.019.

[20] R. A. Viegas, F. A. S. Mota, A. P. C. S. Costa, and F. F. P. dos Santos, "A multi-criteria-based hazard and operability analysis for process safety,"*Process Saf. Environ. Prot.*, vol. 144, pp. 310–321, 2020. doi: 10.1016/j.psep.2020.07.034.

[21] Y. Yousofnejad, F. Afsari, and M. Es'haghi, "Dynamic risk assessment of hospital oxygen supply system by HAZOP and intuitionistic fuzzy," *PLoS One*, vol. 18, no. 2, Feb. 2023. doi: 10.1371/journal.pone.0280918.

[22] K. Hartmann, C. Correa-Jullian, J. Thorson, K. Groth, and W. Buttner, "Hydrogen component leak rate quantification for system risk and reliability assessment through QRA and PHM frameworks," presented at the *9th Int. Conf. Hydrogen Safety (ICHS*

2021), Edinburgh, UK, Sept. 21–23, 2021. [Online]. Available: https://www.nrel.gov/docs/fy22osti/79598.pdf

[23] Oxford Institute for Energy Studies, "Review of Hydrogen Leakage along the Supply Chain," *Energy Transition*, no. ET41, Nov. 2024. [Online]. Elérhető: https://www.oxfordenergy.org/wpcms/wp-content/uploads/2024/11/ET41-Review-of-Hydrogen-Leakage-along-the-Supply-Chain.pdf

[24] Y. Li, Z. Wang, X. Shi, *et al*., "Safety analysis of hydrogen leakage accident with a mobile hydrogen refueling station," *Process Saf. Environ. Prot.*, vol. 171, pp. 619–629, 2023. doi: 10.1016/j.psep.2023.01.051.

[25] X. Zhang, G. Qiu, S. Wang, *et al*., "Hydrogen leakage simulation and risk analysis of hydrogen fueling station in China," *Sustainability*, vol. 14, no. 19, Art. no. 12420, Oct. 2022. doi: 10.3390/su141912420.

[26] J. Qian, X. Li, Z. Gao, and Z. Jin, "A numerical study of hydrogen leakage and diffusion in a hydrogen refueling station," *Int. J. Hydrogen Energy*, vol. 45, pp. 14428–14439, 2020. doi: 10.1016/j.ijhydene.2020.03.140.

[27] J. X. Wen, M. Marono, P. Moretto, E.-A. Reinecke, P. Sathiah, E. Studer, E. Vyazmina, and D. Melideo, "Statistics, lessons learned and recommendations from analysis of HIAD 2.0 database," *Int. J. Hydrogen Energy*, vol. 47, no. 38, pp. 17082–17096, 2022. doi: 10.1016/j.ijhydene.2022.03.170

DOI: https://doi.org/10.12700/btsz.2025.7.4.135

COMPARATIVE ANALYSIS OF BRAKING DISTANCES FOR SELF-DRIVING AND CONVENTIONAL VEHICLES

FÉKTÁVOLSÁG ÖSSZEHASONLÍTÓ ELEMZÉSE ÖNVEZETŐ ÉS HAGYOMÁNYOS JÁRMŰVEK ESETÉBEN

Patrik VIKTOR[1] – Gábor KISS[2]

Abstract

Road safety is of paramount importance to society, especially in an era when autonomous vehicle technology is gaining ground. The aim of our study is to compare the braking distances of self-driving and conventional vehicles, taking into account different road conditions and speed ranges. The focus of the study is on reaction time, which has a decisive influence on stopping distance. The results show that self-driving systems, with an average reaction time of 0.15 seconds, produce shorter braking distances than human drivers under all test conditions, where this value can vary between 0.8 and 2 seconds, especially when distracted (e.g. by mobile phone use). The research showed that self-driving vehicles can stop up to 4.86 metres earlier in urban environments and 23 metres earlier on motorways, which can make a critical difference in accident situations. The study confirms the safety benefits of autonomous systems and supports the hypothesis that self-driving technology can measurably reduce the number of road accidents.

Keywords

Braking distance, self-driving vehicles, conventional vehicles, safety.

Absztrakt

A közúti közlekedés biztonsága kiemelkedő társadalmi jelentőséggel bír, különösen az autonóm járműtechnológia térnyerésének korában. Tanulmányunk célja az önvezető és a hagyományos járművek féktávolságának összehasonlító elemzése, különböző útviszonyok és sebességtartományok figyelembevételével. A vizsgálat középpontjában a reakcióidő áll, mely döntő befolyással bír a megállási távolságra. Az eredmények azt mutatják, hogy az önvezető rendszerek – 0,15 másodperces átlagos reakcióidejükkel – minden vizsgált körülmény között rövidebb féktávolságot produkálnak, mint az emberi vezetők, akiknél ez az érték 0,8–2 másodperc között változhat, különösen zavaró tényezők (pl. mobiltelefon-használat) hatására. A kutatás kimutatta, hogy városi környezetben az önvezető járművek akár 4,86 méterrel, míg autópályán 23 méterrel korábban képesek megállni, ami kritikus különbséget jelenthet baleseti szituációk-ban. A tanulmány megerősíti az autonóm rendszerek biztonsági előnyeit, és alátámasztja azt a hipotézist, hogy az önvezető technológia mérhetően képes csökkenteni a közúti balesetek számát.

Kulcsszavak

Féktávolság, önvezető járművek, hagyományos járművek, biztonság.

[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 | professor, Óbuda University | egyetemi tanár, Óbudai Egyetem

INTRODUCTION

The rise of the autonomous vehicle (AV) signifies one of the most significant technology advances in recent transportation history. With urban populations expanding and deaths from car accidents a serious global concern, autonomous driving could provide a welcome answer to an enduring human challenge: improving traffic safety. Human error, which accounts for about 94 percent of all accidents, could be the main concern when it comes to road injuries and fatalities. Here AVs have the potential to transform mobility: decreasing accidents is just the beginning, as overall traffic flow, fuel economy, and transportation access are also likely to be improved. With the advancement of AI, machine learning and sensors, with the release of autonomous vehicles being more real than science fiction concept and with the push from the car industry, companies in tech and the governments themselves, the work to realise the autonomous vehicle is well on the way. The idea is a modest one on its face but ambitious in scope: vehicles that can perceive the environment around them, understand complex traffic situations and make life-and-death driving decisions, all without human intervention. Yet, even as technology has made great leaps forward, the public response has been apprehensive, questioning whether AVs can really be as good as or even better than humans at driving safely. The hypothesis at the core of this research is, under real-world conditions, can autonomous vehicles be proven to be a safer option to your average human-operated cars?" The study analyses the braking ability of AVs and human-driven vehicles at different driving scenarios, speeds, and pavement types to achieve this. Braking distance as a measure of driving safety is the key metric for understanding whether AVs can react quicker and brake better as compared to humans.

First, preliminary results already make an important case for the safety of AVs. For example, AVs respond much more quickly than humans, taking approximately 0.15 seconds (on average) to react, while human reaction time is 0.8-1.5 seconds. This variation directly translates into stopping differences. For instance, travelling at 50 km/h an AV may be able to stop about 4.86m earlier than a skilled human driver. At 130 km/h on the highway, the distance is even greater-almost 23 meters, which can be the difference between a close call and a fatal crash. In addition to this, soec also exhibit the ability to transfer strategies to different road conditions (e.g., dry, wet, icy), generally achieving a higher degree of consistency and precision to human drivers.

Beyond braking, AVs have other advantages in terms of risk management and situational awareness. While human drivers can lose focus, get tired or drink, systems do not suffer attention lapses. Street robots, with cameras, radar, lidar, and cutting-edge software, keep a 360 degree view of the world around them and are processing traffic data in real-time to determine safe manoeuvres. Too keep up with this level of awareness, AVs can anticipate danger better than humans and swerve to avoid it more accurately. For all these auspices, however, much remains to be done. Sensor robustness and operation in uncertain situations, as well as intricate trolley problem scenarios, remain significant challenges for autonomous technology. For example, how should an AV respond when it is involved in an inevitable collision that could potentially cause injury to a passenger or a pedestrian? Moreover, the design of regulations for liability assignment on AV-related crashes is underdeveloped, and important questions such as accountability are raised. Cybersecurity risks also represent a serious threat, as AVs are largely software- and network-dependent, which

may expose them to malicious activities. Broader socioeconomic implications of self-driving cars should be considered too. On the other, a well-executed deployment of AVs will mean a vast reduction in traffic deaths, lower healthcare and insurance costs, and greater mobility for the elderly and people with disabilities. Alternatively, the mass use of AVs may displace established industries, create unemployment in driving-oriented industries and add health risks associated with system failure and technology reliance. Taking these concerns into account, this study is focused on presenting an overall analysis of AV safety, with a particular focus on the braking performance as a measure of real-world effectiveness. By comparative testing, statistical analysis, and secondary literature, we hope to determine whether the safety benefits of AVs are sufficient to merit a greater degree of public confidence and policy backing.

LITERARY PROCESSING

Self-driving technology

Self-driving technology has increasingly become a symbol of the revolutionisation of transport, with the rise of artificial intelligence (AI) and automation gaining more and more attention. The development and adoption of self-driving vehicles is closely linked to technological innovations, the transformation of transport infrastructure, and social and ethical considerations [1] [2] . Recent research has shown that the safety of self-driving cars is fundamentally influenced by the reliability of the vehicle's sensor systems, which is a key element in the development of AI-based technologies. Saudi Arabian examples also show that adequate infrastructure is essential for these systems to operate successfully [1] . The risk of traffic accidents, which self-driving technologies aim to minimize in the early stages, is influenced by various factors such as adverse weather conditions and cybersecurity threats [3] [4] . The emotional aspects of transportation and the trust of users in the technology are important factors for the adoption of self-driving vehicles. Research has shown that the experience provided by vehicles and the transparency of transport systems have a strong influence on user trust [5] [6] . The level of trust people have in self-driving cars depends on the reliability of the technology and the positivity of the first experience [6] [7]. The implementation of future transport systems and the integration of self-driving technologies also raises various legal and ethical issues. The realisation of societal expectations and legal frameworks are key to the widespread adoption of vehicles [2] [8] . Without these frameworks, developments and innovations could not have the desired impact, which is essential for the future of transport. Nevertheless, detailed statistical analysis and research into the technological challenges will help to define future directions [9] . The expectations of artificial intelligence, data processing and lifelong learning are constantly evolving, not only to improve transport safety but also to improve efficiency [4] [10] . Overall, self-driving technology not only poses technical challenges but also fundamentally transforms social norms, the way transport systems operate and the mobility solutions of the future. The development of an ethical legal framework is essential to ensure that self-driving systems are safely and efficiently integrated into the current transport ecosystem.

Self-driving cars

Self-driving car technology has emerged as one of the most important transport innovations of recent decades, with the potential to radically change social habits. The development of these vehicles is driven by the development of artificial intelligence, sensors and communication technologies, which together enable automated driving. For responsible innovation, it is also important to take into account the social impact and the readiness to adapt the technology, which in some cases may slow down its diffusion [11] [12] .

Among the determinants of user acceptance, safety has been identified as one of the most important aspects that have led to easier perception of self-driving vehicles [13] . Research has observed that consumer attitudes show considerable variability, with different groups reacting differently to technology, which involves not only technical but also social aspects [14] . Gender differences and cultural backgrounds have an impact on the perception of the acceptance of self-driving cars by a given audience [15] .

Furthermore, the business model of fleet use of vehicles offers the potential to reduce the number of cars entering cities, thus improving mobility and also reducing pollution [16] [17] . In addition, research has shown that the introduction of self-driving cars is expected to reduce the incidence of accidents, as artificial intelligence and sensor systems are able to navigate traffic with greater accuracy [18] .

However, the social acceptance of autonomous vehicles is not only a technical issue: there are also a number of ethical dilemmas related to decision-making algorithms and the handling of accident situations [19] . These issues are particularly important as future transport models will depend largely on society's attitude towards these technologies [20] .

Overall, self-driving cars will not only transform transport, but will also have a profound impact on social interactions, mobility patterns and urbanisation processes in the future. Responsible innovation is key to the societal acceptance of autonomous vehicles and to fostering the uptake of the technology [11] [12] .

Self-driving cars vs conventional cars

The comparison between self-driving cars and conventional cars covers a number of aspects, including technology, safety, environmental impact and social acceptance. The introduction of autonomous vehicles could radically transform our transport habits and the future of mobility, while conventional cars are ubiquitous and deeply embedded in everyday life. [21] One of the biggest advantages of self-driving cars is safety. Numerous studies show that the majority of accidents in traditional cars are due to human error, while self-driving cars can reduce the number of accidents by using artificial intelligence and advanced sensor systems [22] . Ujházi et al. (2023) pointed out that real-world experience and understanding of the technology is key to consumer acceptance of self-driving cars, as increasing the sense of safety and reliability is essential [23] .

In terms of environmental impacts, conventional cars provide significant carbon emissions, while self-driving electric vehicles, when properly integrated into transport systems, reduce urban air pollution [24] . In their study, Kecskés and Lukovics (2024) concluded that self-driving fleets can reduce the number of cars on the road, thereby alleviating congestion and environmental burden [24] .

The social dimensions of the adoption of self-driving cars are also controversial. [25] have pointed out that the ethical issues of self-driving cars and trust in the technology

have been largely used to shape consumer attitudes [25] . Confidence in the action of self-driving vehicles over conventional cars is also subject to skeptical perceptions among different social groups, such as older and female groups [26] .

In conclusion, while self-driving cars offer various opportunities to improve the safety and sustainability of transport, the position of conventional cars is still very strong due to social and economic concerns. The future evolution of the technology and acceptance will be fundamentally based on the extent to which conventional cars remain in use over the coming decades.

Self-driving cars safety

The safety of self-driving cars (AVs) is one of the most important issues in the development of transport systems today. These vehicles offer significant potential advantages over conventional cars in reducing the number of collisions and accidents; technological, ethical and legal considerations all play an important role in social acceptance and safety Vaziri et al [27] [28] [29] . One of the main advantages of AVs is the minimization of human error. Research in the United States has shown that 94% of traffic accidents are caused by human error, while self-driving technologies such as artificial intelligence and advanced sensor systems that continuously monitor their environment can make quick decisions based on external conditions, thereby reducing the risk of accidents [29] [30] . Autonomous vehicles offer greater reaction time with more accurate positioning and speed determination, compared to the performance of human drivers [31] [32] . Continuous advances in technology and the integration of advanced driver assistance systems (ADAS) allow for increased road safety [29] . AVs are able to precisely control speed, acceleration and distance, which helps avoid accidents and increases vehicle efficiency [31] [32] .

Category	Aspect	Details
Advantages	Reduced Human Error	94% of accidents caused by human error; AVs eliminate most of these risks.
	Faster reaction time	Human: 0.8-1.5 sec; AV: ~0.15 sec
	Shorter Braking Distances	At 50 km/h: 4.86 m shorter; At 130 km/h: 23 m shorter
	Better Road Adaptability	AVs handle dry, wet, icy roads more reliably
Challenges	Technological Limitations	Sensor accuracy, AI decision limits
	Legal & Ethical Issues	Accident liability, moral dilemmas
	Cybersecurity Threats	Vulnerability to hacking, data manipulation
Expected Impact	Fewer Severe Accidents	Reduction of ~51.14% by 2033 (ADAS estimate)
	Fewer fatalities	Reduction of ~39% (EU forecast)
	Minor Accidents	Reduction of ~9.32%

Table 1 Safety of self-driving cars

If autonomous technologies are properly deployed, the cumulative impact of accidents could be dramatically reduced, saving thousands of lives [28] [33] . It is important to note that despite the maturity of the technology, investments in AVs do not guarantee 100% safety [34] . Autonomous vehicles can cause accidents, which poses challenges for the legal framework and the problem of establishing a proper one [34] . When analysing traffic data and accident conditions, future developments must constantly consider ethical dilemmas related to vehicle decisions and potential victims [35] [36] Moral issues in investigations will become increasingly important as more autonomous vehicles are put on the road, and their liability must be addressed from a legal perspective [35] . In addition to

developing a liability framework for AVs, it is also essential to build social trust related to the benefits expected from reducing the number of road accidents [28] [34] .

In summary, the safety of self-driving cars is a key driver in shaping transport technologies, and exploring the factors that influence safety and reliability in social acceptance is an ongoing challenge for researchers and policy makers. Using the right technologies and frameworks, it is possible to make AVs a flagship for transport sustainability and safety [29] [32] [37] .

Stopping distance

Braking distance is the stopping distance of a vehicle, taking into account several factors such as vehicle speed, braking force, road surface conditions and vehicle weight. Determining the stopping distance is crucial for road safety, as knowing and planning the correct stopping distance is essential to avoid accidents.

Important factors for measuring stopping distances are:

1. Vehicle speed: Braking distance increases in proportion to the square of the speed. The braking distance is proportional to the speed of the vehicle. In addition, the weight of the vehicle and the load must also be taken into account, as these affect the braking force.
2. Braking force: The quality and quantity of braking force is a key element in determining stopping distances. The quality and quantity of the braking force is the key factor in determining the braking distance. The ABS system helps to lock the wheels, thus reducing the detection distance.
3. Road surface and weather conditions. On slippery, wet or icy roads, braking power is reduced, which increases stopping distance. The type and quality of the road surface, such as asphalt or concrete pavement, are also important factors. Environmental conditions, such as precipitation, fog or snow, also affect stopping distances in different conditions.
4. Tyres**.** Tyres that are properly maintained and inflated can reduce stopping distances, while worn, poorly inflated tyres can increase stopping distances.
5. Vehicle type: the type of vehicle, such as a heavy truck or a passenger car, requires different stopping distances. Light-weight passenger cars can stop faster than heavier vehicles, as the effectiveness of the brakes may also vary.

Stopping distances are typically measured using standard test procedures defined by manufacturers, where vehicles are stopped at different speeds. The testing takes into account the above factors and the measured data is analysed using statistical models to determine the behaviour of the vehicle under different conditions. Measurements are often made in a laboratory environment and in real-time traffic situations to obtain the most accurate data. Knowledge of braking distances is essential to improve road safety. Factors such as speed, braking force, road surface condition and vehicle type play a key role in influencing vehicle control. Measuring the correct braking distance and having a thorough knowledge of the factors involved is essential to avoiding accidents and driving efficiently.

MATERIAL AND METHODOLOGY

Comparative analysis of stopping distances for self-driving and conventional vehicles

When modelling a self-driving system, reaction time is a key factor that determines how quickly and efficiently a self-driving vehicle can react to different situations and environmental changes. Reaction time is the time that elapses between the detection of the system and its reaction. We can compare the reaction times of a conventional driver-driven vehicle and a self-driving vehicle in the following aspects:

Conventional Driving:

- Sensing: In the case of a driver-driven vehicle, perception relies on the driver's vision, hearing and other senses. The perception process can be time-consuming and is influenced by the driver's attention, responsiveness and experience. When analysing reaction time, it is important to consider that for human drivers, reaction time is highly dependent on driving routine and the speed of reflexes. It is generally accepted that the human reaction time to a sudden situation can vary between 0.8 and 1.5 seconds, which is the time it takes a person to initiate braking or other driving manoeuvres after detection and decision. The variability of this reaction time depends on a number of factors, including driving experience, reflexes, and physical and mental state. Fatigue, sharing attention with other activities, and the consumption of certain drugs and medicines are all factors that can affect human reaction time. In contrast, reaction times for self-driving systems can typically be significantly shorter, as machine learning algorithms and sensor systems can detect, analyse and respond to environmental changes much more quickly and efficiently. The adaptability and machine response time of autonomous vehicles is essential to manoeuvre effectively and safely in unexpected traffic situations. Therefore, the analysis of reaction times will lead to an understanding of the key differences between driver and self-driving systems and show why autonomous systems can be more effective and safer in handling unexpected situations in road traffic.
- Decision: The driver makes a decision about how to control the vehicle after sensing it. Many variables and subjective elements play a role in the decision process. For a fully human-driven vehicle, different reaction times are defined, such as a fast reaction time of half a second, while a medium reaction time is one second. A slow reaction time is defined by ADAS research as two seconds, and is usually used to include reaction in old age and under the influence of alcohol. [38]
- Control response: The reaction time of a driver-driven vehicle depends on the driver's judgment, including steering, acceleration and braking.

Physical limitations, such as reflexes, affect the duration of the control response.

- Distraction: It is a complex failure phenomenon that has been present since the beginning of driving, but with the increase in the achievable speed of vehicles and the advances in technology, the importance of whether or not a vehicle is involved in an accident has become even more pronounced. Looking at Valeo's research, stimulus influence has a very strong influence in the 21st century, based on this I identify 8 factors that influence the driver and their reaction time[39].

1. Telephone use,
2. Conversation,
3. Illness,
4. Dressing appropriately,
5. Sexual influence,
6. An external event, such as an accident,
7. Eating,
8. Harmful addiction.

Self-Driving System

- Perception: The self-driving system uses sensors to continuously sense its surroundings, including other vehicles, pedestrians, and road conditions. The sensors provide data in real time, minimizing the time required for the sensing process.
- Decision: The algorithms in the self-driving system quickly process the data provided by the sensors and make decisions. The computational power of the algorithms allows them to handle a large number of variables and optimise the decision-making process.
- Control response: Self-driving vehicles have the ability to control directly, such as steering, braking or accelerating, in response to decisions made by the system. At the current level of development of self-driving systems, the self-driving reaction time is 0.15 seconds.40 This number will decrease in the future as technology and data transfer speeds increase.Electronic control allows fast and accurate reactions, minimising the time required for a control reaction. In the case of self-driving systems, the response time can often be faster because the information provided by sensors is processed by computers and reacts instantaneously to changes in the environment. This can contribute to safer and more efficient transport. However, it is important to note that the performance and reaction time of self-driving systems still depends on the complexity of the hardware and software, as well as on the environmental challenges.
- Confounding factor: At self-driving level 3 or higher, there is no influence of distraction on driving, and at self-driving level 2, there is minimal influence.

Braking distance calculation for self-driving and conventional vehicles

The stopping distance is the sum of the distance calculated from the reaction time of a person driving a car or other vehicle and the distance travelled during braking (stopping distance). The formula that describes the stopping distance is as follows:

stopping distance = distance travelled during reaction time + stopping distance

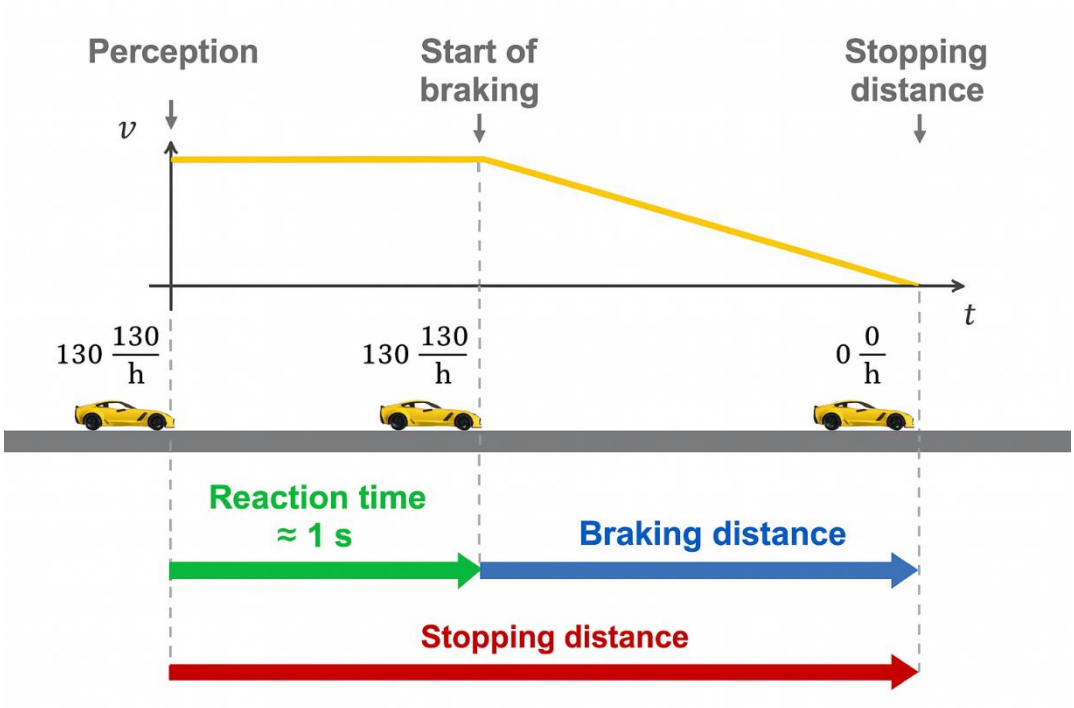


Figure 1 Braking distance. Source:[41]

- **Reaction Time Distance**: This distance is the time it takes the driver to react to the emergency and the distance the car travels at its speed. The longer the reaction time, the greater this distance will be.
- **Braking distance:** Braking distance is the distance the car will travel after the driver starts braking. The length of the braking distance depends on a number of factors, such as speed, road conditions (e.g. wet or dry road) and the condition of the vehicle's braking system.

As a result of this summation, the stopping distance is a distance that includes both the distance travelled during the reaction time and the distance covered by the stopping distance. Thus, overall, it characterises the braking performance of the car in emergency or normal traffic situations. [42]

Braking distance formula (1):

$$s = t_r v \frac{v^2}{2a} \qquad (1)$$

s - distance (metres)

t_r- reaction time (seconds)

v - speed (m/s)

a - deceleration m/s^2

Deceleration rate for different road conditions:

On dry road: 7,5 m/s^2

On wet roads: 4,5 m/s^2

On snowy/icy roads: 1,5 m/s^2

Braking force build-up: 0,5 s

In the case of a conventional vehicle, the distraction factor (e.g. looking at the telephone while driving) must also be taken into account (2):

$$s = t_r v \frac{v^2}{2a} + Z_t \qquad (2)$$

This modification can be interpreted in several ways, which I will explain in the following table. In the tables, I compare one typical distraction, phone use. This is a common problem according to several studies and affects 82-87% of Generation Y and younger, Chen et al. 2021 which is so common that these studies provide a detailed database. [43] For our study, 4 very important domains can be identified:

- 20 km/h: Used in residential zones where there are many active minors who can easily stray onto the road.
- 30 km/h: Speed limit in pedestrian zones around schools and kindergartens
- 50 km/h: km limit used in residential areas where there are many pedestrians crossing.
- 130 km/h: The speed limit on motorways, the highest speed allowed in Hungary. According to 2019 data, 17.63% of car accidents occur on Hungarian motorways, of which 41.8% are fatal.

	Braking distance on dry roads								
	Autonomous vehicle	Fast reaction time	Braking distance difference	Medium reaction time	Braking distance difference	Slow reaction time	Braking distance difference	When looking at the phone	Braking distance difference
	Reaction time								
v (km/h)	0,15 s	0,5 s	Deviation compared to autonomous vehicle	1 s	Deviation from autonomous vehicle	2 s	Deviation from autonomous vehicle	4 s	Deviation from autonomous vehicle
15	3,87 m	5,32 m	1,46 m	7,41 m	3,54 m	11,57 m	7,71 m	19,91 m	16,04 m
20	5,67 m	7,61 m	1,94 m	10,39 m	4,72 m	15,95 m	10,28 m	27,06 m	21,39 m
30	10,05 m	12,96 m	2,92 m	17,13 m	7,08 m	25,46 m	15,42 m	42,13 m	32,08 m
40	15,45 m	19,34 m	3,89 m	24,90 m	9,44 m	36,01 m	20,56 m	58,23 m	42,78 m
45	18,54 m	22,92 m	4,38 m	29,17 m	10,63 m	41,67 m	23,13 m	66,67 m	48,13 m

	Braking distance on dry roads								
	Autonomous vehicle	Fast reaction time	Braking distance difference	Medium reaction time	Braking distance difference	Slow reaction time	Braking distance difference	When looking at the phone	Braking distance difference
	Reaction time								
50	**21,89 m**	26,75 m	4,86 m	33,69 m	11,81 m	47,58 m	25,69 m	**75,36 m**	53,47 m
60	29,35 m	35,19 m	5,83 m	43,52 m	14,17 m	60,19 m	30,83 m	93,52 m	64,17 m
70	37,84 m	44,65 m	6,81 m	54,37 m	16,53 m	73,82 m	35,97 m	112,71 m	74,86 m
80	47,37 m	55,14 m	7,78 m	66,26 m	18,89 m	88,48 m	41,11 m	132,92 m	85,56 m
90	57,92 m	66,67 m	8,75 m	79,17 m	21,25 m	104,17 m	46,25 m	154,17 m	96,25 m
100	69,50 m	79,22 m	9,72 m	93,11 m	23,61 m	120,88 m	51,39 m	176,44 m	106,94 m
110	82,10 m	92,80 m	10,69 m	108,08 m	25,97 m	138,63 m	56,53 m	199,74 m	117,64 m
130	110,41 m	123,05 m	**12,64 m**	141,10 m	30,69 m	177,21 m	66,81 m	249,43 m	**139,03 m**

Table 2 Stopping distances on dry roads Source:[39] own ed.

Table 38 compares the self-driving system with the conventional system on dry roads. It can be clearly seen that at a speed of 130 km/h, the vehicle stops 12.64 m slower without distraction. Whereas, when distracted, the braking distance is more than doubled, i.e. 139.03 metres, and it takes a quarter of a kilometre to stop. In other words, even under ideal conditions, using the self-driving system in zone 50, you can stop 3 thirds faster.

	Braking distance on wet roads as a function of reaction time				
	Autonomous vehicle	Fast reaction time	Medium reaction time	Slow reaction time	In case of telephoning
v (km/h)	0,15 s	0,5 s	1 s	2 s	4 s
15	4,64 m	6,10 m	8,18 m	12,35 m	20,68 m
20	7,04 m	8,98 m	11,76 m	17,32 m	28,43 m
30	13,13 m	16,05 m	20,22 m	28,55 m	45,22 m
40	20,94 m	24,83 m	30,38 m	41,50 m	63,72 m
45	25,49 m	29,86 m	36,11 m	48,61 m	73,61 m
50	**30,46 m**	35,32 m	42,27 m	56,16 m	**83,93 m**
60	41,70 m	47,53 m	55,86 m	72,53 m	105,86 m
70	54,65 m	61,45 m	71,18 m	90,62 m	129,51 m
80	69,31 m	77,09 m	88,20 m	110,43 m	154,87 m
90	85,69 m	94,44 m	106,94 m	131,94 m	181,94 m

	Braking distance on wet roads as a function of reaction time				
	Autonomous vehicle	Fast reaction time	Medium reaction time	Slow reaction time	In case of telephoning
100	103,79 m	113,51 m	127,40 m	155,18 m	210,73 m
110	123,60 m	134,29 m	149,57 m	180,13 m	241,24 m
130	**168,36 m**	181,00 m	199,06 m	235,17 m	**307,39 m**

Table 3 Stopping distances on wet roads Source: [39] owned.

On wet roads, 2 speed ranges were considered important to investigate. At 50 km/h, where the stopping distance increases by almost 2.5 times when using a phone. Or at 130 km/h, where the stopping distance increases by 83% when using a phone. This is a serious accident risk on motorways, where this speed is allowed.

	Braking distance on icy/snowy roads as a function of reaction time				
	Autonomous vehicle	Fast reaction time	Medium reaction time	Slow reaction time	In the case of telep-honing
v (km/h)	0,15 s	0,5 s	1 s	2 s	4 s
15	6,91 m	8,37 m	10,45 m	14,62 m	22,95 m
20	**11,62 m**	13,57 m	16,34 m	21,90 m	**33,01 m**
30	24,90 m	27,81 m	31,98 m	40,31 m	56,98 m
40	43,32 m	47,21 m	52,76 m	63,87 m	86,10 m
45	54,46 m	58,83 m	65,08 m	77,58 m	102,58 m
50	**66,88 m**	**71,74 m**	78,69 m	92,58 m	**120,36 m**
60	95,59 m	101,43 m	109,76 m	126,43 m	159,76 m
70	129,45 m	136,25 m	145,97 m	165,42 m	204,31 m
80	168,44 m	176,22 m	187,33 m	209,55 m	254,00 m
90	212,58 m	221,33 m	233,83 m	258,83 m	308,83 m
100	261,87 m	271,59 m	285,48 m	313,26 m	368,81 m
110	316,30 m	326,99 m	342,27 m	372,83 m	433,94 m
130	440,59 m	453,23 m	471,28 m	507,39 m	579,62 m

Table 4 Stopping distances on icy/snowy roads Source: [39] owned.

When looking at the reaction time on icy/snowy roads, it can be seen that there is approximately a 3% difference between the stopping time of public transport vehicles and conventional vehicles, but once disturbance is taken into account, this difference increases. What I would like to highlight is the stopping distance at 50 km/h, where it is 66.88 metres for a public transport vehicle and almost double that at 120.36 metres with distraction. As this speed range is the typical urban speed. As well as in the 20km/h hour category, which is a typical speed limit in suburban areas, there you can see that compared to a self-driving system, you can stop 3 times as far while driving by phone while driving conventionally. In all cases, people using self-driving systems stop faster, as the system has a reaction time of

0.15s, whereas an average person with a fast reaction time reacts in 0.5s. Continuing this line of thought, here could be the difference in the injury and death that can occur at different speed ranges. From my investigation it is clear that there are substantial differences in the different conditions using the self-driving system. Thus the number of accidents and fatalities that occur can be reduced. Based on this, ADAS estimates that by 2020, if self-driving vehicles on the road reach level 3 or higher of self-driving technology, road accidents could be reduced by 38%, to be achieved by 2033. [166] In the EU, ADAS estimates that fatal accidents will decrease by approximately 39%, while serious injury accidents will decrease by 51.14%. But even the self-driving system needs to improve, because current estimates suggest that the number of minor collisions will fall by only 9.32%. Taking my research above into account, using a self-driving system will reduce stopping distances by a third in many cases, and can even reduce fatal collisions to serious ones. Based on these and the above conclusions, I conclude that the safety of self-driving technology can be measured from a road safety perspective. In other words, this technology will reduce and, as it spreads, will reduce the number of road accidents.

My hypothesis I assumed that self-driving technology has the potential to reduce the number of road accidents.

Based on my analysis of stopping distances and computational data, I can state that it can reduce the number of road accidents by reducing the number of hit-and-run accidents by allowing faster reaction times of self-driving systems resulting in shorter stopping distances.

My hypothesis I/A assumed that the safety of self-driving technology in traffic terms can be measured.

Based on braking distance analyses, it can be stated that on dry roads at urban speeds, a self-driving vehicle, typically the size of a car, will stop 4.86 metres faster than a routine driver. At highway speeds, the difference is 23 metres, which is about 4 car lengths. On wet, snowy roads, this difference increases further. We can see that not only can self-driving technology be shown to reduce the number of road accidents, but also that its safety can be measured in this area.

Based on the above, Hypotheses I and I/A can be summarised in a single thesis.

SUMMARY

In recent years, autonomous vehicle (AV) technology has become a central topic in discussions surrounding the future of transportation. With the increasing presence of AVs on public roads and the pressing need to improve road safety, this study explores the hypothesis that self-driving vehicles offer measurable safety benefits compared to conventional, human-driven cars. Specifically, it examines whether the braking distance-a key indicator of traffic safety-can be reduced through autonomous driving systems.

Braking distance is composed of two critical elements: the distance a vehicle travels during the driver's or system's reaction time, and the distance required to come to a full stop once braking is initiated. This research places special emphasis on reaction time, as it significantly influences the overall braking distance and the likelihood of preventing accidents.

One of the most striking findings of the study is the dramatic difference in reaction times between human drivers and AV systems. Autonomous vehicles exhibit an average reaction time of approximately 0.15 seconds, thanks to their advanced sensors and real-time

data processing capabilities. In contrast, human drivers have a reaction time that typically ranges from 0.8 to 2 seconds, depending on factors such as age, alertness, and the presence of distractions-most notably mobile phone use. This variation in human response introduces significant safety risks, especially in high-speed or complex traffic environments.

By analyzing real-world data and simulated braking scenarios, the study demonstrates that self-driving vehicles consistently achieve shorter stopping distances across all tested conditions. At a moderate urban speed of 50 km/h, AVs can stop up to 4.86 meters earlier than human drivers. This difference becomes even more substantial at highway speeds of 130 km/h, where AVs can come to a stop approximately 23 meters sooner than their human-operated counterparts. These figures represent distances that could mean the difference between a collision and a near miss, particularly in densely trafficked or high-risk environments. The analysis also considers a wide range of environmental variables such as dry, wet, and icy road conditions. On slippery surfaces, braking performance becomes even more critical. AVs demonstrate superior consistency and adaptability in these conditions, maintaining more reliable control than human drivers. Even when human drivers are not distracted, they still tend to perform worse under adverse conditions due to delayed perception and slower manual responses. To illustrate the danger posed by distractions, the study evaluates the impact of mobile phone usage during driving-a widespread and well-documented issue. In scenarios involving phone use, braking distances increased dramatically. For example, under wet road conditions and travelling at 50 km/h, distracted human drivers required nearly 84 meters to stop, while an AV under the same conditions needed just 30 meters. This difference highlights the vulnerability of human attention and the potential of AVs to reduce accident severity through faster and more reliable reactions.

Despite these clear benefits, the study acknowledges that autonomous technology still faces several important challenges. While AVs outperform human drivers in controlled and repeatable situations, complex ethical dilemmas-such as choosing between two harmful outcomes in an unavoidable collision-remain unresolved. Furthermore, the reliability of sensor systems under extreme weather conditions, and the cybersecurity risks associated with networked, software-dependent systems, present ongoing technological and regulatory concerns.

The study also touches on the legal and ethical implications of AV deployment. Questions about liability in the event of an accident, moral decision-making by algorithms, and the general lack of regulatory frameworks are critical areas that require further attention. Nevertheless, the projected benefits of AV implementation remain substantial. According to forecasts from the European Union and other sources cited in the research, the adoption of advanced autonomous systems could lead to a 38-51% reduction in serious accidents and a 39% decrease in fatalities by the year 2033.

From a broader societal perspective, AVs also offer the potential to transform urban mobility. Through fleet optimization, reduced congestion, and enhanced access for the elderly and disabled, autonomous vehicles may bring about more sustainable and inclusive transportation systems. However, public acceptance remains a key obstacle. Trust in the technology is influenced by factors such as user experience, cultural attitudes, gender, and age. The transition from traditional to autonomous driving will depend not only on technical reliability but also on successful public engagement and education.

In conclusion, the research confirms the hypothesis that autonomous vehicles can significantly improve road safety, particularly by reducing braking distances. This advantage is grounded in their superior reaction times, consistent performance under various conditions, and immunity to human distraction. While challenges remain in terms of technology, legislation, and societal acceptance, the evidence suggests that AVs represent a safer alternative to conventional driving. If these systems are properly implemented and integrated into existing transport infrastructure, they hold the potential to drastically reduce the number and severity of road accidents, ultimately saving lives and reshaping the future of mobility.

LITERATURE

[1] F. Alsubaei, "Reliability and security analysis of artificial intelligence-based self-driving technologies in Saudi Arabia: a case study of openpilot", Journal of Advanced Transportation, vol. 2022, p. 1-25, 2022. https://doi.org/10.1155/2022/2085225

[2] R. Nagashree and K. Gowda, "Review of self-driving cars - technologies, standards and safety", International Research Journal of Modernization in Engineering Technology and Science, 2023. https://doi.org/10.56726/irjmets35638

[3] A. Chougule, V. Chamola, A. Sam, F. Yu, & B. Sikdar, "A comprehensive review on limitations of autonomous driving and its impact on accidents and collisions", Ieee Open Journal of Vehicular Technology, vol. 5, p. 142-161, 2024. https://doi.org/10.1109/ojvt.2023.3335180

[4] K. Muhammad, A. Ullah, J. Lloret, J. Ser, & V. Albuquerque, "Deep learning for safe autonomous driving: current challenges and future directions", Ieee Transactions on Intelligent Transportation Systems, vol. 22, no. 7, p. 4316-4336, 2021. https://doi.org/10.1109/tits.2020.3032227

[5] 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

[6] S. Tolbert and M. Nojoumian, "Cross-cultural expectations from self-driving cars",, 2023. https://doi.org/10.21203/rs.3.rs-2432387/v1

[7] E. Rovira, A. McLaughlin, R. Pak, & L. High, "Looking for age differences in self-driving vehicles: examining the effects of automation reliability, driving risk, and physical impairment on trust", Frontiers in Psychology, vol. 10, 2019. https://doi.org/10.3389/fpsyg.2019.00800

[8] W. Ratoff, "Self-driving cars and the right to drive", Philosophy & Technology, vol. 35, no. 3, 2022. https://doi.org/10.1007/s13347-022-00551-1

[9] J. Gwak, J. Jung, R. Oh, M. Park, M. Abdu, K. Rakhimovet al., "A review of intelligent self-driving vehicle software research", Ksii Transactions on Internet and Information Systems, vol. 13, no. 11, 2019. https://doi.org/10.3837/tiis.2019.11.002

[10] Y. Li, Y. Zhou, X. Ma, & Y. Zhang, "Forecasting the development of self-driving technology in china by multidimensional information," Journal of Advanced Transportation, vol. 2021, pp. 1-12, 2021. https://doi.org/10.1155/2021/1693459

[11] M. Lukovics and N. Nádas, "The role of responsible innovation in the relationship between autonomous vehicles and society", Civic Review, vol. 18, no. 4-6, p. 295-317, 2022. https://doi.org/10.24307/psz.2022.1221
[12] M. Lukovics, T. Ujházi, & S. Prónay, "Social science aspects of the adoption of self-driving vehicles: research opportunities and methodological limitations", Polgári Szemle, vol. 19, no. 4-6, p. 266-280, 2023. https://doi.org/10.24307/psz.2023.1220.
[13] T. Ujházi, M. Lukovics, Z. Majó-Petri, & S. Prónay, "Investigating consumer preferences towards self-driving vehicles after an actual test drive",, 2023. https://doi.org/10.62561/emok-2023-29
[14] B. Nagy, S. Prónay, & M. Lukovics, "I drive, you drive or self-drive? - five perspectives of self-driving car acceptance in hungary", Marketing & Management, vol. 56, no. 2, p. 23-34, 2022. https://doi.org/10.15170/mm.2022.56.02.03
[15] M. Lukovics and B. Gábor, "Self-driving cars and Hungarian women", Polgári Szemle, vol. 17, no. 1-3, p. 178-193, 2021. https://doi.org/10.24307/psz.2021.0713
[16] E. Kecskés and M. Lukovics, "The potential impact of the cost benefits of self-driving fleet use on the mobility of Hungarian cities", North-Hungarian Strategic Notes, vol. 21, no. 1, p. 82-97, 2024. https://doi.org/10.32976/stratfuz.2024.7
[17] B. Zuti and M. Lukovics, "Adoption of self-driving vehicles in behavioural economics. the role of nudge in the development of sustainable urban mobility", Közgazdasági Szemle, vol. 70, no. 2, p. 149-166, 2023. https://doi.org/10.18414/ksz.2023.2.149
[18] L. Gál and T. Sipos, "The impact of autonomous vehicle penetration on specific economic loss values", Transport Economics Review, vol. 68, no. 4, p. 74-82, 2018. https://doi.org/10.24228/ktsz.2018.4.6
[19] M. Miskolczi, K. Ásványi, M. Jászberényi, & L. Kökény, "Hogyan döntsön a mesterséges intelligencia? az ön-driving autók morális kérdései - how should artificial intelligence decide? moral challenges of self-driving cars", Hungarian Science, 2021. https://doi.org/10.1556/2065.182.2021.3.6
[20] G. Kiss and P. Bakucz, "Handling unavoidable accident situations by self-driving vehicles", Gradus, vol. 10, no. 2, 2023. https://doi.org/10.47833/2023.2.csc.023
[21] M. Lukovics, T. Ujházi, & S. Prónay, "Social science aspects of self-driving vehicle adoption : research opportunities and methodological limitations", Citizen Review, vol. 19, no. 4-6, p. 266-280, 2023. https://doi.org/10.24307/psz.2023.1220
[22] L. Gál and T. Sipos, "The impact of autonomous vehicle penetration on specific economic loss rates", Transport Science Review, vol. 68, no. 4, p. 74-82, 2018. https://doi.org/10.24228/ktsz.2018.4.6
[23] T. Ujházi, M. Lukovics, Z. Majó-Petri, & S. Prónay, "Investigation of consumer preferences towards self-driving vehicles following an actual test drive",, 2023. https://doi.org/10.62561/emok-2023-29
[24] E. Kecskés and M. Lukovics, "The potential impact of the cost benefits of self-driving fleet use on the mobility of Hungarian cities", North-Hungarian Strategic Notes, vol. 21, no. 1, p. 82-97, 2024. https://doi.org/10.32976/stratfuz.2024.7
[25] M. Miskolczi, K. Ásványi, M. Jászberényi, & L. Kökény, "Hogyan döntsön a mesterséges intelligencia? az öndriving autók morális Frageni - how should artificial intelligence decide? moral challenges of self-driving cars", Hungarian Science, 2021. https://doi.org/10.1556/2065.182.2021.3.6

[26] M. Lukovics and B. Gábor, "Self-driving cars and Hungarian women", Polgári Szemle, vol. 17, no. 1-3, p. 178-193, 2021. https://doi.org/10.24307/psz.2021.0713
[27] I. Vaziri, F. Ahmadi, Z. Rizi, & M. Saffarzadeh, "The impact of interactions between resources, technology, and technical aspects of autonomous vehicles on urban smart spaces", IJIMOB, vol. 4, no. 2, p. 142-154, 2024. https://doi.org/10.61838/kman.ijimob.4.2.17
[28] T. Gill, "Ethical dilemmas are really important to potential adopters of autonomous vehicles", Ethics and Information Technology, vol. 23, no. 4, p. 657-673, 2021. https://doi.org/10.1007/s10676-021-09605-y
[29] E. Huff, K. Lucaites, A. Roberts, & J. Brinkley, "Participatory design in the classroom: exploring the design of an autonomous vehicle human-machine interface with a visually impaired co-designer", Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 64, no. 1, p. 1921-1925, 2020. https://doi.org/10.1177/1071181320641463
[30] A. Papadoulis, M. Quddus, & M. Imprialou, "Evaluating the safety impact of connected and autonomous vehicles on motorways", Accident Analysis & Prevention, vol. 124, p. 12-22, 2019. https://doi.org/10.1016/j.aap.2018.12.019
[31] U. Montanaro, S. Dixit, S. Fallah, M. Dianati, A. Stevens, D. Oxtobyet al., "Towards connected autonomous driving: review of use-cases", Vehicle System Dynamics, vol. 57, no. 6, p. 779-814, 2018. https://doi.org/10.1080/00423114.2018.1492142
[32] M. Garg and M. Bouroche, "Can connected autonomous vehicles improve mixed traffic safety without compromising efficiency in realistic scenarios?", Ieee Transactions on Intelligent Transportation Systems, vol. 24, no. 6, p. 6674-6689, 2023. https://doi.org/10.1109/tits.2023.3238889
[33] A. Bakar, M. Abas, M. Said, & T. Azhar, "Synthesis of autonomous vehicle guideline for public road-testing sustainability", Sustainability, vol. 14, no. 3, p. 1456, 2022. https://doi.org/10.3390/su14031456
[34] Q. Yao, T. Li, C. Yan, & Z. Deng, "Accident responsibility identification model for internet of vehicles based on lightweight blockchain", Computational Intelligence, vol. 39, no. 1, p. 58-81, 2022. https://doi.org/10.1111/coin.12529
[35] M. Mayer, A. Buchner, & R. Bell, "Humans, machines, and double standards? the moral evaluation of the actions of autonomous vehicles, anthropomorphized autonomous vehicles, and human drivers in road-accident dilemmas", Frontiers in Psychology, vol. 13, 2023. https://doi.org/10.3389/fpsyg.2022.1052729
[36] B. Wang, "Approaches to autonomous driving vehicle traffic accidents liability in china", Lecture Notes in Education Psychology and Public Media, vol. 26, no. 1, p. 167-174, 2023. https://doi.org/10.54254/2753-7048/26/20230901
[37] A. Botezatu, A. Burlacu, & C. Orhei, "A review of deep learning advancements in road analysis for autonomous driving", Applied Sciences, vol. 14, no. 11, p. 4705, 2024. https://doi.org/10.3390/app14114705
[38] ADAS, 'Guest commentary: Unlocking the future of autonomous vehicle safety through ADAS simulation', Automotive News. Accessed: Jan. 19, 2024. [Online]. Available: https://www.autonews.com/guest-commentary/how-adas-simulation-can-enhance-autonomous-vehicle-safety

[39] fbilly@wordappeal.com, 'Valeo report 2022', Valeo. Accessed: Jan. 19, 2024. [Online]. Available: https://www.valeo.com/en/2022-financial-results/
[40] Why We should be Careful when Using Self-driving Vehicle Features! | IEEE Conference Publication | IEEE Xplore'. Accessed: Jan. 19, 2024. [Online] Available: https://ieeexplore.ieee.org/abstract/document/9570269
[41] Juhász A. and Molnár M. S., 'The effect of mobile phone use while driving on attention', BELÜGYI Szle. BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA 2010-, vol. 70, no. 6, Art. no. 6, 2022.
[42] Stopping distance, stopping distance, reaction time, stopping delay time. Accessed: Jan. 19, 2024. [Online]. Available: https://www.netfizika.hu/tudas/node/7894
[43] T. Chen et al, 'The Genome Sequence Archive Family: Toward Explosive Data Growth and Diverse Data Types', Genomics Proteomics Bioinformatics, vol. 19, no. 4, pp. 578-583, Aug. 2021, doi: 10.1016/j.gpb.2021.08.001.

DOI: https://doi.org/10.12700/btsz.2025.7.4.153

TERRORIST ATTACKS AGAINST THE FACILITY OF THE GREEK BANKING INDUSTRY

TERRORISTA TÁMADÁSOK A GÖRÖG BANKRENDSZER LÉTESÍTMÉNYI INFRASTRUKTÚRÁJA ELLEN

SOMOGYI Tamás[1] – NAGY Rudolf[2]

Abstract

Counter-terrorism have become a key issue within the field of security studies, particularly after the attacks on the 11th of September, 2001. Financial services are considered as essential services in the literature with examples of terrorist attacks. However, scant attention has been paid to the terrorist attacks against the banking industry's infrastructure. This study investigates the terrorist attacks against the infrastructure of the Greek banking industry based on the data of the Global Terrorism Database. The aim of this paper is to analyse the attacks, identify trends and patterns and provide recommendations to increase the level of resilience. The results may hold significance for researchers, operators of essential services, law enforcement bodies and policymakers.

Keywords

Greece; terrorism; bank; Global Terrorism Database; critical infrastructure

Absztrakt

A terrorizmussal szembeni fellépés és a védekezés kérdésköre a biztonsági kutatások egyik lényeges elemévé vált, különösen a 2001. szeptember 11-i támadásokat követően. A szakirodalom a pénzügyágazat szolgáltatásait is a létfontosságú rendszerelemek közé sorolja, ellene elkövetett terrortámadásokat is említve. Ennek ellenére a bankrendszer infrastruktúrájának terrorizmussal szembeni védelme kevés figyelmet kapott. Kutatásunkban a görögországi bankrendszer létesítményi infrastruktúrája elleni terrortámadásokat elemezzük a Global Terrorism Database adatai alapján. Célunk a megtörtént esetek vizsgálatából következtetéseket levonni, trendet, mintázatot találni és javaslatot tenni a hazai bankrendszer létesítményi infrastruktúrája ellenálló-képességének fokozására. Eredményeinket hasznosíthatják a téma kutatói, az ágazat szereplői, a rendvédelmi szervek, valamint a jogszabályalkotó.

Kulcsszavak

Görögország; terrorizmus; bank; Global Terrorism Database; létfontosságú rendszerelem

[1] somogyit588@gmail.com | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@bgk.uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habilitált egyetemi docens, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A létesítményi infrastruktúra és az általa biztosított szolgáltatások egy részét kritikusnak tekinthetjük, mivel azok elengedhetetlenek a társadalom számára nyújtott alapvető szolgáltatások működtetéséhez. A szakirodalom általában a létfontosságú rendszerelemek közé sorolja például az egészségügyi rendszert [1], az élelmiszer-ellátást [2], a vízszolgáltatást [3], az energiaellátás- és az energiahordozók infrastruktúráját [4], valamint a bankrendszert [5] is. A létfontosságú rendszerelemek zavartalan működését veszélyeztetik egyfelől a természeti csapások, másfelől a szándékos rosszakaratú támadások [6]. Az előbbi kategóriában kiemelt kérdés a klímaváltozás hatása [7], [8], míg az utóbbi csoport egyik központi kérdése a terrorizmus [9], [10]. A létfontosságú rendszerelemek védelme a szándékos támadással szemben a biztonságtudomány egyik fő területe, azon belül pedig kiemelt kutatási téma a kiberbiztonság [11], [12], [13], [14] és a mesterséges intelligencia veszélyei [15], a fizikai védelem [16], [17], a terror-elhárítás [18] és ezek megfelelő eszközei [19]. A fenyegetésekre válaszul a biztonságtudomány és a katonai műszaki tudományok jelentős multidiszciplináris tudományterületté váltak [20] és folyamatosan fejlődnek [21], az állami szervekkel és fegyveres szolgálatokkal szemben pedig elvárás lett, hogy sikerrel szálljanak szembe a társadalmat veszélyeztető erőkkel, köztük a terrorizmussal [22], [23], mindez pedig megjelenik a jogszabályokban is [24]. A gazdasági életben, a versenyszférában, az alapvető szolgáltatásokat nyújtó vállatok életében kiemelt jelentőségű és fejlődik a kockázatkezelés és biztonság témaköre [25], [26], [27].

A bankrendszert és alapvető szolgáltatásait is veszélyezteti a szándékos támadás, így ezen emberi fenyegetésekkel szembeni védelme kiemelt feladat. Egy terrortámadás hatása az ágazat szempontjából nézve súlyos lehet, hiszen - az emberi életek kioltásán túl - fennakadást eredményezhet a lakosság készpénz-ellátásában, a banki szolgáltatásokhoz való hozzáférésben, továbbá aláásha a bankrendszer biztonságába és rendelkezésre állásába vetett bizalmat. Kiemelt jelentőségű tehát a bankrendszert érő terrorfenyegetés alaposabb megértése és az ellene való védekezés fokozása. A terrorveszély határokon átívelő természete és a bankrendszer különböző országokbeli infrastruktúrájának hasonlósága is felveti a nemzetközi kitekintés alkalmazását. Cikkünk ehhez a védekezési feladathoz kapcsolódva a görögországi bankrendszer infrastruktúrája elleni terrortámadásokat vizsgálja, és ez alapján javaslatokat fogalmaz meg a hazai bankrendszer ellenálló-képességének fokozása érdekében.

KUTATÁSI MÓDSZERTAN

Kutatásunk célja a görögországi bankrendszer infrastruktúrája ellen elkövetett terrortámadások vizsgálata. Az ehhez szükséges adatok forrásának a Global Terrorism Database (GTD) adatait választottuk. Ez az angol nyelvű adatbázis több, mint 200,000, 1970 utáni terrortámadás adatait tartalmazza, az adatok megbízhatóságát pedig alátámasztja a rájuk épülő számos kutatás, például: [28], [29] és [30].

Azon terrortámadásokat dolgoztuk fel, melyeknél

- az ország (Country) Görögország („Greece“),
- a támadás célpontjának kategóriája (Target/Victim Subtype) “Bank/Commerce”,
- a támadás típusa (Attack type) infrastruktúra elleni („facility/infrastructure attack“),

- az esemény leírása (Incident summary) mező kitöltöttsége lehetővé tette az esemény elemzését.

Az esemény leírása (Incident summary) mező elemzésével döntöttük el, hogy az adott terrortámadás a bankrendszer infrastruktúráját érintette-e, és hogyan. Összesen 60 eseményt találtunk és dolgoztunk fel, melyek a fenti kritériumoknak megfelelnek, és a támadás célpontja bank, biztosító vagy ATM automata volt. Ezek a támadások 1998 - 2021. közöttiek voltak.

A TERRORIZMUS JELENTETTE FENYEGETÉS

Mirza és Rana felfedezte, hogy a 2001. szeptember 11-i terrortámadásokat követően megnövekedett a terrorizmussal foglalkozó tudományos publikációk száma [31]. Manapság kiemelt figyelem övezi ezt a területet, ráadásul a terrorfenyegetettség a védelmi rendszerek fejlesztésekor hivatkozási ponttá vált [32]. Érdekes azonban, hogy a terrorizmusnak nincsen egységesen elfogadott meghatározása [33]. Kutatásunk során mi elfogadtuk azt az általános meghatározást, mely szerint terrortámadásnak az az erőszakos cselekmény tekinthető, melyet radikalizálódott emberek követnek el szélsőséges politikai céljaik elérése érdekében.

A nagy hatású terrortámadásokat követően megnövekszik a létfontosságú rendszerelemek védelmével foglalkozó kutatások száma [34]. De vajon tényleg fenyegetést jelent a terrorizmus a létfontosságú rendszerelemekre? Khan a Közel-Kelet példáján úgy találta, hogy a terrorizmus fenyegeti az infrastruktúra zavartalan működését és negatívan hat a gazdaságra, mivel fizikailag rombol és megzavarja a szolgáltatások nyújtását és az üzleti életet [35]. Glickman igazolta, hogy a terrorizmus óriási kihívás a létfontosságú rendszerelemek védelme szempontjából [36]. Mindezen felül feltételezhetjük, hogy a terrorista támadások a jövőben is célba veszik a létfontosságú rendszerelemeket, így a védekezés kérdéskörében a jövőben is figyelembe kell venni a terrorizmust [37]. A téma jelentőségét mutatja az a tény is, hogy az infrastruktúra összekötöttsége és a szolgáltatások egymásra hatása miatt egy-egy ágazaton belül fellépő zavar más ágazatok szolgáltatásaira is kihatással lehet [38]. Példaként említhető a telekommunikációs ágazat infrastruktúrája elleni támadás okozta fennakadás, mely természetszerűleg más ágazatokat, illetve a védekezésben dolgozókat is érinti [39]. A pénzügyi ágazat szolgáltatásai is jól példázzák az egymásra utaltságot: a létfontosságú rendszerelemek üzemeltetői is igénybe veszik a pénzügyágazat szolgáltatásait az alkalmazottjaikkal, ügyfeleikkel és beszállítóikkal való elszámolás során, mely elérhetetlensége veszélyezteti a saját létfontosságú rendszerelemük üzemeltetését. Egy-egy ágazaton belüli hatás és az ágazatok közötti kapcsolatok miatt tovaterjedő hatás okán kijelenthető, hogy a terroristák számára vonzó létfontosságú rendszerelemben üzemzavart okozni.

Terrortámadások elemzése rámutatott arra, hogy a támadások lehetnek egyszerűek, valamint komplexek és költségesek is. Például az energiaszektorban a támadók a vezetékeket megrongálva fennakadásokat tudnak okozni egyszerű szerszámokkal vagy robbanóanyagokkal [40]. Besenyő említ eseteket, amikor terroristák kövekkel, baseballütőkkel és késekkel támadtak kórházakat [41]. Egyszerű eszközökkel nem csak az infrastruktúra támadható, hanem széles körű sérülések is okozhatóak terrortámadás során [42]. Másfelől, a terroristák eszköztárában megjelenik a modern technika is, hiszen az információbiztonság területén belül is fenyegetésként tekintenek a terrorizmusra [43]. A modern információ technológiát a terroristák is használják információszerzésre, pénzügyi támogatások és bevételek céljából, továbbá kapcsolattartásra és új tagok beszervezésére [44], [45], [46], sőt, némely

terrorszervezet saját hírszerző szolgálattal rendelkezik [47], ami egyértelműen láttatja az erejüket és képességeiket. Létfontosságú rendszerelemek szempontjából kijelenthető, hogy mind az egyszerű eszközökkel, mind pedig a legfejlettebb eszközökkel elkövetett terrortámadások veszélyt jelentenek. Ezt támasztják alá Marx és szerzőtársai az egészségügy területéről vett példával: úgy vélik, hogy a kórházakat érintő két legnagyobb terrorfenyegetés a kibertámadás és a hagyományos fegyverekkel elkövetett támadás [48].

Meg kell említeni, hogy a terrorszervezetek némelyikét államok is támogatják [49], a terrorizmus az úgynevezett proxy-háború részévé vált [50]. A hibrid háború olyan valóság lett Európában, mely nem hagyható figyelmen kívül létfontosságú rendszerelemek elleni védekezés során [51], [52]. Következésképpen némely terrorszervezet rendelkezhet olyan anyagi erőforrással és technológiával (például vegyi fegyverekkel [53]), melyekkel nagy hatású támadást tudnak indítani. Mindez megvilágítja a létfontosságú rendszerelemek védelmének jelentőségét, beleértve a bankrendszer létesítményi infrastruktúráját is.

Terrorszervezetek bankrendszer elleni támadására példát ad többek között Besenyő és Hegedűs [54]. Az ilyen terrortámadások motivációja sokrétű lehet [55], de minden bizonnyal szerepet játszik a lakosság megfélemlítésének, a zavarkeltésnek és az anyagi károk előidézésének a célja. Az elektronikus fizetési megoldásokhoz való hozzáférésben és a készpénzellátásban okozott zavarral a terroristák elérhetik ezen céljaikat. Ráadásul hosszabb távú hatást is el tudnak érni. Bizonyított ugyanis, hogy a terrorizmus jelenléte csökkenti az egy főre jutó GDP értékét [56], ugyanis a konfliktusok általában és a terrorizmus konkrétan negatívan hatnak a befektetésekre és a gazdasági fejlődésre. A befektetések mellett említhető még a turizmus is, mivel természetes módon csökken a turizmus és az ebből származó bevétel a terrortámadásokkal terhelt régiókban, hiszen a turizmus megköveteli a biztonságot [57].

A bankok és a pénzügyi élet elleni támadások elérhetik a fentebb említett célokat [58], különösen, ha a szektorokon átívelő egymásra hatást is figyelembe vesszük. A pénzügyi szolgáltatások kiesése likviditási problémát okozhat más ágazatokban, továbbá a lakosság készpénz-ellátását és fizetési képességeit megzavarhatja, mely politikai instabilitáshoz is vezethet. Ráadásul Posso igazolta, hogy a terrorizmus- és fegyveres konfliktusok sújtotta régiókban az emberek a hivatalos bankrendszeren kívül keresnek pénzügyi megoldásokat, melyeket ellenállóbbnak vélnek [59]. Ezzel szemben a felügyelt és szigorú szabályok szerint működő bankrendszer fontos szerepet játszik a terrorizmus elleni küzdelemben [60], illetve a radikalizálódó szervezetek pénzeszközei korlátozásának végrehajtásában [61], [62]. Itt meg kell említeni, hogy a bankrendszer a bevezetett gazdasági szankciókat végrehajtja (például az elmúlt években Oroszországgal szemben bevezetett szankciók [63], ez pedig növeli annak kockázatát, hogy egyes államok és az általuk támogatott terrorszervezetek célpontjává válhat. A bankrendszer elleni terrortámadások egy további motivációja lehet a migráció ösztönzése az instabilitás előidézésével. Igazolt, hogy a terrorszervezetek is részesei az embercsempészetnek és az illegális migráció segítésének [64]. Mindezek alapján kijelenthető, hogy a létfontosságú rendszerelemek, beleértve a pénzügyágazatot is, terrortámadásokkal szemben kitettek, így védelmük kiemelt jelentőségű.

A bemutatott eredmények alátámasztják a terrorizmus veszélyét a létfontosságú rendszerelemekre, és ezt vetítik előre a jövőre nézve is [65]. Ráadásul a fentiek alapján elmondható, hogy a terrorszervezetek lépést tartanak a technológiai fejlődéssel, ami tovább növeli a fenyegetést. Látható tehát a terrorizmus elleni küzdelem jelentősége, melynek része a terrorizmus- és a terrortámadások alaposabb megismerése is. A következő rész ezért a

görögországi bankrendszer létesítményi infrastruktúrája elleni terrortámadások bemutatásával és elemzésével foglalkozik.

A GÖRÖGORSZÁGI BANKRENDSZER LÉTESÍTMÉNYI INFRASTRUKTÚRÁJA ELLEN ELKÖVETETT TERRORTÁMADÁSOK

A Global Terrorism Database (GTD) adatait a Kutatási módszer részben leírtak szerint szűrtük le, és eredményként 60 terrortámadást kaptunk. A támadások többségében bankfiókokat támadtak, azonban előfordult 3 esetben valamely biztosítócég fiókja elleni támadás, továbbá 11 támadás során bankfiókon kívüli ATM automata volt a célpont. Az adatbázisban regisztrált 60 megtörtént esetből az alábbiak állapíthatóak meg.

A bankrendszer infrastruktúrája elleni terrortámadás példájaként hozható a 2003. március 22-én, Koropi városában történt támadás, mely során a kora reggeli órákban a Citibank fiókjánál gyújtóbomba lépett működésbe. A támadásban az ATM automata rongálódott meg. Egy másik jellegzetes eset a 2007. június 5-i támadás, amikor is Athénban 10 ismeretlen elkövető molotov-koktélokat dobott az Eurobank egyik fiókjára, megrongálva a bankfiókot és benne az ATM automatát. Ehhez hasonló esetet jegyeztek fel 2008. május 30-án Thesszalonikiben, ahol a hajnali órákban a Millenium bank egyik fiókjára dobtak gyújtóbombát, mely megrongálta a homlokzatot.

Az eddig említett jellegzetes egyedi támadások mellett összehangolt, több helyszínt érintő támadássorozatot is találni az esetek között. Kavalában 2009. december 16-án a késői órákban egy összehangolt terrortámadás során négy bank fiókját támadták meg molotov-koktélokkal, és két másik bankfiók ablakait kőtörő kalapácsokkal betörték. Hasonló eseménysorozat történt 2009. június 4-én Athénban az éjszakai órákban: három bankfiókot támadtak meg kis propán-gázpalackból barkácsolt bombákkal. Szintén Athénban történt 2020. május 18-án az a terrortámadás-sorozat, melyben negyedórán belül összesen 8 helyszín lobbant lángra, köztük két helyszínen bankfiókon kívüli ATM automatákat gyújtottak fel. Az összes eset közül a legnagyobb összehangolt támadássorozat 2008. február 21-én történt hajnal 2 órakor Athénban és az agglomerációjában, amikor is egy biztosítót, nyolc bankfiókot és egy banki céges gépjárművet támadtak meg terroristák házilag épített gyújtóbombákkal. Említettük, hogy kis számban biztosítók is célpontjai voltak terrortámadásoknak. Erre egy másik példa a 2008. szeptember 26-án, Athénban történt támadássorozat, amikor a hajnali órákban egyidőben egy bankfiókot és két biztosítói irodát támadtak meg.

A hatóságok gyanúja szerint politikai okok húzódtak meg az 1999. július 7-i támadás mögött, mely során Athénban a Nemzeti Bank épületére három gyújtóbombát dobtak ismeretlenek. Ezt a terrortámadást összefüggésbe hozták egy minisztériumi épületet korábban időzített bombával támadó terrorista akkor folyamatban lévő bírósági tárgyalásával. Egy másik, szintén extrém politikai célok elérése érdekében indított támadássorozat történt 2014. november 30-án, amikor is egyszerre összesen hét ATM automatát robbantottak fel a főváros különböző kerületeiben egy akkor börtönben lévő terrorista társuk melletti kiállásukat demonstrálandó.

Az összes, feldolgozott terrortámadást tekintve elmondható, hogy a nagy többségüknél nem jelentettek személyi sérülést vagy halálos áldozatot. Ez valószínűleg annak köszönhető, hogy ezen terrortámadásokat banki nyitvatartási időn kívül követték el. A személyi sérülés szempontjából kivételes eset a 2008. november 2-án Thesszalonikiben zajlott

támadás, mely során az elkövetők nem csak hogy megtámadtak egy bankfiókot és a közelben parkoló autók közül is megrongáltak 30 járművet, hanem harcba is bocsátkoztak a kiérkező rendőri erőkkel, nyolc rendőrnek okozva sérülést.

A görögországi bankrendszer infrastruktúrája elleni terrortámadások helyszínei kapcsán elmondható, hogy a 60 támadásból 48 (80%) a fővárosban, Athénban történt. A többi támadás nagy része a fontosabb kikötővárosokban (Thesszaloniki, Pireusz, Iráklio) zajlott. Ez valószínűleg annak is köszönhető, hogy ezen nagy kikötővárosokban zajló jelentős kereskedelmet és utasforgalmat több bank és biztosító szolgálja ki, ebből fakadóan ezen helységekben nagyobb a bankrendszer létesítményi infrastruktúrája.

A terrortámadások áttekintése után érdemes megvizsgálni a támadások évenkénti darabszámát trend és mintázat megállapítása érdekében. Az alábbi táblázat mutatja a görögországi bankrendszer infrastruktúrája ellen elkövetett és itt elemzett 60 terrortámadás évenkénti eloszlását. Ezekből az adatokból kiolvasható, hogy a terrortámadások száma nem egyenletes, sőt, vannak évek, amikor egyetlenegy támadást sem regisztráltak. Viszont a vizsgált támadások által lefedett bő két évtizedben kb. évtizedenként volt egy év, amely során kiemelkedően magas volt a terrortámadások száma.

Évszám	terrortámadás (db)
1998	1
1999	1
2000	0
2001	0
2002	0
2003	6
2004	0
2005	0
2006	6
2007	1
2008	17
2009	15
2010	1
2011	0
2012	0
2013	1
2014	7
2015	0
2016	0
2017	0
2018	0
2019	0
2020	4
2021	0

1. Táblázat A görögországi bankrendszer létesítményi infrastruktúrája ellen elkövetett terrortámadások száma évenkénti bontásban (szerzői szerkesztés)

A görögországi bankrendszer létesítményi infrastruktúrája elleni terrortámadások áttekintése után a levonható következtetéseket és az ezek alapján megfogalmazható javaslatokat a következő rész tartalmazza.

KÖVETKEZTETÉSEK

Első következtetésként elmondható, hogy az áttekintett terrortámadások, mint megtörtént események alátámasztják azt, hogy a bankrendszer infrastruktúrájának megzavarása, szolgáltatásainak nyújtásában fennakadások okozása a terrorszervezetek gyakorlata, Európában is valóság. A bankrendszer támadásával kétségtelenül fel tudják hívni magukra a figyelmet, továbbá félelmet kelthetnek a lakosságban és a pénzügyi élet szereplői körében, mely akár gazdasági és politikai instabilitáshoz is vezethet. Valószínűleg a terroristák ezen céljai is magyarázzák - a létesítményi infrastruktúra nagyobb fokú jelenléte mellett - azt a tényt, hogy a támadások túlnyomó többsége a fővárosban és jelentős kikötővárosokban történt. Mindenesetre az adatok alapján kijelenthető, hogy a fővárosi és a nagyobb városokban lévő banki infrastruktúra terrortámadásnak kitett.

Fontos kiemelni, hogy az elemzett támadások során az elkövetők nem vették célba a banki- és biztosítói alkalmazottakat, és az ügyfeleket sem, céljuk az infrastruktúra megrongálása és a szolgáltatásokban fennakadás okozása volt. Az elkövetőek a támadások időpontját úgy választották meg, hogy a támadáskor se alkalmazottak, se ügyfelek ne tartózkodjanak a helyszínen. Ugyanakkor a hazai bankrendszer számárára már másfél évtizede javasolt fejlesztés fontosságát [66] kutatásunk eredménye is alátámasztja: a vagyonvédelmi eszközök fejlesztése mellett sürgethető az alkalmazottak pszichés felkészítése munkahelyük terroristatámadásokkal szemben való kitettségére.

A támadásoknak a kizárólag a létesítményi infrastruktúrát célzó természetükből az is következik, hogy a támadás észlelése, a keletkezett tűz terjedésének korlátozása és az oltás megkezdése kizárólag a vagyonvédelmi- és tűzvédelmi berendezésekre hárul. Következésképpen a bankrendszer létesítményi infrastruktúrájának üzemeltetésekor, illetve általánosságban a létfontosságú rendszerelemek üzemeltetésekor kiemelt figyelmet kell fordítani ezen védelmi eszközök telepítésére és karbantartására. Igazolt ugyanis, hogy az ilyen eszközök nem megfelelő üzemeltetése csökkenti az általuk nyújtott védelem szintjét [67].

Levonható továbbá az a következtetés is, hogy vagyonvédelmi- és tűzvédelmi berendezések fejlesztési irányának meghatározásakor figyelembe kell venni a - házilag barkácsolt, egyszerű eszközökből épített - gyújtóbombákkal elkövetett támadásokat is. Esszenciális a védelmi eszközök és tűzoltásban használt anyagok folyamatos fejlesztése [68], mely folyamatba javasolható bevonni a bankrendszer szereplőit is a bankfiókok, ATM automaták kialakításának és elhelyezkedésének sajátosságainak figyelembe vétele érdekében. A bankrendszer számára javasolható vonatkozó kutatás-fejlesztés megrendelőjeként és finanszírozójaként való fellépés.

A görögországi terrortámadások évenkénti számossága alapján látható, hogy csekély számú terrortámadások után, körülbelül évtizedenként egyszer bekövetkezik egymáshoz időben közel több támadás. Hazánkban 2014. január 13-án Budapesten, a CIB bank egyik fiókjánál történt robbantás, utána a GTD több hazai eseményt nem tartalmaz. Ugyanakkor a görögországi adatokon látható, hogy a támadások eloszlása nem egyenletes, ezért nem lehet az esetleges alacsony támadási számból egy jövőbeli alacsony bekövetkezési va-

lószínűségre következtetni. Időszerű és lényeges tehát a hazai bankrendszer terrortámadásokkal szembeni ellenálló-képességének vizsgálata és növelési lehetőségének kutatása, mely hozzájárulhat a védekezés, megelőzés és elhárítás szereplőinek fejlődéséhez is, továbbá más ágazatok létfontosságú rendszerelemeinek tekintetében is hasznosnak bizonyulhat.

ÖSSZEFOGLALÁS

Szakirodalom a bankrendszert a terrorszervezetek számára vonzó célpontként tartja számon, némely szerző megtörtént támadásokat is említ. Kutatásunkban egy hazánkkal több szempontból hasonló országban, Görögországban a bankrendszer infrastruktúrája ellen elkövetett terrortámadásokat dolgoztuk fel. Az eseteket a Global Terrorism Database adatbázisából vettük.

Az eredményeink alátámasztják, hogy a bankrendszer infrastruktúrája terrortámadásnak kitett, főleg a fővárosban és a nagyobb városokban. A regisztrált támadások alapján elmondható, hogy a terroristák célpontja az infrastruktúra volt, és nem alkalmazottak vagy ügyfelek. A támadások száma nem egyenletes eloszlású, néhány nyugodt év után is bekövetkezhet több támadás. Így időszerű és lényeges kérdés a bankrendszer infrastruktúrájának, tágabban pedig a létfontosságú rendszerelemek védelmének kérdésköre.

Az elemzésünkből az látható, hogy a görögországi terrortámadásokat robbantással vagy gyújtogatással követték el nyitvatartási időn kívül. Ebből következően a támadás észlelése, a keletkezett tűz terjedésének korlátozása és az oltás megkezdése kizárólag a vagyonvédelmi- és tűzvédelmi berendezésekre hárul. Következésképpen a bankrendszer infrastruktúrájának üzemeltetésekor, illetve általánosságban a létfontosságú rendszerelemek üzemeltetésekor kiemelt figyelmet kell fordítani ezen védelmi eszközök telepítésére és karbantartására, valamint a bankrendszer infrastruktúrája sajátosságainak figyelembe vételével a fejlesztésükre.

FELHASZNÁLT IRODALOM

[1] Veresné, R.J., Berek, L. „Kórházak biztonsága és védelme I.: Kockázati tényezők és lehetséges következmények” *HADMÉRNÖK*, 16(4), 2021, https://doi.org/10.32567/hm.2021.4.2

[2] Al Harbi, B., Marikar, F. „Food security and its impact on Saudi Arabia’s national security and Gulf security.” *Journal of Defense Resources Management*, (16)1, 2025, http://dx.doi.org/10.64404/JoDRM.2025.1.06

[3] Berek, T. „ A vészhelyzeti vízellátás biztonsági aspektusai” In: Földi, L. (szerk.) *Szemelvények a katonai műszaki tudományok eredményeiből I.*, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2021) https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16207/905_KMDI_I_oktatoi_tanulmany-kotet.pdf#page=14

[4] Polat, M.A., Kovács, T.A. „A hidrogén tulajdonságainak, előállításának, tárolásának, logisztikájának és biztonsági kritériumainak áttekintése” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(2), 2025, https://doi.org/10.12700/btsz.2025.7.2.1

[5] Somogyi, T. „A készpénz-ellátás jelentősége és biztosítása Magyarországon és Írországban.” *BIZTONSÁGTUDOMÁNYI SZEMLE*, 5(3), 2023 https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/359/291
[6] Faramondi, L., Oliva, G., and Setola, R. „Multi-criteria node criticality assessment framework for critical infrastructure networks.” *International Journal of Critical Infrastructure Protection*, 28, 2020, https://doi.org/10.1016/j.ijcip.2020.100338
[7] Földi, L., Berek, T. and Padányi, J. „Hungary’s Energy and Water Security Countermeasures as Answers to the Challenges of Global Climate Change.” *AARMS*, 20(2), 2021, https://doi.org/10.32565/aarms.2021.2.7
[8] Bodnár, L., Teknős, L. „The effect of global climate change on wildfires - Major changes in the fire trends.” In: Lestyán, Mária; Bodnár, László; Érces, Gergő; Varga, Ferenc (szerk.) *International Disaster Management Scientific Conference - Focus on Changes in the Fire Safety Situation* Budapest, Magyarország : Magyar Tűzvédelmi Szövetség (2024) ISBN: 9786150209876
[9] Besenyő, J., Issaev, L., Korotayev, A. „Introduction: Terrorism and Political Contention in North Africa and the Sahel Region.” In: Korotayev, A., Issaev, L., Besenyő, J. (szerk.) *Terrorism and Political Contention : New Perspectives on North Africa and the Sahel Region*, Cham, Svájc : Springer Nature Switzerland (2024) https://doi.org/10.1007/978-3-031-53429-4_1
[10] Besenyő, J. „Prevention of the Terror Attack and the Social Aspects in the European Union” In: Kovács, Tünde Anna; Fürstner, Igor (szerk.) *Critical Infrastructure Protection: Advanced Technologies for Crisis Prevention and Response* Dordrecht, Hollandia : Springer Netherlands (2025) ISBN: 9789402423075
[11] Kovács, L. „Offenzív kiberműveletek II. Kibererők és képességeik.” *Hadmérnök*, 16(3), 2021, https://doi.org/10.32567/hm.2021.3.7
[12] Csercsa, K., Rajnai, Z. „Adatvédelem és információbiztonság: az online térben fellelhető veszélyforrások, adathalászati módszerek (social engineering)” *BIZTONSÁGTUDOMÁNYI SZEMLE* 7(2), 2025, https://doi.org/10.12700/btsz.2025.7.2.49
[13] Mandić, D., Kiss, G. „Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában” In: Kiss, Gábor (szerk.) *30TH ANNIVERSARY CONFERENCE OF THE SAFETY AND SECURITY ENGINEERING EDUCATION : A BIZTONSÁGTECHNIKAI MÉRNÖK KÉPZÉS 30 ÉVI JUBILEUMI KONFERENCIÁJA* Budapest, Magyarország : Óbudai Egyetem (2023) ISBN: 9789634493297
[14] Dér, A. „Aspects of cyber defence in Africa” *Journal of Central and Eastern European African Studies*, 5(1), 2025 https://doi.org/10.12700/jceeas.2025.5.1.341
[15] Kollár, Cs. „A magyarországi magánbiztonsági szektor válasza a mesterséges intelligencia kihívásaira, avagy: Biztonság és technika a mesterséges intelligencia korában” In: Kiss, Gábor (szerk.) *30TH ANNIVERSARY CONFERENCE OF THE SAFETY AND SECURITY ENGINEERING EDUCATION : A BIZTONSÁGTECHNIKAI MÉRNÖK KÉPZÉS 30 ÉVI JUBILEUMI KONFERENCIÁJA* Budapest, Magyarország : Óbudai Egyetem (2023) ISBN: 9789634493297
[16] Daruka, N. „Options for Implementing Explosion Protection in Critical Infrastructure” In: Kovács, Tünde Anna; Stadler, Róbert Gábor; Daruka, Norbert (szerk.) *The Impact of the Energy Dependency on Critical Infrastructure Protection : Proceedings of the 5th International Conference on Central European Critical Infrastructure Protection*

(ICCECIP 2023) Budapest, Hungary, Cham, Svájc : Springer Nature Switzerland (2025) ISBN: 9783031785436

[17] Márton, Z., Rajnai, Z. and Berek, L. „Kritikus infrastruktúrák objektumvédelmének kihívásai a social engineering támadások kontextusában" *BIZTONSÁGTUDOMÁNYI SZEMLE,* 7(2), 2025, https://doi.org/10.12700/btsz.2025.7.2.57

[18] Jasenszky, N., Regényi, K.M. and Lippai, Zs. „A biztonságtudatosság fogalma, fejlődése nemzetbiztonsági, terrorelhárítási és magánbiztonsági szempontból." *Nemzetbiztonsági Szemle,* 9(4), 2021, https://doi.org/10.32561/nsz.2021.4.1

[19] Nyikes, Z., Tóth, L. „Cybersecurity Challenges in the Age of Drones: Navigating the Integration of Unmanned Aerial Vehicles with Cyberspace" In: Kovács, Tünde Anna; Stadler, Róbert Gábor; Daruka, Norbert (szerk.) *The Impact of the Energy Dependency on Critical Infrastructure Protection : Proceedings of the 5th International Conference on Central European Critical Infrastructure Protection (ICCECIP 2023), Budapest, Hungary,* Cham, Svájc : Springer Nature Switzerland (2025) ISBN: 9783031785436

[20] Vuk, P. „Military Science and Educational Institutions." *Contemporary Military Challenges*, 25(2), 2023, https://doi.org/10.2478/cmc-2023-0011

[21] Záhonyi, L., Szűcs, E. „Examining the relationships and legal regulation of information security and data protection, with particular regard to the communication habits of young people" *NATIONAL SECURITY REVIEW* 2023/1, 2023 https://s2prodstorage.blob.core.windows.net/s2cmsblob/Files/National%20Security%20Review/2023_1_NSR.pdf

[22] Resperger, I. „A jövő biztonsági problémái." *Szakmai Szemle*, 19(2), 2021, https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_2_szam.pdf#page=5

[23] Besenyő, J., Sikimić, M. „Police Role in the Security of Critical Infrastructure." In: Kovács, T.A., Stadler, R.G., Daruka, N. (eds) *The Impact of the Energy Dependency on Critical Infrastructure Protection. ICCECIP 2024.* Advanced Sciences and Technologies for Security Applications. Springer, Cham (2025) https://doi.org/10.1007/978-3-031-78544-3_45

[24] Trinchillo, F. „Critical infrastructures: European context and evolution of the law." *Journal of Defense Resources Management*, 16(1), 2025 https://doi.org/10.64404/JoDRM.2025.1.15

[25] Michelberger, P. „Integrált vállalati kockázatmenedzsment: Lehetőségek és veszélyek a szabványok és ajánlások tükrében", BIZTONSÁGTUDOMÁNYI SZEMLE 7(1), 2025, https://doi.org/10.12700/btsz.2025.7.1.25

[26] Mészáros, Á., Csiszárik-Kocsir, Á. „A pszichológiai biztonság egyes elemeinek megjelenése az oktatásban a csapatfeladatok abszolválása során", *BIZTONSÁGTUDOMÁNYI SZEMLE* 6(4), 2024, https://doi.org/10.12700/btsz.2024.6.4.16

[27] Kollár, Cs. „A biztonság fontosabb fogalmai", *BIZTONSÁGTUDOMÁNYI SZEMLE*, 7(1), 2025, https://doi.org/10.12700/btsz.2025.7.1.15

[28] Jasani, G., Alfalasi, R., Liang, S. „Terrorist attacks against emergency departments." *The American Journal of Emergency Medicine*, 64, 2023, https://doi.org/10.1016/j.ajem.2022.11.011

[29] Hermann, Z. „15 years of analyzing the Global Terrorism Database: An overview." *Scientia et Securitas*, 4(1), 2023, https://doi.org/10.1556/112.2023.00139

[30] Guohui, L. et al. „Study on Correlation Factors that Influence Terrorist Attack Fatalities Using Global Terrorism Database." *Procedia Engineering*, 84, 2014 https://doi.org/10.1016/j.proeng.2014.10.475
[31] Mirza, M.N.E., Rana, I.A. „A systematic review of urban terrorism literature: Root causes, thematic trends, and future directions." *Journal of Safety Science and Resilience*, 5, 2024, https://doi.org/10.1016/j.jnlssr.2024.03.006
[32] Kátai-Urbán, L., Vass, Gy., Zellei, G. „25 éve működik hazánkban a radiológiai távmérő hálózat." *Hadtudomány*, 28(2), 2018, https://doi.org/10.17047/HADTUD.2018.28.2.140
[33] Pék, R.T. „Jelzőkkel teleaggatott terrorizmus." *Magyar Rendészet*, 2022/2, 2022, https://doi.org/10.32577/mr.2022.2.14
[34] Papamichael, M., Dimopoulos, C., Boustras, G. „Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations." *Sustainable and Resilient Infrastructure*, 2024, https://doi.org/10.1080/23789689.2024.2340368
[35] Khan, H.U. „An analytical investigation of consequences of terrorism in the Middle East." *Journal of Economic Criminology,* 4, 2024, https://doi.org/10.1016/j.jeconc.2024.100067
[36] Glickman, T. „Program portfolio selection for reducing prioritized security risks." *European Journal of Operational Research,* 190, 2008, https://doi.org/10.1016/j.ejor.2007.06.006
[37] Jenelius, E., Westin, J., Holmgren, Å. „Critical infrastructure protection under imperfect attacker perception." *International Journal of Critical Infrastructure Protection*, 3(1), 2010, https://doi.org/10.1016/j.ijcip.2009.10.002
[38] Sellevåg, S.R. „Changes in inoperability for interdependent industry sectors in Norway from 2012 to 2017." *International Journal of Critical Infrastructure Protection*, 32, 2021, https://doi.org/10.1016/j.ijcip.2020.100405
[39] Besenyő, J., Sinkó, G. „Challenges to National DRM Systems: Analyzing the Reactions of Al-Shabaab's 2022 Attack on Hormuud Telecom in Somalia." In: Kowalkowski, S., Kaźmierczak, D., Paul, S. (eds) *Civil Protection Systems and Disaster Governance*. Palgrave Macmillan, Cham. 2024. https://doi.org/10.1007/978-3-031-60167-5_6
[40] Eze, J., Nwagboso, C. and Georgakis, P. „Framework for integrated oil pipeline monitoring and incident mitigation systems." *Robotics and Computer–Integrated Manufacturing*, 47, 2017, http://dx.doi.org/10.1016/j.rcim.2016.12.007
[41] Besenyő, J. „Terror attacks against African health facilities." In: Florian, CÎRCI-UMARU and Constantin-Crăișor, IONIȚĂ (eds.) *P R O C E E D I N G S: INTERNATIONAL SCIENTIFIC CONFERENCE STRATEGIES XXI - THE COMPLEX AND DYNAMIC NATURE OF THE SECURITY ENVIRONMENT*, Bukarest, Romania : Carol I National Defence University Publishing House (2022) https://cssas.unap.ro/en/pdf_books/conference_2021.pdf
[42] Faggyas, A., Rémai, D. „A modern és posztmodern terrorizmus: a helyszíni terrorizmus: a helyszíni egészségügyi ellátás kihívásai." *Magyar Rendészet*, 2024/1., 2024, https://doi.org/10.32577/mr.2024.1.3
[43] Theoharidou, M., Xidara, D. and Gritzalis, D. „A CBK for Information Security and Critical Information and Communication Infrastructure Protection." *International*

Journal of Critical Infrastructure Protection, 1, 2008, https://doi.org/10.1016/j.ijcip.2008.08.007
[44] Suller, Z. „Trendi terrorizmus: terroristamarketing, toborzás és megfélemlítés a közösségi médiában." *Nemzetbiztonsági Szemle*, 11(2), 2023, https://doi.org/10.32561/nsz.2023.2.3
[45] Bufnea, I.-M. „The terrorist phenomenon, social media and the internet. social and psychological implications." *Strategic Impact (Romania)*, 3(92), 2025, https://doi.org/10.53477/1842-9904-24-16
[46] Gulyás, A. „Cybercrime and dark web in Africa." *Journal of Central and Eastern European African Studies*, 4(3-4), 2025, https://doi.org/10.12700/jceeas.2024.4.3-4.278
[47] Sinkó, G., Besenyő, J. „More than Survival: The Role of al-Shabaab Secret Service, Amniyat, in Information-Gathering" *Connections QJ*, 22(1), 2024, https://doi.org/10.11610/Connections.22.1.36
[48] Marx, J., Leroy, C., Philippe, J. and Vivien, B. „L'hôpital attaqué." *La Presse Médicale Formation*, 5(3), 2024, https://doi.org/10.1016/j.lpmfor.2024.04.003
[49] Besenyő, J., Keresztes, V. „Hezbollah and Boko Haram: Cooperation or Imitation?" *Strategic Impact (Romania),* 61(4), 2016, http://cssas.unap.ro/en/pdf_periodicals/si61.pdf
[50] Boda, M. „A proxyháború filozófiai és etikai megközelítésben." *Honvédségi Szemle*, 151(6), 2023, https://doi.org/10.35926/HSZ.2023.6.3
[51] Vasilescu, C., Codreanu, A. „Bridging the gap between analysis and prediction – towards the development of an integrated predictive model for hybrid threat risk assessment." *Romanian Military Thinking*, 4, 2024, https://doi.org/10.55535/RMT.2024.4.35
[52] Prebilič, V., Rebrica, P. „Cyber Warfare in the Russo-Ukrainian War." *CONTEMPORARY MILITARY CHALLENGES*, 26(4), 2024, https://doi.org/10.2478/cmc-2024-0030
[53] Nagy, R. „Hólyaghúzó harcanyagok gázkromatográfiás paramétereinek azonosítása alacsony dízelolaj-szennyezettség mellett." *BIZTONSÁGTUDOMÁNYI SZEMLE*, 5(3), 2023, https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/358/304
[54] Besenyő, J., Hegedűs, É. „Countering Extremist Violence and Terrorism in Cabo Delgado: (How) Can Past Peace-Building and DDR Lessons Be of Use?" *Journal of Central and Eastern European African Studies* 3(4), 2024, https://doi.org/10.59569/jceeas.2023.3.4.244
[55] Erdélyi, Á. „Az ámokfutás és a pszichopatológiai terrorizmus lélektana" Nemzetbiztonsági Szemle, 10(2), 2022, https://doi.org/10.32561/nsz.2022.2.7
[56] Paul, J.A., Bagchi, A. „Immigration, terrorism, and the economy" *Journal of Policy Modeling*, 45(3), 2023, https://doi.org/10.1016/j.jpolmod.2023.03.002
[57] Rácz, A. „Magyarország országképe és a turizmusbiztonsággal kapcsolatos attitűdök empirikus vizsgálata 2018-ban" *Turizmus Bulletin*, 19(4), 2019, https://doi.org/10.14267/TURBULL.2019v19n4.5
[58] Somogyi, T., Nagy, R. „Terrorist attacks against the european banking industry since 2001" *Strategic Impact (Romania),* 3(92), 2025, https://doi.org/10.53477/1842-9904-24-17

[59] Posso, A. „Terrorism, banking, and informal savings: Evidence from Nigeria" *Journal of Banking & Finance,* 150, 2023, https://doi.org/10.1016/j.jbankfin.2023.106822
[60] Bugyáki, A. „A pénzmosás gyakorlata a szervezett bűnözés és a terrorizmus összefonódásában – Fogalmi tisztázás és gyakorlati kapcsolatok" *Nemzet és Biztonság*, 16(1), 2023, https://doi.org/10.32576/nb.2023.1.5
[61] Udvarvölgyi, Zs. „Európai iszlám közösségek a politikai önszerveződés útján" *Szakmai Szemle*, 19(2), 2021, https://www.knbsz.gov.hu/hu/letoltes/szsz/2021_2_szam.pdf
[62] Bálint, F. „Anti-money laundering with a special focus on the cyber security threats and vulnerabilities" *NATIONAL SECURITY REVIEW,* 2023/2, 2023, https://s2prodstorage.blob.core.windows.net/s2cmsblob/Files/National%20Security%20Review/2023_2_NSR.pdf?sp=r&st=2025-03-25T09:37:58Z&se=2035-03-25T16:37:58Z&spr=https&sv=2024-11-04&sr=c&sig=PAOb3jtCphbbzRgBEutrTUH2uSjRNnF3G8dVaL8Y3Z0=
[63] Tóth, T.E. „A világ ezután nem ugyanaz, mint azelőtt volt – Korszakváltás a német külpolitikában?" *Nemzet és Biztonság*, 16(4), 2024, https://doi.org/10.32576/nb.2023.4.4
[64] Csányi, Cs. „Terrorizmus és Szervezett bűnözés, Avagy Profit Vs. Ideológia?" *Belügyi Szemle*, 66(2), 2018, https://doi.org/10.38146/BSZ.2018.2.5
[65] Vajda, E. „A radikális iszlám várható tendenciái Európában" *Nemzetbiztonsági Szemle*, 10(1), 2022, https://doi.org/10.32561/nsz.2022.1.2.
[66] Fialka, Gy. „A pénzintézetek technikai biztonságának történeti fejlődése és jövője" *Hadmérnök*, 5(2), 2010, http://hadmernok.hu/2010_2_fialka.pdf
[67] Berek, L., Hódosi, V. „Veszélyes objektumok biztonsági rendszereinek ellenőrzése" *Hadmérnök*, 14(3), 2020, https://doi.org/10.32567/hm.2019.3.1
[68] Krepuska, A.I. „Fejlesztések jelentősége az aktív tűzvédelemben" In: Nagy, Rudolf (szerk.) *Szilvay Kornél Tűzvédelmi Konferencia*, Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar (2023) (2025.11.14.)

DOI: https://doi.org/10.12700/btsz.2025.7.4.167

FROM THEORY TO PRACTICE: ANALYSIS OF ARTIFICIAL INTELLIGENCE REGULATION IN THE EUROPEAN UNION – RECOMMENDATION ON GENERAL TERMS AND CONDITIONS

ÚT AZ ELMÉLETTŐL A GYAKORLATIG: A MESTERSÉGES INTELLIGENCIA EURÓPAI UNIÓS SZABÁLYOZÁSÁNAK ELEMZÉSE – AJÁNLÁS AZ ÁLTALÁNOS FELHASZNÁLÁSI FELTÉTELEKRE

ANTAL Tímea[1] – SZÁMADÓ Róza[2]

Abstract

The rapid development of artificial intelligence (AI)-based applications has brought with it new legal and security challenges. In order to reduce the pitfalls and risks of practical application, it is necessary to examine the stages of development of European Union regulations and, based on this, make proposals for the main elements of the general terms of use for artificial intelligence applications. Regulations and the general terms and conditions of use that appear in specific applications play a key role in ensuring regulatory compliance. The aim of this study is twofold: on the one hand, to present and analyze the development of EU artificial intelligence regulation, and on the other hand, to formulate recommendations for the general terms of use of AI applications on a scientific and legal basis.

Keywords

artificial intelligence regulation, European Union, general terms of use of AI, compliance

Absztrakt

A mesterséges intelligencia (MI) alapú alkalmazások gyors fejlődése új jogi és biztonsági kihívásokat hozott magával. A gyakorlati alkalmazás buktatóinak, kockázatának csökkentése érdekében szükséges vizsgálni az európai uniós szabályozás fejlődési lépcsőit, és erre alapozva javaslatot tenni a mesterséges intelligencia alkalmazások általános felhasználási feltételeinek főbb elemeire. A szabályozás és a konkrét alkalmazásoknál megjelenő általános felhasználási feltételek kulcsfontosságú szerepet játszanak a szabályozási megfelelőség (compliance) biztosításában. Jelen tanulmány célja kettős, egyrészt be kívánja mutatni majd elemezni az uniós mesterséges intelligencia szabályozás kialakításának folyamatát, másrészt kísérletet tesz arra, hogy tudományos és jogi alapokon nyugvó ajánlást fogalmazzon meg az MI-alkalmazások általános felhasználási feltételeire vonatkozóan.

Kulcsszavak

mesterséges intelligencia szabályozás, Európai Unió, MI általános felhasználási feltételek, compliance

[1] timea.antal0@gmail.com | ORCID: 0009-0006-7258-1715 | PhD student, Óbuda University | doktorandusz hallgató, Óbudai Egyetem

[2] szamado.roza@bgk.uni-obuda.hu | ORCID: 0009-0000-9684-335X | Assistant Professor, Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering | egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

The spread of artificial intelligence is an important driver of the digitization of the European economy. The importance of this topic is reflected in the fact that the European Commission has set key objectives in the areas of digital infrastructure, skills, business and government services, and has also identified performance indicators that will enable the measurement of progress towards the 2030 goals of the digital decade in the Digital Decade Program [1]. According to the program's 2025 report [2] by 2025, the artificial intelligence revolution will gain further momentum due to breakthroughs in fundamental technologies, as they transform the boundaries of innovation, redefine competitiveness, and radically change people's everyday lives. Employees are already using artificial intelligence tools to increase productivity, simplifying work tasks and supporting decision-making processes. At the same time, however, new potential risks and challenges have emerged with the use of artificial intelligence.

The European Union Agency for Cybersecurity (ENISA) ranked artificial intelligence ninth among the ten factors posing the greatest potential threat to society in its 2024 March report [3]. This may rightly undermine people's initial trust. The use of artificial intelligence applications from a compliance perspective can be aided by a recommendation on general terms of use. The topic of this article is therefore timely and has practical benefits in this regard.

METHODOLOGY

During the research, I analyzed eleven publicly available documents (strategies, recommendations, guidelines, statements, regulations) related to artificial intelligence in the European Union. The methodology of the study was qualitative document analysis, which enabled the systematic processing and comparison of the content of the documents and the identification of structural patterns. The time frame for the selection of documents was 2017–2025. I examined only documents directly related to the topic. The analysis for the development of the regulatory map was based on the definition of objectives and principles, the development of a legal and ethical framework, and the guarantee of security. The artificial intelligence regulatory map formed the basis for the preparation of the recommendation on artificial intelligence.

EUROPEAN UNION ARTIFICIAL INTELLIGENCE REGULATORY MAP

The European Union has been working on developing regulations for artificial intelligence for years. The main reason for these efforts is that the EU recognizes the importance of AI, which it primarily associates with economic development. Since 2017, numerous recommendations, strategies, guidelines, and statements have been issued on this subject. It took seven years for the EU's regulatory framework to come into force. The main focus of the regulations is on defining basic principles, developing a legal and ethical framework, and guaranteeing safety by minimizing risks:

- Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy [4];

- European Parliament Report 27.1.2017 with recommendations to the Commission on Civil Law Rules on Robotics [5];
- The European Council EUCO 14/17. conclusions [6];
- EU Declaration on Cooperation on Artificial Intelligence [7];
- Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe [8];
- High-Level Expert Group on Artificial Intelligence - Ethical Guidelines for Trustworthy Artificial Intelligence [9];
- Digital Europe Strategy [10];
- Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence [11];
- White Paper On Artificial Intelligence [12];
- Artificial Intelligence Act [13];
- Artificial Intelligence Code of Practice [14].

The EU primarily associates AI with economic development and the strengthening of technological and industrial capacities (Digital Europe Strategy, Artificial Intelligence for Europe, Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence), i.e. the strategic idea that digitization will primarily determine the future of industry has come to the fore, and therefore views AI as a tool that contributes to the integration of intelligent technologies into industrial processes, thereby expanding the range of service elements (Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy).

The specific definition of AI is as follows: artificial intelligence refers to a system that is capable of intelligent behavior and examines its environment in order to achieve specific goals, then—with a certain degree of autonomy—takes action. (Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe) [15].

Although the current regulations only define general principles, they emphasise the importance of developing ethical and legal frameworks (EU Declaration on Cooperation on Artificial Intelligence, Recommendations to the Commission on Civil Law Rules on Robotics). According to the statement, building on the fundamental rights and values of the EU, the main objective of Member States should be to develop continuous cooperation and common thinking. It also highlights the importance of measures to support small and medium-sized enterprises and innovative start-ups operating in the robotics sector, creating new market segments or using robots. With regard to ethical principles, it emphasises risk analysis and proposes the development of a clear, strict and authoritative ethical framework for the development, design, manufacture, use and modification of robots (Recommendations to the Commission on Civil Law Rules on Robotics). Another significant achievement of the Recommendation is that it makes charter-like proposals: it precisely defines the code of conduct for robotics engineers, i.e. the rules to be used when examining robotics protocols, the rules to be applied by research ethics committees, and sample licences for designers and users.

The European Council has stated that a European model for artificial intelligence must also be developed: among other things, the establishment of a forward-looking regulatory framework, the creation of an unified regulatory framework for cyber security, and swift action to respond to emerging trends are essential for the successful development of the Digital Europe Programme (The European Council EUCO 14/17. conclusions).

The EU has recognised the need to prepare for the socio-economic changes resulting from artificial intelligence and considers it important to ensure an appropriate ethical and legal framework based on the values of the Union and in line with the EU Charter of Fundamental Rights. It has stated that it is necessary to develop draft ethical guidelines on artificial intelligence, while also analysing the adequacy of certain existing rules on safety and civil liability issues. The experts also recognised the importance of ideas that have emerged in relation to the modernisation of the legal frameworks for product liability and data protection (Artificial Intelligence for Europe).

The EU considers trustworthiness to be a key factor (Ethical Guidelines for Trustworthy Artificial Intelligence), and has therefore set out the basic elements of trustworthy artificial intelligence, which must be fulfilled throughout the entire life cycle of the system.

- legality, i.e. compliance with applicable legal regulations;
- ethics, i.e. ensuring compliance with ethical principles;
- ensuring technical and social stability.

The ethical guidelines were formulated to promote compliance with ethical principles based on fundamental rights (respect for human autonomy, prevention of harm, fairness, explainability). The guidelines define seven key requirements that a reliable artificial intelligence system must meet:

- Human agency and oversight
- Technical stability and security
- Data protection and data management
- Transparency
- Diversity, non-discrimination and fairness
- Social and environmental well-being
- Accountability.

These requirements undergo continuous technical and non-technical testing processes to filter out operational deficiencies in order to verify their necessity and effectiveness.

The Digital Europe Strategy has defined artificial intelligence as a specific, unique objective in Article 5. The objective of artificial intelligence is to achieve the following operational objectives:

- building and strengthening the basic capacities of artificial intelligence in the Union, including data sources and algorithm libraries that comply with data protection legislation;
- ensuring access to such capabilities for all businesses and public administrations;
- strengthening and networking existing artificial intelligence testing and experimentation facilities in Member States.

White Paper On Artificial Intelligence [12]: The EU aims to create a legal environment that promotes innovation and reduces risks. The White Paper is the first document to explicitly define a possible legal framework for the development and application of artificial intelligence. The book emphasises that, as a general rule, EU legislation remains fully applicable regardless of the involvement of AI. However, it is necessary to bear in mind that it is advisable to strictly manage the risks arising from artificial intelligence: it may even be necessary to adjust certain legal instruments. In this regard, the basic principle is that the new regulatory framework for artificial intelligence must be effective and safe, which can only be achieved through a risk-based approach. According to the Commission's position, an AI application should, as a general rule, be considered high-risk if it meets the following two cumulative conditions:

- It is used in a sector where, given the nature of the activities typically carried out, significant risks can be expected.
- The AI application is used in the sector in a way that could cause significant risks.

The White Paper also set out the main elements of the requirements for high-risk AI applications:

- data used to train systems;
- data and record retention;
- communication;
- stability and accuracy;
- human oversight;
- specific requirements for certain specific AI applications.

In order to verify and ensure compliance with the requirements, an objective ex ante conformity assessment is necessary, which may include testing, inspection or certification procedures. Conformity assessment would be mandatory for all operators: monitoring by national authorities and effective judicial redress mechanisms would also be necessary.

The content of the White Paper had a fundamental influence on the drafting of the Artificial Intelligence Act.

It is clear, therefore, that the AI Act is a significant milestone in the regulation of artificial intelligence. It establishes a complex, risk-based regulatory environment and allows for fines of up to 6% of global turnover. Although the regulation does not define the concept of artificial intelligence, it does define what an AI system is and what the basic operating requirements are for systems based on such technology. The legislation also sets out its specific objectives, as well as the expected results and performance indicators arising from its application. It is worth examining the data that make up the performance indicators in advance in order to track changes as accurately as possible. I see the essence of the risk management system detailed in Article 9 as following the plan-do-check-act logic in order to minimize and prevent risks. In other words, professionals first plan what needs to be done, then carry out the task, check the results, and finally intervene in the process to make the work more efficient next time; they do this over and over again, monitoring the entire process each time. The risk management system is an iterative process that runs continuously throughout the entire life cycle of a high-risk AI system and requires regular and systematic updating of data.

Article 53 of the Regulation sets out the practical obligations for providers of general-purpose AI models. It emphasizes that technical documentation for the model must be prepared and kept up to date, and that information and documentation must be developed, kept up to date, and made available to providers of AI systems who wish to incorporate the general-purpose AI model into their AI systems. A policy for compliance with EU law on copyright and related rights is needed, as well as a sufficiently detailed summary, and it is also essential to publish educational material used to teach the functioning of the general-purpose AI model.

Article 54 of the Regulation serves to ensure security and transparency, as service providers established in third countries must appoint a representative based in the Union by written authorization prior to placing a general-purpose AI system on the Union market.

Article 55 imposes additional obligations on providers of general-purpose AI models that pose a systemic risk. Accordingly, model evaluation must be carried out in accordance with standardised protocols and tools that reflect the current state of the art, and the EU and systemic risks arising from the development, marketing or use of general-purpose AI models that may pose systemic risk must be assessed and mitigated. Serious and unexpected events must be monitored, documented and reported without undue delay to the AI Agency and, where appropriate, to the competent national authorities, so that the relevant information on corrective measures taken to address them can be analyzed by the competent bodies in order to ensure an appropriate level of cybersecurity protection.

At the level of EU regulation, Article 56 also contains practical regulations, according to which practical codes must be developed for the proper practical application of the regulation. This led to the creation of the MI general practical code, which will apply from the 2nd August 2025. Table 1 shows the relationship between this code of practice and the AI Regulation and also contains a summary of its content relevant to the research.

Artificial Intelligence Code of Practice	AI Act	Content
Transparency chapter	Article 53	It provides a practical template for developing data, measurements, and methodologies related to the content of the documentation. Its main elements are: general information; model properties; distribution methods and licenses; usage parameters; training process; information on data used for training, testing, and validation; computing resources (during training); energy consumption (during training and application).

Artificial Intelligence Code of Practice	AI Act	Content
Copyrifght chapter	Article 53	Defines a 5-point action plan for the protection of copyright. It is necessary to develop, update, and implement a copyright policy. When searching the World Wide Web, only legally accessible, copyright-protected content may be reproduced and used. When mapping the World Wide Web, copyright restrictions must be identified and respected. The risk of results that infringe copyright must be reduced. A contact person must be designated and a mechanism for submitting complaints must be provided.
Safety and security chapter	Article 55	This chapter provides the most accurate and detailed practical recommendations for managing systemic risks by defining ten commitments: • Developing, implementing, and renewing a security and protection framework. • dentifying system-level risks within a structured process by developing system-level risk scenarios. • Developing a system-level risk analysis. • Defining system-level risk acceptance. • Defining security measures. • Defining protection measures. • Developing security and protection model reports. • Clearly dividing system-level risk responsibility. • Reporting serious incidents. Defining additional documentation tasks and ensuring transparency.

1. Table: The relationship between the Artificial Intelligence Code of Practice – AI Act and the summary of its content (Source: own edited)

Alongside the practical advancement of artificial intelligence, the practical application of legal regulations is an essential task: without regulations, data, processes, methodologies, and measurements, artificial intelligence is a one-armed giant. Based on the above, it is clear that the role of AI system regulation is becoming increasingly important for a number of reasons.

Since the use of artificial intelligence is associated with increased security risks, the application of practical tools to respond to these risks plays a key role. EU AI regulations focus on security, human-centeredness, and sustainability. For the time being, EU documents mainly provide theoretical frameworks for practical work. The EU's increasingly comprehensive legal regulations show that decision-makers recognize the importance of AI:

therefore, practical guidelines have followed strategies and statements, and risk management has also taken on a more prominent role. The following key aspects have appeared in EU AI regulations and documents:

- Emphasis on economic development;
- Consideration of ethical and legal frameworks;
- Definition of terms;
- Identification and management of risks;
- Identification of processes;
- Ensuring transparency;
- Establishment of security and protection.

RECOMMENDATION ON THE TERMS OF USE FOR ARTIFICIAL INTELLIGENCE APPLICATIONS

The legal, ethical, risk, and security regulation of artificial intelligence applications is ongoing. There is a need to ensure the accountable and appropriate functioning of artificial intelligence systems, which requires regulated processes, legal regulations, and enforcement tools. Regulated processes must be designed, applicable, and monitored to maintain security. Processes and appropriate regulations can ensure that risks become identifiable and manageable.

A sufficiently detailed and accurate set of terms of use that can be understood by users enables the safer use of artificial intelligence applications. Below, I set out 14 recommendations concerning the main content elements:

- Definitions - Precise definition of data related to the AI application and its use (Article 3 of the EU AI Act).
- Service provider contact details: name, registered office, website; customer service contact details.
- Service description and changes - Presentation of the operating environment, exclusion of errors, definition of prohibited uses (Articles 5-6 of the EU AI Act). Presentation of model characteristics, distribution methods and licenses, usage parameters.
- Application availability - Determination of availability.
- Data processing conditions - Ensuring compliance with GDPR [16], data retention and deletion rules [17].
- User rights and obligations - Access, modification, correction, deletion, data portability [16].
- Security measures, protection rules - Cybersecurity standards (GDPR Article 32 [16]; NIS2 Article 21 [18]).
- Fees - Determination of the basic fee, other fees payable based on usage, and payment terms.
- Copyright, intellectual property rights - Copyright status of content generated by AI.
- Liability regulation - Human supervision of high-risk decisions, limitation of liability.

- Contract conclusion, changes, and notification - Acceptance of terms of use, rules for modification, and notification obligations.
- Jurisdiction and applicable law - Definition of national and international law.
- Ethical and transparency supplements - Definition of detailed documentation, training process, information on data used for training, testing and validation.
- Customer relations, complaint handling - Complaint handling and process, fee complaints.

In the interests of transparency, I recommend creating a table of contents and clearly indicating the date of entry into force. I recommend that the general terms and conditions be published on the service provider's website in an easily accessible, downloadable, storable, displayable, and printable format, with searchability within the text.

CONCLUSION

The practical application of EU regulations on artificial intelligence could be ensured by detailed and compliance-oriented general terms of use. Legal compliance, protection, security, and ethical responsibility also need to be regulated within the framework of general terms of use for AI. Transparent and detailed contractual terms and conditions can contribute to building trust, transparency, and minimizing regulatory risks. In the future, it will therefore be worth examining what regulatory conditions are included in the general terms and conditions of use of ChatGPT, DeepL, Microsoft Copilot, and other similar services in practice.

REFERENCES

[1] European Parliament, European Council, Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. In: https://net.jogtar.hu/jogszabaly?docid=a22h2481.eup
[2] European Commission, „State of the Digital Decade 2025 report ”. In: https://digital-strategy.ec.europa.eu/hu/library/state-digital-decade-2025-report
[3] European Union Agency for Cybersecurity (ENISA), „ENISA Foresight Cybersecurity threats for 2030 - UPDATE.”, 2024. In: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-full-report_en_0.pdf
[4] European Commission, Investing in a smart, innovative and sustainable Industry - A renewed EU Industrial Policy Strategy. COM/2017/0479 final. In: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52017DC0479
[5] European Parliament, Report 27.1.2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL). In: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017IP0051&from=EN
[6] Eurpean Council, „European Council EUCO 14/17. conclusions”. In: https://www.consilium.europa.eu/media/21607/19-euco-final-conclusions-hu.pdf
[7] European Commission, „EU Declaration on Cooperation on Artificial Intelligence”. In: https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence

[8] European Commission, „Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe”. 2018. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

[9] High-Level Expert Group on Artificial Intelligence, Ethical Guidelines for Trustworthy Artificial Intelligence . In: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[10] European Commission, Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM(2018) 434 final. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN

[11] Europena Parliament, „Artificial intelligence - Conclusions on the coordinated plan on artificial intelligence 6177/19”. In: https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf

[12] European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust. In: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52020DC0065

[13] European Parliament,European Council, 2024/1689 12.7.2024 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). In: https://net.jogtar.hu/jogszabaly?docid=a2401689.eup

[14] European Commission, „Az MI általános célú gyakorlati kódexe”. 2025. In: https://digital-strategy.ec.europa.eu/hu/policies/contents-code-gpai

[15] European Commission, „Communication from the Commission to European Parliament, European Council, the Council, the European Economic and Social Committee, the Committee of the Regions on Artificial Intelligence for Europe”. 2018. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

[16] European Parliament, European Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In: https://net.jogtar.hu/jogszabaly?docid=a1600679.eup

[17] P. Voigt és A. Von Dem Bussche, The EU General Data Protection Regulation (GDPR). Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-57959-7.

[18] European Parliament, European Council, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). In: https://net.jogtar.hu/jogszabaly?docid=a22i2555.eup

DOI: https://doi.org/10.12700/btsz.2025.7.4.177

COMPARATIVE ANALYSIS OF LLM ARCHITECTURES IN SAFETY-CRITICAL SYSTEMS: DEPLOYMENT MODELS, SOVEREIGNTY, AND VULNERABILITY

LLM ARCHITEKTÚRÁK ÖSSZEHASONLÍTÓ ELEMZÉSE BIZTONSÁGKRITIKUS RENDSZEREKBEN: TELEPÍTÉSI MODELLEK, SZUVERENITÁS ÉS SEBEZHETŐSÉG

BEDNÁRIK Boldizsár[1] – GOGOLÁK László[2]

Abstract

This study examines the possibilities and risks of applying large language models (LLM) in safety-critical systems and demonstrates how LLMs can be integrated into decision making process (support) and automated systems. It provides a detailed comparison of on-premise, cloud-based, and hybrid deployment models, with particular focus on data sovereignty, information security, and operational flexibility. Based on OWASP and DHS guidelines, the paper outlines key vulnerabilities. It also analyzes the relevance of the NIS2 Directive, and the AI Act framework. To reduce risks, it highlights the importance of the ALARP principle, human oversight, validation mechanisms, multi-layered protection, and security-conscious training. The study's aim is to support a sustainable balance between safety and innovation.

Keywords

LLM, Data Sovereignty, Risk Management, Artificial Intelligence (AI), Data Security

Absztrakt

Ez a tanulmány a nagy nyelvi modellek (LLM) biztonságkritikus rendszerekben történő alkalmazásának lehetőségeit és kockázatait elemzi, valamint bemutatja, hogyan épülhetnek be az LLM-ek a döntéstámogató és automatizált rendszerekbe. Részletesen összehasonlítja a lokális, felhőalapú és hibrid telepítési modelleket, különös tekintettel az adatszuverenitásra, adatbiztonságra és működési rugalmasságra. Az OWASP és a DHS irányelvei alapján bemutatásra kerülnek a legfontosabb sebezhetőségek.A tanulmány elemzi a NIS2 irányelv és az AI Act előírásainak relevanciáját. A kockázatok csökkentésére az ALARP-elv, valamint emberi felügyelet, validáció, több rétegű védelem és biztonságtudatos oktatás kerül kiemelésre. A tanulmány célja a biztonság és innováció közötti fenntartható egyensúly elősegítése.

Kulcsszavak

LLM, adatszuverenitás, kockázatkezelés, Mesterséges Intelligencia (MI), adatbiztonság

[1] bednarik.boldizsar@uni-obuda.hu | ORCID: 0009-0005-5198-1210 | PhD Student, Doctoral School on Safety and Security Sciences, Óbuda University| Doktorandusz, Biztonságtudományi Doktori Iskola, Óbudai Egyetem

[2] gogolak@mk.u-szeged.hu |ORCID: 0000-0002-6653-3534 | Associate Professor, Department of Mechatronics and Automation, Faculty of Engineering, University of Szeged| Főiskolai Docens, Mechatronikai és Automatizálási Tanszék, Mérnöki Kar, Szegedi Tudományegyetem

BEVEZETÉS

A nagy nyelvi modellek (LLM-ek) rohamos fejlődése - mint megannyi más területen - új távlatokat nyitott a biztonságkritikus rendszerekben is - az energetikától és közlekedéstől a védelmi szférán át az egészségügyig. E rendszerekben az LLM-ek bevezetése egyszerre kecsegtet forradalmi előnyökkel és vet fel komoly biztonsági és etikai kihívásokat.

Az LLM-ek alkalmazása ezen a területen azért vált központi kérdéssé, mert segítségükkel nagy adatmennyiségek gyorsabban és könnyebben elemezhetők, ezzel lehetővé válhat az esetleges problémák előrejelzése, és az egyszerűbb - megközelítőleg valósidejű - automatizált döntéshozatal. Egy másik ok, hogy az LLM-ek képesek tanulni és összefüggéseket felfedezni olyan összetett rendszerekben és adathalmazokban, ahol az emberi szakértők kapacitása véges. Mindez különösen vonzó az olyan kritikus infrastruktúráknál, ahol az üzemzavar vagy támadás emberéleteket veszélyeztethet, jelentős anyagi-, személyi kárt okozhat, vagy nemzetbiztonsági kockázattal jár.

Ugyanakkor az LLM-ek integrálása biztonságkritikus környezetben nem pusztán technikai kérdés. A biztonságtudomány maga is multidiszciplináris terület: magában foglalja a műszaki, társadalomtudományi, jogi és etikai dimenziókat egyaránt. A biztonság fogalma komplex és multidimenzionális, több tudományág metszéspontjában áll, ami megnehezíti az egységes megközelítést [1]. Ez a mi esetünkben azt jelenti, hogy amikor LLM-alapú mesterséges intelligenciát építünk be például egy atomerőmű vezérlőrendszerébe vagy egy autonóm jármű irányításába, akkor nem elég csupán a gépi tanulás technikai teljesítményét néznünk. Figyelembe kell venni a humán tényezőt (pl. a kezelők bizalmát a rendszer iránt), a jogszabályi megfelelést (pl. adatvédelmi előírásokat), az etikai normákat (pl. dönthet-e gép emberi életet érintő kérdésben), és nem utolsó sorban a szervezeti és nemzeti szuverenitás kérdését is.

Az LLM-ek biztonságkritikus területen történő alkalmazása így valódi multidiszciplináris kihívás, amely érinti a különböző tudományterületek szempontjait. Ezt szemelőtt tartva tanulmányunk célja, hogy megpróbáljon átfogó képet adni az LLM-ek biztonságkritikus rendszerekben való alkalmazásáról, különös tekintettel a lehetséges telepítési modellekre és feltárja az ezzel járó dilemmákat.

TELEPÍTÉSI MODELLEK ÖSSZEHASONLÍTÁSA

Az LLM-ek integrációja során alapvető kérdés, hogy milyen telepítési modellt (deployment) válasszunk: házon belüli (on-premise), felhőalapú (cloud) vagy hibrid megoldást. Ezek a modellek jelentősen eltérnek az adatkezelés, hozzáférés, szuverenitás és biztonság szempontjából, ezért fontos a tudatos mérlegelés.

Az **On-premise (helyszíni) telepítés** alkalmazása esetében az LLM rendszert és az adatait teljes mértékben a saját, helyi infrastruktúrán futtatjuk. Ennek nagy előnye a teljes felügyelet az adataink felett: az érzékeny adatokat nem kell kiadni külső szolgáltatónak, így jobban biztosítható a megfelelés a szigorú iparági vagy nemzeti előírásoknak. Katonai vagy kormányzati alkalmazásoknál például elsődleges szempont, hogy az adat a rendszer határain belül maradjon. A NATO NCIA Technology Strategy 2030 is kiemeli, hogy a NATO műveleti környezetében a nyilvános, privát, hibrid, szuverén és edge felhőmegoldások egyaránt mérlegelendők a különböző biztonsági besorolású adatok és

szolgáltatások esetén [2]. Az on-premise LLM tehát maximális kontrollt nyújt, ugyanakkor hátránya a magas iniciális költség és erőforrásigény: a nagy modell futtatásához szükséges hardver-infrastruktúrát ki kell építeni és karban kell tartani, a modell fejlesztését és frissítését saját erőből kell megoldani. Ez pénzben és időben is jelentős terhet róhat a szervezetre. Ráadásul skálázhatósági korlátok is lehetnek: a felhasználói igények gyors növekedése esetén nehézkes lehet lépést tartani a szükséges szerverkapacitás bővítésével.

Az LLM **Cloud (felhőalapú) telepítésénél** a szolgáltatást egy felhőszolgáltató infrastruktúráját használva vesszük igénybe (pl. nagy tech cégek AI platformjain). Előnye a gyors fejlesztési és bevezetési ciklus: a felhőben általában azonnal rendelkezésre áll a szükséges számítási kapacitás, valamint hozzáférhetők a legkorszerűbb pre-trainelt nyelvi modellek. Ezáltal a fejlesztés felgyorsul, és a szolgáltatás rugalmasan skálázható (nagy terhelés esetén automatikusan több erőforrást kapunk). A felhőszolgáltatók gyakran erős beépített biztonsági mechanizmusokat kínálnak, folyamatos frissítésekkel, és nagyfokú redundanciával üzemeltetik rendszereiket. Ugyanakkor a felhőmodell jelentős adatvédelmi kockázatot hordoz: az adatok kikerülnek a saját infrastruktúránkból, ami aggályos lehet pl. személyes vagy érzékeny adatok esetén. A felhőszolgáltatóval szemben bizalomra van szükség - nem mindegy, hogy a cég mely ország joghatósága alá tartozik, és hogyan garantálja az adatszuverenitást. Gyakori elvárás, hogy szuverén felhő opció álljon rendelkezésre, ahol biztosított az adatok országon vagy szövetségi kereteken belüli tárolása és kezelése [3]. A NATO pl. az Oracle által kínált szuverén felhőmegoldásokra való áttérés célja, hogy a legújabb felhő- és AI-innovációkat a kritikus adatok biztonságának feláldozása nélkül vehessék igénybe [3]. Meg kell még említeni a felhőmodellel kapcsolatos másik kockázatot is, ami a szolgáltatótól való függés: a vendor lock-in és a szolgáltatás kimaradása (downtime) is veszélyeztetheti a működést. Továbbá egy nyilvános felhőben futó LLM esetén számolni kell azzal is, hogy több-bérlős környezetben fut a rendszer, potenciálisan megosztva erőforrásokat ismeretlen ügyfelekkel, ami kifinomult támadások (pl. oldalcsatornás támadások) kockázatát felvetheti [4].

A **Hibrid** megközelítés igyekszik ötvözni az on-premise és felhő előnyeit. A kritikus vagy érzékeny adatokat és funkciókat házon belül tartja, míg a kevésbé érzékeny feladatokat, valamint a csúcsterhelés esetén szükséges többletkapacitást a felhőbe delegálja. Például egy egészségügyi alkalmazásnál a páciensek személyes adatait helyben tárolhatják és kezelhetik, míg az általános nyelvi elemző modellt felhőben futtatják. A NATO stratégiában is megjelenik a multi-cloud integráció igénye, melynek célja, hogy egységes szolgáltatásként lehessen kezelni a különböző (privát és publikus) felhők erőforrásait [2].

Összességében a telepítési modell megválasztása szorosan összefügg a szuverenitás kérdésével. Biztonságkritikus rendszerekben sokszor a nemzeti/üzleti szuverenitás megőrzése az elsődleges szempont, ami az on-premise vagy szuverén felhős megoldások felé billenti a mérleget. Azonban, ahol gyors innovációra és skálázhatóságra van szükség, ott a felhő előnyei (sebesség, rugalmasság, költséghatékonyság) előtérbe kerülnek, persze csak abban az esetben, ha megfelelő szerződéses és technikai garanciákkal kezelik az adatvédelmi kockázatokat. A következőkben áttekintjük az ilyen rendszerekben rejlő főbb előnyöket és kockázatokat.

ELŐNYÖK ÉS KOCKÁZATOK

Egy LLM alkalmazása biztonságkritikus rendszerben számos előnyt kínál: képes komplex mintázatokat felismerni az adatokban, szabályalapú rendszerekkel nem detektálható anomáliákra figyelmeztetni, előre jelezni várható eseményeket (pl. berendezéshibát vagy kibertámadást), sőt bizonyos mértékű autonóm döntést is hozhat rutinszerű helyzetekben [5]. Ezáltal növelheti a rendszer hatékonyságát (gyorsabb reakcióidő, 24/7 rendelkezésre álló "mesterséges szakértő"), és tehermentesítheti az emberi operátorokat a monoton vagy túl sok adatot igénylő feladatok alól. Például egy energiatermelő hálózatban az LLM képes lehet a szenzoradatokból és üzemzavari jegyzőkönyvekből tanulva előre jelezni egy transzformátor meghibásodását, megelőzve ezzel a nagyobb balesetet vagy kiesést [6]. A kórházi környezetben egy LLM segíthet gyorsan áttekinteni az orvosi protokollokat és javaslatot tenni a sürgősségi ellátás priorizálására, amikor nagyszámú sérült érkezik. Ezek az előnyök - a gyorsaság, skálázhatóság, tudás-integráció - teszik vonzóvá az LLM-eket a kritikus alkalmazásokban.

De beszélni kell a másik oldalról is: az LLM-ek bevezetése új kockázatokat és sebezhetőségeket hoz a rendszerbe, amelyeket nem szabad alábecsülni. A DHS (Amerikai Belbiztonsági Minisztérium) 2024-es AI-CI iránymutatásai három fő kockázati kategóriát különböztetnek meg a kritikus infrastruktúrák kapcsán [7]:

1. Az AI által végrehajtott támadások - amikor a támadók magukat az LLM-eket használják fel fegyverként, például a kibertámadások automatizálására vagy a félrevezető álhírek tömeges generálására
2. Az AI rendszerek elleni támadások - amikor magát az LLM-alapú rendszert veszik célba, például adverszáriális (megtévesztő) módszerekkel manipulálják a bemeneteket (evasion támadások) vagy adatmérgezéssel (data poisoning) rontják le a modell teljesítményét [7] [8]
3. Az AI tervezési hibáiból fakadó problémák - ide tartoznak a rendszer belső gyengeségei, úgymint a túlzott autonómia, a törékenység (brittleness - amikor váratlan bemenetre kiszámíthatatlanul reagál a modell) vagy az értelmezhetetlenség, ami miatt az AI döntéseit nem lehet megmagyarázni [7]

Ezek a kategóriák rávilágítanak, hogy az LLM-ek kapcsán nem csak a külső rosszindulatú szereplőktől kell tartanunk, hanem a rendszer belső hiányosságaitól is.

Fontos még az etikai és jogi kockázatok figyelembevétele. Egy LLM által hozott döntés diszkriminatív vagy igazságtalan lehet, ha a modell torz adatokon tanult - például az egészségügyben előfordulhat, hogy egy AI rendszer alulértékeli egyes kisebbségi csoportok rizikófaktorait a tanulási adatok hiányosságai miatt. A felelősség kérdése is felmerül: ki a felelős, ha egy LLM hibás javaslata kárt okoz? Jogi szempontból az EU friss AI Act (2024/1689) rendelete kockázati szintek alapján szabályozza az AI rendszereket, és a magas kockázatú alkalmazásokra (ahová a biztonságkritikus felhasználások is tartoznak) szigorú átláthatósági, biztonsági és megfelelőségi követelményeket ír elő [9]. Hasonlóképpen, az EU NIS2 irányelv (Directive (EU) 2022/2555) kibővíti a létfontosságú ágazatok kibervédelmi előírásait, kötelező kockázatkezelési gyakorlatokat és incidens-jelentési rendszert vezet be - ez közvetett módon az AI-alapú komponensekre is vonatkozik, hiszen azokat is integrálni kell a teljes kockázatmenedzsment folyamataiba [10]. Végül, a szuverenitási aggályok is ide tartoznak: például, ha egy kritikus infrastruktúra külső,

külföldi AI szolgáltatást használ, az adott ország kiszolgáltatottá válhat egy idegen entitásnak, ami geopolitikai kockázatot hordozhat.

Összefoglalva, az LLM-ek alkalmazása a biztonságkritikus rendszerekben egyszerre ígéretes és kockázatos: a mérleg egyik serpenyőjében az intelligens automatizáció és hatékonyságnövelés áll, a másikban pedig az új támadási felületek, tervezési hibák és szabályozási dilemmák. A következő szakaszban egy összehasonlító mátrix segítségével szemléltetjük, hogy különböző alkalmazási területeken hogyan viszonyul egymáshoz a várható előny és a kockázati szint.

ALKALMAZÁSI TERÜLETEK ÖSSZEHASONLÍTÁSA A FELMERÜLŐ KOCKÁZAT ÉS NYÚJTOTT ELŐNYÖK SZEMPONTJÁBÓL

Az 1. táblázat hat lehetséges alkalmazási területen szemlélteti az LLM-ek biztonságkritikus használatának kockázati szintjét (alacsony / közepes / magas) és a várható előnyt (alacsony / közepes / magas). Minden cellában rövid értékelés foglalja össze a kockázat-előny mérlegét, indokolva a besorolást. Az értékelések általános, útmutatás jellegűek. Jól látszik az AI alkalmazás biztonság/előny kettős természete.

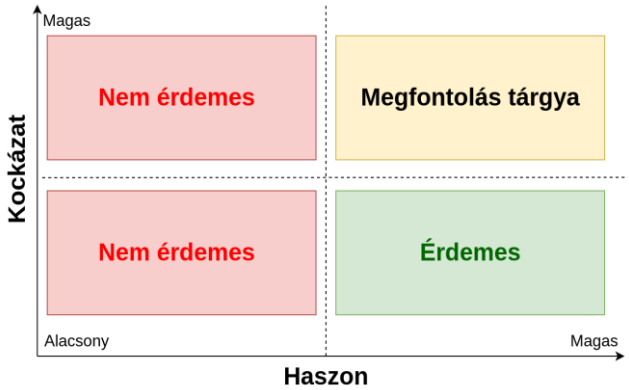
Alkalmazási terület	Fő előny	Fő kockázat	Kockázati szint	Potenciális előny
Kritikus infrastruktúra üzemeltetés	**Gyors hibadetektálás, prediktív karbantartás**	**Automatizált döntések hibás működése, modellmanipuláció**	Magas	Közepes-magas
Egészségügyi döntéstámogatás	**Diagnosztikai pontosság növelése, adminisztrációs teher csökkentése**	**Életet veszélyeztető hibás javaslat, adatvédelmi incidens**	Nagyon magas	Magas
Közigazgatás és e-kormányzat	**Ügyintézés gyorsítása, emberi erőforrás tehermentesítése**	**Adatszivárgás, torzított döntéstámogatás**	Közepes	Magas
Oktatás és tudásmenedzsment	**Személyre szabott tanulás, tartalomgenerálás**	**Félrevezető információ, túlzott automatizálás**	Alacsony-közepes	Közepes
Pénzügyi szektor / FinTech	**Csalásdetektálás, automatizált kockázatelemzés**	**Adatszivárgás, modell-torzítás, megfelelőségi kockázat**	Magas	Magas

Vállalati támogatórendszerek (HR, marketing, ügyfélszolgálat)	**Produktivitásnövelés, gyors információáramlás**	**Bizalmas adatok kiszivárgása, torz eredmények**	Alacsony-közepes	Magas

1. táblázat: Egyes alkalmazási területek becsült haszna és kockázata a különböző telepítési modellek (on-premise, cloud, hibrid) függvényében

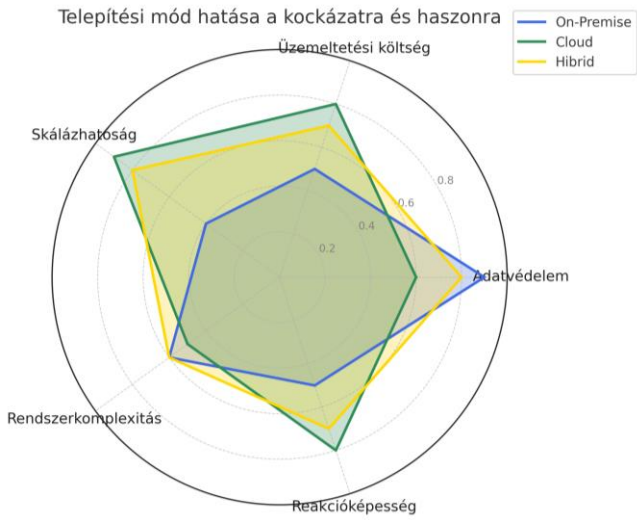
A döntéshozatal egyik fő eleme a kockázat - haszon egyensúly megfelelő értékelése. Az ALARP (As Low As Reasonably Practicable) elv szerint a kockázatot addig kell csökkenteni, amíg az ésszerűen megvalósítható - azaz amíg a kockázatcsökkentés költségei és erőforrásigénye arányban állnak a várható haszonnal [11].

A 1. ábra szemlélteti hogy mely zónákban tekinthető az alkalmazás indokoltnak, útmutatóként a döntéshozatalhoz.



1. ábra: A kockázat és a haszon viszonya négy döntési kategóriában.

A telepítési modell kiválasztása döntő szerepet játszik abban, hogy az AI-rendszer milyen kockázat-haszon arányt képvisel. A cloud környezetek magasabb hasznot kínálnak a skálázhatóság és az innováció gyors elérhetősége révén, ugyanakkor növelik az adatvédelmi és szolgáltató-függőségi kockázatokat. Az on-premise rendszerek ezzel szemben fokozott biztonságot és kontrollt adnak, de nagyobb beruházási és üzemeltetési költségekkel járnak. A hibrid megközelítés az ALARP-elvnek megfelelő kompromisszumot jelentheti, ahol a kockázat és a haszon egyensúlyban tartható. A 2. ábra szemlélteti ezeket az összefüggéseket.



2. ábra: A különböző telepítési modellek eltérő mértékben befolyásolják a mesterséges intelligencia rendszerek kockázati és haszon-profilját.

AJÁNLÁSOK, MEGELŐZÉS ÉS KÁRENYHÍTÉS

A fenti elemzés alapján kirajzolódik, hogy az LLM-ek biztonságkritikus alkalmazása során az egyik kulcskérdés a kockázatok megfelelő csökkentése. Az ALARP-elv (As Low As Reasonably Practicable - amilyen alacsony szintre csak ésszerűen csökkenthető) alkalmazása megkerülhetetlen: törekedni kell arra, hogy minden azonosított kockázatot olyan alacsony szintre mérsékeljünk, amennyire az ésszerűen megvalósítható [11]. Ahogyan a biztonságtechnikában általános, el kell fogadnunk, hogy zéró kockázat nem létezik (fokozottan igaz ez a komplex AI-rendszerekre), de a fennmaradó kockázat soha nem haladhatja meg az elfogadható szintet. Ha egy további védelmi intézkedés már csak aránytalanul nagy ráfordítással lenne bevezethető a várható nyereséghez képest, akkor teljesül az ALARP kritérium [11]. Ezt az elvet követve az LLM-ek esetében is minden ésszerű biztonsági kontrollt implementálni kell, és csak azokról mondjunk le, amelyek költsége vagy komplexitása már nincs arányban a hozott biztonsági előnnyel. Tekintsünk át néhány ajánlást, bevált kárenyhítési javaslatot és gyakorlatot:

Többrétegű védelem alkalmazása

Az LLM-ek köré többszintű védelmi mechanizmusokat kell építeni (defense-in-depth). Egyetlen intézkedés sem véd minden ellen, de több, egymást kiegészítő kontroll kombinációja erős biztonsági hálót ad. Például: a rendszer inputját egy előszűrő modul ellenőrizze, mielőtt az LLM-hez jut (kiszűrve a nyilvánvalóan káros vagy injekciós próbálkozásokat); az LLM kimeneteit egy utóellenőrző modul vizsgálja, mielőtt a külvilág felé továbbléptetnénk (pl. ne generálhasson közvetlenül parancsot egy vezérlőrendszernek emberi jóváhagyás nélkül). Emellett gondoskodni kell a hálózati szintű védelemről (tűzfalak, behatolásészlelés), és az LLM-et futtató környezet izolációjáról (konténerezés, homokozó jellegű futtatás), hogy egy esetleges kompromittálás ne terjedhessen tovább a rendszerben.

Bemeneti és kimeneti validáció (valódiság-ellenőrzés)

Az LLM-ek sajátossága, hogy bármilyen utasítást követnek a promptban, hacsak nincsenek korlátok közé szorítva. Az OWASP útmutatók is hangsúlyozzák: a modellt kezeljük úgy, mintha egy külső felhasználó lenne - ne bízzunk vakon a generált válaszában [12]. Implementáljunk szigorú bemeneti (input) validációt: engedélyezett parancsok és formátumok listáját (allowlist) használva, és utasítsuk el vagy semlegesítsük (és naplózzuk!) a gyanús bemeneteket. Például egy LLM ne kaphasson olyan rendszerpromptot a felhasználótól, ami érzékeny információ kiadására vagy tiltott műveletre buzdítja. A kimeneteknél pedig alkalmazzunk kontextusfüggő kódolást és szűrést: például ha az LLM kódot vagy parancsot generál (pl. SQL lekérdezést, shell parancsot), azt csak megfelelő escaping/encoding után használjuk fel [12]. Egy webes megjelenítésnél pl. HTML kimenetet escape-elni kell, hogy megelőzzük az XSS támadást, még akkor is, ha azt az LLM "magától" írta. Soha ne futtassuk egy LLM kimenetét közvetlenül a rendszerben ellenőrzés nélkül (ne hívjunk meg eval-t a generált kódra, ne küldjük el nyers formában e-mailben stb.). Az ilyen validációs-szűrési lépések automatizálhatók és beépíthetők az alkalmazás logikájába.

Prompt injection elleni védelem

A prompt injection - amikor a támadó olyan bemenetet ad, amivel átveszi az irányítást a modell kimenete felett - az LLM-ek speciális Achilles-sarka. Ennek kivédésére kombinált módszerek szükségesek. Egyrészt használjunk statikus prompt sablonokat, amelyekből a felhasználó által beírható részt minimálisra szorítjuk, és nem engedjük felülírni a rendszer üzeneteket. Másrészt monitorozzuk a párbeszédeket automatizáltan: gyanús minták detektálására (pl. ha a felhasználó arra utasítja az LLM-et, hogy ne tartsa be a korábbi utasításokat, vagy adjon ki tiltott tartalmat). Megfelelő eszközökkel felismerhetők az ilyen injekciós kísérletek, és ilyenkor a rendszer adjon egy generikus választ vagy tagadja meg a kérést. Továbbá a figyelmeztető jelzések (pl. a modell hirtelen a rendszerprompt érzékeny részleteit akarja felfedni) indítsanak el egy incidenskezelési folyamatot. Nem utolsó sorban pedig tartsuk naprakészen a modellünket: az újabb LLM verziók tipikusan javítanak a biztonsági korlátokon, az ismert prompt injection trükkök ellen védettebbek. Amennyiben saját modellt használunk, rendszeresen finomhangolhatjuk ellenpéldákkal (adversarial training), hogy ellenállóbb legyen az ilyen támadási mintákra.

Emberi felügyelet és vészfunkciók

Bármilyen fejlett is legyen egy AI, biztonságkritikus rendszerekben nem szabad felügyelet nélkül hagyni. Elengedhetetlen egy olyan emberi felügyeleti mechanizmus, amely folyamatosan követi az LLM működését, és szükség esetén közbe tud lépni. Ez jelentheti azt, hogy az LLM döntései vagy ajánlásai csak emberi jóváhagyással válnak végrehajthatóvá (human-in-the-loop), vagy legalább azt, hogy egy operátor vissza tud vonni/ki tud kapcsolni egy AI által indított műveletet (pl. ha az AI tévesen egy rossz lépést javasolna, az ember felülbírálhatja). Különösen az autonómabb funkciók esetén legyen egy "vörös gomb" (kill switch), amivel az AI modul gyorsan leállítható, ha rendellenes működést produkál. A felügyelet része a monitoring: valós idejű naplózás és riasztások arról, hogy az LLM milyen döntéseket hoz, milyen bizalmas adatot kér vagy ad ki.

Biztonságtudatos tervezés és oktatás

Az LLM-ek biztonságos használata nem csak technikai kérdés, hanem emberi tényező is. Gondoskodni kell róla, hogy mindazok, akik a rendszert tervezik, üzemeltetik

vagy használják, megfelelő képzést kapjanak az AI sajátosságairól és kockázatairól. A fejlesztők számára szervezzünk biztonsági tréninget kifejezetten AI témában (pl. OWASP LLM Top 10 ismertetése, tipikus támadási vektorok bemutatása) [12]. Az üzemeltető csapat ismerje az LLM monitorozási eszközeit, tudja értelmezni a riasztásokat és legyen kész vészhelyzeti eljárásrend (pl. ha azt gyanítják, hogy az AI kompromittálódott, hogyan vegyék ki a rendszerből). A végfelhasználóknak - pl. egy erőmű vezérlőtermében dolgozó mérnököknek vagy kórházi orvosoknak - pedig oktatni kell, hogy mire képes és mire nem képes a bevezetett LLM-alapú asszisztens. Fontos, hogy megértsék: az AI által adott tanács nem szentírás, kritikusan kell kezelni. Tanítsuk meg nekik az alapvető „AI-higiéniát": ne adjanak be a rendszernek értelmetlen vagy rosszindulatú utasítást (hiszen ezzel ők maguk is előidézhetnek hibás működést), figyeljenek a rendszer szokatlan válaszaira, és jelentsék, ha valami gyanúsat tapasztalnak. A szervezeti biztonsági kultúra kiterjesztése az AI területére kulcsfontosságú - a biztonságtudatosság növelése az egyik leghatékonyabb, bár gyakran alulértékelt védelmi vonal [13].

Ezen ajánlások egy része már megjelent a nemzetközi szabványokban és ajánlásokban, más részüket a józan ész és tapasztalat diktálja. A lényeg az, hogy holisztikusan, a szervezet egészére kiterjedően kezeljük az LLM-ekből fakadó biztonsági kihívásokat - egyszerre fókuszálva a technológiára (secure coding, monitoring, hardening) és a szervezetre (irányítás, folyamatok, képzés) [13]. Így minimalizálhatjuk annak esélyét, hogy egy AI miatt következzen be súlyos incidens, illetve, ha mégis bekövetkezik, felkészülten, jól begyakorolt tervvel reagálhassunk.

KORLÁTOK ÉS TOVÁBBI KUTATÁS

A tanulmány elsősorban az LLM-ek biztonságkritikus környezetekben való alkalmazásának elméleti és tervezési szempontjaira összpontosít, tehát a bemutatott megközelítés elméleti keretet ad, de működésének gyakorlati ellenőrzése még nem történt meg, és nem tartalmaz konkrét (mennyiségi) kockázati mutatókat sem. A telepítési modellek összehasonlítása is jelenleg leíró jellegű, ahogy a költség-haszon elemzés és a teljesítménymérés is további kutatási feladat lesz.

KÖVETKEZTETÉS

A nagy nyelvi modellek integrációja a biztonságkritikus rendszerekbe egyaránt hordoz magában óriási lehetőségeket és jelentős felelősséget. Az LLM-ek lehetőséget nyújtanak arra, hogy a biztonságtechnika területén új szintre lépjünk: intelligensebb felügyeleti rendszerek, proaktív hibamegelőzés, gyorsabb és pontosabb vészhelyzeti reagálás valósulhat meg általuk. Például képzeljünk el egy okos elektromos hálózatot, ahol az AI előre jelzi és megakadályozza a hálózati túlterhelést, vagy egy önvezető jármű-flottát, mely minimális emberi beavatkozással, de maximális biztonsággal közlekedik. Ezek nem távoli sci-fi víziók, hanem reális középtávú célok, ha az LLM-eket sikerül megfelelő korlátok között, biztonságosan alkalmazni, ehhez azonban elengedhetetlen, hogy ezek a rendszerek alkalmazhatóságát mindig a társadalom és az üzemeltetők bizalom-küszöbéhez mérjük. Ahogy a biztonságtudományban alapelv, itt is csak akkor tekinthető elfogadhatónak egy új technológia bevezetése, ha a hozzá kapcsolódó kockázatok az ALARP-elv szerint kellően lecsökkentek. Ez a gyakorlatban azt jelenti, hogy addig nem szabad egy LLM-et

éles kritikus környezetbe állítani, amíg minden ésszerű biztonsági intézkedést meg nem tettünk, és a megmaradt, tovább nem csökkenthető kockázatot el tudjuk fogadni.

A nagy nyelvi modellek a biztonságtechnika fejlődésének következő mérföldkövét jelenthetik, de csak akkor, ha bevezetésük okosan, felelősen történik. A jövő biztonságkritikus rendszerei talán már együtt fognak működni a mesterséges intelligenciával, mint társsal a fenyegetések elleni küzdelemben - de az emberi felügyelet, ítélőképesség és felelősség minden bizonnyal továbbra is kulcsfontosságú marad.

HIVATKOZÁSOK

[1] C. Kollár, "A biztonság fontosabb fogalmai," *Biztonságtudományi Szemle*, VII. évf. 1. szám oldal 15-23, 2025, doi: 10.12700/btsz.2025.7.1.15.

[2] N. C. and I. Agency, "NCIA Technology Strategy towards 2030." 2023. [Online]. Elérhető: https://www.ncia.nato.int/resources/site1/General/newsroom/publications/Public_NCIA_Technology%20Strategy_external_v6%20-%20digital.pdf

[3] R. Group, "The NATO Communications and Information Agency Selects Oracle Cloud Infrastructure." [Online]. Elérhető: https://www.reply.com/en/newsroom/news/the-nato-communications-and-information-agency-selects-oracle-cloud-infrastructure

[4] F. Piessens, P. C. van Oorschot, F. Piessens, and P. C. van Oorshot, "Side-Channel Attacks: A Short Tour," *IEEE Secur. Priv.*, vol. 22, no. 2, pp. 75–80, 2024, doi: 10.1109/MSEC.2024.3352848.

[5] J. Su *et al.*, "Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review," 2024, *arXiv*: arXiv:2402.10350. doi: 10.48550/arXiv.2402.10350.

[6] S. Madani, A. Tavasoli, Z. K. Astaneh, and P.-O. Pineau, "Large Language Models integration in Smart Grids," 2025, *arXiv*: arXiv:2504.09059. doi: 10.48550/arXiv.2504.09059.

[7] M. Stone, "DHS: Guidance for AI in Critical Infrastructure." 2024. [Online]. Elérhető: https://www.ibm.com/think/x-force/dhs-guidance-for-ai-in-critical-infrastructure

[8] S. Sivapiromrat, C. Zhang, M. Basaldella, and N. Collier, "Multi-Trigger Poisoning Amplifies Backdoor Vulnerabilities in LLMs," 2025, *arXiv*: arXiv:2507.11112. doi: 10.48550/arXiv.2507.11112.

[9] European Parliament and Council, "Artificial Intelligence Act (Regulation (EU) 2024/1689)." 2024. [Online]. Elérhető: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[10] European Union, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)." 2022. [Online]. Elérhető: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[11] J. Abonyi and T. Fülep, *Biztonságkritikus rendszerek*. Veszprém, Magyarország: Pannon Egyetem, 2014.

[12] OWASP, "Top 10 for Large Language Model Applications." 2024. [Online]. Elérhető: https://owasp.org/www-project-top-10-for-large-language-model-applications/

[13] S. Bottyán, "Nagy nyelvi modellek össebezhetőségeinek információbiztonsági kockázatai és kezelésük," Biztonságtudományi Szemle, VII. évf. 3. szám oldal 157-165, 2025, doi: 10.12700/btsz.2025.7.3.157.

DOI: https://doi.org/10.12700/btsz.2025.7.4.187

WORK ACCIDENT ANALYSIS IN A FUZZY LOGIC SYSTEM

MUNKABALESET ELEMZÉS FUZZY RENDSZERBEN

HERÉNYI Zoltán[1]

Abstract

Machine safety has traditionally been a cornerstone of occupational safety. However, with the rise of artificial intelli-gence (AI), new types of risks have emer-ged that go beyond classical technical failures. This study aims to develop a fuzzy logic-based inference model capable of identifying patterns, correlations, and regularities in workplace accidents. The model is built upon the methodological guidelines of the Hungarian Ministry of National Economy and accident case stu-dies published by the Employment Su-pervision Authority. The research also explores whether human knowledge and intent, when translated into machine logic, can generate new, relevant insights in other domains.

Keywords

artificial intelligence, fuzzy logic, accident analysis, AI-related risks, human–machine interaction

Absztrakt

A gépek biztonsága hagyományosan a munkavédelem egyik alappillére, azonban a mesterséges intelligencia (MI) térnyerésével új típusú kockázatok jelentek meg, amelyek túlmutatnak a klasszikus műszaki hibákon. A tanulmány célja egy fuzzy logikai alapú következtetési modell kidolgozása, amely képes baleseti mintázatok, összefüggések és szabályszerűségek feltárására. A modell alapját a Nemzetgazda-sági Minisztérium módszertani útmutató-ja és a Foglalkoztatás-felügyelet által közzétett esettanulmányok képezik. A kutatás célja továbbá annak vizsgálata, hogy a gépi logikára fordított emberi tudás és szándék képes-e új, releváns tudás generálására más területeken is.

Kulcsszavak

mesterséges intelligencia, fuzzy logika, balesetelemzés, MI-kockázatok, ember–gép interakció

[1] zoltan.herenyi@gmail.com | ORCID: 0009-0000-2583-7104| PhD student, Doctoral School of Safety and Security Sciences, Óbuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A munkahelyi biztonság megteremtése szorosan összefügg az ott működő gépek biztonságos üzemeltetésével és az általuk végzett munkafolyamatok kontrollálhatóságával. A gépek biztonsága mindig is kiemelt szerepet töltött be a munkavédelemben, hiszen minél nagyobb mértékben haladják meg teljesítményükben az emberi képességeket – legyen szó erőről, gyorsaságról vagy pontosságról, annál nagyobb kockázatot jelent a működésük feletti irányítás elvesztése.

Ez a kockázat az intelligens rendszerek és a mesterséges intelligenciával támogatott gépek megjelenésével új dimenziókat ölt. Az ilyen gépek számos tekintetben meghaladják az emberi teljesítőképességet, ugyanakkor működésük során nemcsak egyszerű mechanikai hibák jelentkezhetnek, hanem a feladatok értelmezéséből fakadó, komplex korábban ismeretlen viselkedési hibák is.

Külön figyelmet érdemel az a tény, hogy a kezelőszervek hagyományos használatát egyre inkább felváltja a természetes nyelvű, verbális utasításadás. Bár ez elsődlegesen a kezelők számára egyszerűsítést jelent, a félreértelmezések esélye is jelentősen megnő, különösen összetett vagy kontextusfüggő feladatok esetén. A gépi intelligencia számára nemcsak a nyelvi utasítás helyes értelmezése kihívás, hanem az emberi szándék mélyebb, környezeti és szakmai kontextusba ágyazott felismerése is.

Ezért válik kulcsfontosságúvá egy olyan előfeldolgozási mechanizmus kidolgozása, amely képes a humán szándékokat formalizált szabályrendszerek mentén, a munkakörnyezet sajátosságait figyelembe véve értelmezni.

Ezen tanulmány egy kutatás eredményeit mutatja be. A vizsgálat célja az volt, hogy a Foglalkoztatás-felügyelet hivatalos felületén publikált halálos munkabaleseti esettanulmányokat elemezze. A feldolgozás alapját a Nemzetgazdasági Minisztérium által kiadott „Módszertani útmutató a munkabalesetek hatósági vizsgálatához” című dokumentum elvei képezték.

A kutatás során egy fuzzy logikán alapuló szabálybázis került kialakításra. Ennek célja, hogy a rendszer képes legyen hasonló következtetések levonására, mint amilyenekre egy tapasztalt munkavédelmi szakember jutna. Ez a megközelítés nem csupán a múlt tanulságainak strukturált feldolgozását teszi lehetővé, hanem jövőorientált alapot biztosíthat olyan intelligens döntéstámogató rendszerek számára is, amelyek segíthetik a mesterséges intelligenciával vezérelt gépek biztonságos beillesztését a munka világába.

Számos tanulmány található ebben a témában [1], [2] köztük olyan is mely több erre vonatkozó munkát gyűjtött össze strukturált formában [3] A gyakorlati alkalmazásokra jó példa a LumApps vállalati rendszer, amely a tudásalapú döntéstámogatás számos aspektusát mutatja be digitális platformokon keresztül [4].

A tudásalapú döntéstámogató rendszerek gyakorlati alkalmazására a Brain Pod AI komplex mesterséges intelligencia platformja is több példát kínál [5]. A kutatás célkitűzései összhangban állnak az EU-OSHA kutatási programjával [6] , az Európai Unió munkahelyi egészségvédelemre és biztonságra vonatkozó stratégiájával [7],valamint Magyarország munkavédelemre vonatkozó nemzeti politikájával [8]Amennyiben a fejlesztések a mesterséges intelligenciával támogatott kiterjesztett intelligencia irányába haladnak, az nemcsak a hatósági munka hatékonyságát növelheti, hanem hozzájárulhat a munkavédelem digitalizációs céljainak eléréséhez is [9].

A kutatás fő kérdései:

- K1. Annak vizsgálata, hogy a komplex emberi tudás formalizálható-e oly módon, hogy az gépi feldolgozásra alkalmassá váljon numerikus értékek, logikai struktúrák vagy szabályalapú reprezentációk formájában?
- K2. Ezt követően annak feltérképezése válik kulcsfontosságúvá, hogy az ily módon kódolt tudásból kiindulva lehetőség nyílik-e új, eddig ismeretlen vagy rejtett tudáselemek, összefüggések feltárására. Azaz a rendszer egy fejlettebb változata képes lehet-e tanulni, következtetni és önállóan tovább építeni a meglévő ismeretbázist?

SZAKIRODALOMI ÁTTEKINTÉS

Az Európai Unió országainak munkavédelmi tapasztalatai alapján az Európai Bizottság rendszeresen új keretirányelveket dolgoz ki, melyeket a tagállamoknak nemzeti stratégiáikba kell illeszteniük [10]. A munkavédelem európai szabályozásának alapkövét a 89/391/EGK keretirányelv[11] képezi, amely a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedéseket vezet be. A dokumentum általános jelleggel határozza meg a munkáltatók kötelezettségeit, így például az 5. cikk (1) bekezdése kimondja, hogy a munkáltató felelőssége a munkavállalók biztonságának és egészségvédelmének biztosítása minden, a munkával kapcsolatos szempontból. A 6. cikk (1) bekezdés tovább részletezi e kötelezettségeket, hangsúlyozva a megelőzés, a tájékoztatás, az oktatás és a megfelelő szervezettség fontosságát. Ez az általános alap képezi a kiindulópontját azoknak a további irányelveknek, amelyek konkrét technikai és tárgyi kockázatok kezelésére irányulnak. Kiemelendő közülük a 2009/104/EK irányelv [12] Munkavédelem, amely a munkaeszközök biztonsági és egészségvédelmi minimumkövetelményeit határozza meg. A dokumentum 2. cikk a) pontja alapján „munkaeszköz minden olyan gép, eszköz, szerszám vagy felszerelés, amelyet munka során használnak”, így közvetlen kapcsolatot teremt a munkavédelem és a gépek használatának szabályozása között. A gépek tervezésére és megfelelőségi követelményeire azonban már nem munkavédelmi irányelv, hanem a 2006/42/EK irányelv[13]. közismertebb nevén a gépdirektíva vonatkozik. Ez a szabályozás külön kezeli a gépek műszaki biztonságát, azonban célja szorosan kapcsolódik a munkavédelemhez: a veszélyforrások azonosítása, megszüntetése és a maradék kockázatok kezelése.

A fenti uniós szabályokat a magyar jogrendszer több lépcsőben integrálta. A keretirányelv rendelkezéseinek harmonizálására az 1993. évi XCIII. törvény a munkavédelemről (munkavédelmi törvény) szolgál[14]. A 2009/104/EK irányelv [12] hazai megfelelője a 10/2016. (IV. 5.) NGM rendelet, amely a munkaeszközök biztonsági és egészségügyi követelményeinek minimumszintjét rögzíti. A gépdirektíva nemzeti átültetése a 16/2008. (VIII. 30.) NFGM rendeletben [15] történt meg, amely a gépek megfelelőségi tanúsításáról és biztonsági követelményeiről rendelkezik.

Ezek az irányelvek, valamint kapcsolódó dokumentumok és statisztikák elérhetők az Európai Unió hivatalos honlapján [16]. A hivatalos munkavédelmi felületek nem csupán a szakemberek számára nyújtanak tájékozódási alapot, hanem a cégvezetők számára is irányt mutatnak az ipar és a technológia fejlődési irányairól. Ezáltal segítik az új kihívásokra való felkészülést és a biztonságos működéshez szükséges stratégiai döntések meghozatalát. Az EU 2014–2020-as munkavédelmi stratégiája kiemelten kezeli a tagállami érvényesítés

javítását, és hangsúlyozza, hogy a jogi eszközök mellett felhasználóbarát informatikai megoldásokra is szükség van [17]. A 2023–2025-ös Egészséges munkahelyek – Biztonságos és egészséges munkahely a digitális korban kampány újabb lendületet ad a munkavédelem digitalizációjának [18].

Magyarországon a 2024. január 12-én kiadott „A munkavédelem nemzeti politikája 2024-2027" minisztériumi tájékoztató is megerősíti, hogy a zöld és digitális átállás a stratégia három kulcseleme között szerepel [8] a munkavédelem jövője tehát erősen technológia orientált irányba mozdul el.

A munkavédelem digitalizációja nem teljesen újkeletű dolog, így ennek megfelelően már évek óta léteznek olyan szoftverek a világpiacon melyek képesek valamilyen munkavédelmi feladat megoldására. Erre láthatunk példát ,[19]munkája nyomán is, aki tanulmányában az ergonómiai szoftverekre vonatkozó tapasztalatokat mutatta be. A mesterséges intelligencia iparra és társadalomra gyakorolt hatását vizsgáló tanulmányok egyre gyakrabban utalnak arra, hogy a már napjainkban is érzékelhető változások egy újabb ipari forradalom előhírnökei lehetnek. [20] A szerzők szerint az MI nem csupán következménye, hanem egyre inkább motorja is a társadalmi és gazdasági átalakulásoknak, új korszakokat nyitva meg az ipar és a munka világában.

Számos tanulmány foglalkozik az AI felhasználási területeinek kutatásával, illetve működési mechanizmusaival.

Kollár és társai gyakorlati [21], [22] és szakértői oldalról is [23],[24],[25] megvilágították a mesterséges intelligencia használatának kérdését.

Egyes kutatások már kifejezetten az intelligens gyárak számára szükséges készségek és képességek feltérképezésére fókuszálnak – például Kelemen-Erdős és Beke munkája [26]

A mesterséges intelligencia jelen fejlettségével [27] ,[28] ugyanis elérkeztünk egy olyan ponthoz, ahol az informatikai eszközök már nemcsak támogatják, hanem alapjaiban alakítják át a munkavédelem működését,[29] melyet mi sem bizonyít jobban mint az (EU) 2023/1230 rendelet [30] közismert nevén az új géprendelet megjelenése, amelyet az Európai Parlament és a Tanács 2023. június 29-én fogadott el. Ez a rendelet hatályon kívül helyezi a korábbi 2006/42/EK gépirányelvet [13]és a 73/361/EGK tanácsi irányelvet [31] , egyúttal teljesen új alapokra helyezi a gépek és kapcsolódó termékek biztonsági követelményeit – immár kifejezetten figyelembe véve a mesterséges intelligenciát alkalmazó rendszerek kockázatait is. A második sarokkő az AI Act (mesterséges intelligenciáról szóló rendelet) [32] , amelyet az Európai Parlament 2024. március 13-án szavazott meg, és amely az első olyan átfogó jogi keretrendszert teremti meg világszinten, amely kockázatalapú megközelítés mentén szabályozza a mesterséges intelligencia rendszerek fejlesztését, forgalmazását és használatát az Európai Unió területén. Az új géprendelet 2023/1230 rendelet [30] III. mellékletének 1.1.6. szakaszában található az idézett szöveg. „Adott esetben olyan gép vagy kapcsolódó termék átalakítása, amelynek szándékoltan teljesen vagy részben önfejlődő viselkedése vagy logikája különböző szintű önálló működésre van tervezve, hogy helyesen és megfelelő módon reagáljon az emberekre (például verbálisan szavak, nem verbálisan pedig arckifejezések vagy testmozgás révén), és hogy érthető módon tájékoztassa a kezelőket a tervezett műveleteiről (például mire és miért fog sor kerülni)" Ez elővetíti azt hogy az egyre dinamikusabban átalakuló munkakörnyezethez való alkalmazkodást fejlett döntéstámogató rendszerek fogják segíteni.

A döntéstámogató rendszerek fejlesztése tehát ma már nem pusztán elméleti lehetőség, hanem egyre inkább kézzelfogható gyakorlati cél, amelynek hatékony alkalmazására több sikeres példa is létezik. [33], [34], [35] Mindezek fényében már csak idő kérdése, hogy ezek a rendszerek a munkavédelemben is vezető szerephez jussanak a munkáltatói oldalon. A megváltozott ipari környezet új típusú kihívásokat is magával hozhat, amelyek vizsgálata nem csupán új szemléletmódot kíván a munkavédelmi hatóságoktól, hanem az ellenőrzések hatékonyságának számottevő növekedését is.

Egy mesterséges intelligenciával támogatott döntéstámogató rendszer használata egy potenciálisan jó irány egy magasan fejlett hatósági működés felé.

Számos tanulmány utal arra, hogy a legnagyobb eredményeket az ember és a mesterséges intelligencia közös tanulása, egymás képességeinek kiegészítése hozza. [9]A kiterjesztett intelligencia két alapformája ismert: a kiterjesztett humán intelligencia esetében az ember hozza meg a végső döntést a gép által előkészített adatok alapján, míg a kiterjesztett mesterséges intelligencia esetén a döntés végső pontját már a rendszer maga határozza meg. A mesterséges intelligencia alkalmazása emberi szűrőn keresztül optimális – ugyanakkor figyelembe kell venni, hogy a döntés minősége ebben az esetben már az ember aktuális értelmi, érzelmi és mentális állapotától is függ. Ezért a magyarázható mesterséges intelligencia (XAI) rendszerek alkalmazása különösen indokolt lehet a munkavédelmi területen, ahol az emberi felhasználó számára érthető indoklások elengedhetetlenek a döntések elfogadásához és validálásához. Az XAI biztosítja, hogy az MI által javasolt következtetések és ajánlások átlátható logikai láncon keresztül visszakövethetők legyenek [36].

Ez a dinamikus ember-gép döntési rendszer új lehetőségeket nyithat a munkavédelmi ellenőrzések és balesetkivizsgálások hatékonyságának növelésében. Ebben az összefüggésben például Nemzetgazdasági Minisztérium által kiadott „Módszertani útmutató a munkabalesetek hatósági vizsgálatához” című dokumentum nemcsak útmutatásként szolgálhat, hanem egy lehetséges döntéstámogató rendszer strukturált tudásbázisát is képezheti [2] amennyiben tartalmát a gépi intelligencia számára is értelmezhető formába lehet transzformálni, [37]

A döntéstámogató rendszerek működése során az egyik legnagyobb kihívás annak biztosítása, hogy a rendszer ne csak adattárolóként, hanem értelmezőként is funkcionáljon. Ehhez szükséges, hogy az emberi szakértelemből származó tapasztalatokat abstrakt szabályok, súlyozások, prioritási sorrendek formájában transzformáljuk [38], [39]Mindez lehetővé teszi egy olyan adaptív rendszer kialakítását, amely nem csupán tényeket rögzít, hanem képes helyzetértékelésre, kontextusfüggő következtetések levonására is [40], [41]

KUTATÁSMÓDSZERTAN

A kutatás módszertani alapját egy kvalitatív megközelítésű, részben Grounded Theory (GT) [42] alapú módszer képezi, amelyet deduktív és induktív logikai lépések együttes alkalmazása egészít ki. A GT célja, hogy az esettanulmányok elemzése során alulról építkezve feltárja azokat a szempontokat, relációkat és szabályszerűségeket, amelyek később a fuzzy logikai modell alapstruktúráit képezik. A kvalitatív tartalomelemzés segítségével az egyes baleseti esetekből nyert emberi tudás – beleértve a szándékokat, hibázási láncokat és környezeti kontextusokat – numerikus és logikai formába került átalakításra.

A kutatás célja egy olyan fuzzy logikára épülő következtetési modell kialakítása, amely képes munkabaleseti esettanulmányok alapján rejtett összefüggések és mintázatok

feltárására, a humán szándék és tudás gépi logikába történő átültetésével. A módszertan az alábbi négy egymásra épülő szakaszra tagolható.

Forrásanyagok rendszerezése

Az elemzéshez használt esettanulmányok a Foglalkoztatás-felügyelet által publikált halálos munkabaleseti esetleírásokból származnak, melyeket a Nemzetgazdasági Minisztérium „Módszertani útmutató a munkabalesetek hatósági vizsgálatához” alapján kerültek újra strukturálásra. A cél az adatok formalizálása gépi feldolgozásra alkalmas formában.

Szempontrendszer és szabályalapú modellezés

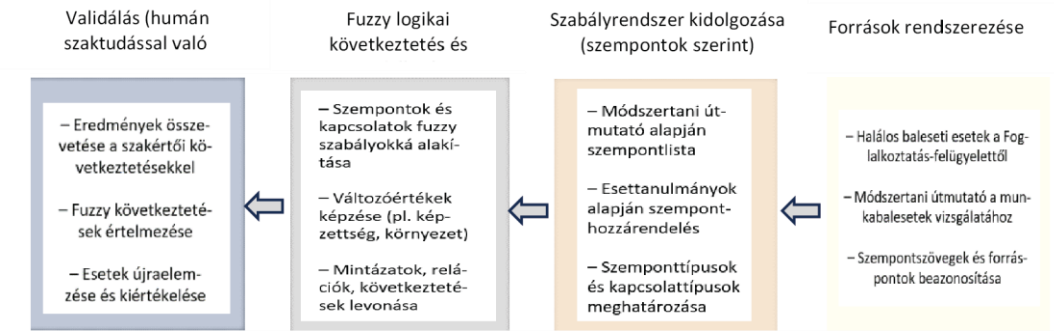
A kvalitatív megfigyelések kvantifikálása egy előre definiált vizsgálati szempontrendszer alapján történik. Minden szempont esetében rögzítésre kerül annak jelenléte, relevanciája és a kapcsolódó logikai viszonyok. Ezek alapján fuzzy szabályok alkotása történik, amelyek képesek leképezni a szakértői gondolkodás alapmintáit.

Fuzzy következtetési rendszer kiépítése

Az azonosított szempontok és szabályok alapján fuzzy logikai modell kerül kialakításra, ahol a szöveges, gyakran bizonytalan megfogalmazások numerikus logikai reprezentációval párosulnak. A rendszer célja nem bináris döntések hozatala, hanem a valószínűségi relációk értelmezése a gépi tudásalkotás elősegítésére.

Validálás és reflexív tanulságlevonás

A modell teljesítménye az eredeti esettanulmányok alapján ellenőrzésre kerül, összevetve a szakhatósági következtetésekkel. Ezen felül vizsgálatra kerül, hogy a rendszer képes-e új, eddig nem dokumentált összefüggések azonosítására, azaz tanul-e a szabályalapú tudásból. Ez nemcsak a munkavédelmi területen, hanem más, emberi szándék visszafejtésére épülő rendszerekben is alkalmazhatóvá teszi a módszert.



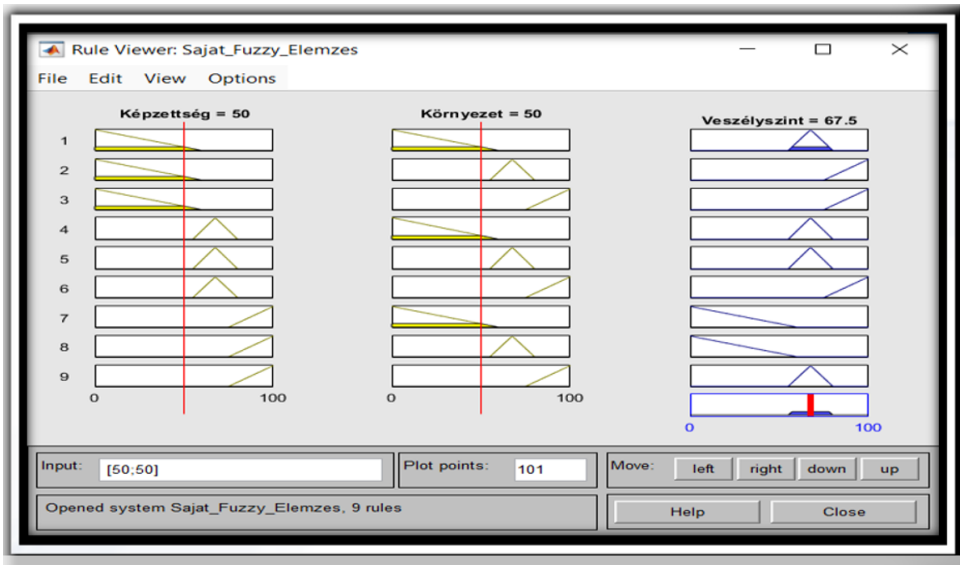
1. Ábra: A fuzzy logikai következtetési modell felépítése a munkabaleseti elemzés során
Forrás: Saját szerkesztés

Az alábbi ábra a mesterséges intelligencia alkalmazásán alapuló, fuzzy logikai következtetési modell kialakításának lépéseit mutatja be, amely strukturáltan vezeti végig a baleseti esettanulmányok szöveges tartalmától a gépi következtetésekig.

A folyamat során az emberi szakértői tudás formális szabályokká alakul, majd ezek alapján lehetőség nyílik új, releváns tudás generálására. Az ábra balról jobbra haladva végigkíséri a tudás kinyerés, szerkezetépítés, súlyozás, logikai kapcsolás, és végül a fuzzy

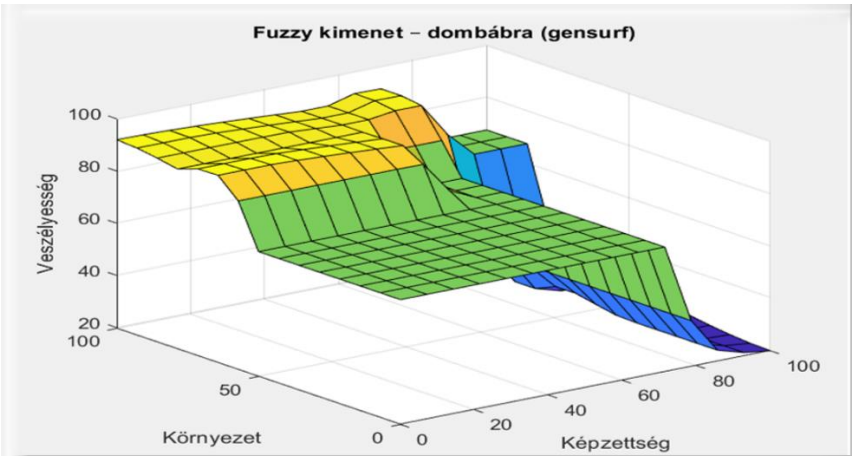
következtetés egyes szakaszait – összekapcsolva a valóságos tapasztalatokat a gépi értelmezés világával.

KUTATÁSI EREDMÉNYEK



2. Ábra A rendszer szabályrendszerének grafikus megjelenítése Forrás: Saját szerkesztésű

A 2. ábra a fuzzy döntéstámogató rendszer szabályrendszerének grafikus megjelenítését mutatja. Az ábrán a bemeneti változók („Képzettség” és „Környezet”) értékei 50–50, amelyek alapján a rendszer a kilenc szabály mindegyikét aktiválja különböző mértékben. A jobb oldalon látható kimeneti változó („Veszélyszint”) értéke 67,5, amely a szabályok által súlyozott következtetés eredménye. A piros függőleges vonalak a bemeneti értékeket, míg az alsó, vastag piros vonal a defuzzifikált kimeneti értéket jelöli. Az ábra jól szemlélteti, hogy a rendszer miként építi fel az eredményt a különböző szabályok és bemeneti értékek kombinációjából.



3. Ábra Veszélysűrűség ábra az első vizsgálat elvégésekor Forrás: Saját szerkesztésű

A 3. ábra a fuzzy modell első vizsgálatának eredményeként létrejött kimeneti felületet (gensurf) szemlélteti. A dombábra azt mutatja meg, hogy a „Képzettség” és a „Környezet” változók különböző értékeinél mekkora a várható „Veszélyesség” szintje. Jól látható, hogy a veszélyesség mértéke különösen akkor magas, ha a képzettség alacsony, miközben a környezeti kockázat magas – ez a térképen sárgás és narancsszínű régióként jelenik meg. Ezzel szemben a magasabb képzettségi szintek egyértelműen csökkentik a veszély mértékét még kedvezőtlen környezeti feltételek mellett is. Az ábra megerősíti a modell várakozásait, és vizuálisan is igazolja, hogy a két bemeneti változó között erős, nemlineáris kapcsolat figyelhető meg a kimeneti veszélyérték tekintetében.

	Kepzettseg	Kornyezet	CoA	Szint
1	27	59	88.5000	MV
2	38	67	89.9000	MV
3	38	69	89.9000	MV
4	53	67	88.5000	MV
5	35	82	89.4000	MV
6	47	82	89.1000	MV
7	32	91	90.4000	MV
8	32	91	90.4000	MV

4. Ábra Az első vizsgálat eredményei Forrás: Saját szerkesztésű

A 4. ábra az első modellfutás eredményeit tartalmazza, amelyben a „Képzettség” és a „Környezet” tényezők együttes hatása jelenti a maximálisan lehetséges veszélyszintet. Ebben az esetben az értelmezés szerint a két változó teljes mértékben lefedi a balesetveszélyt, így azok együttes hatása alkotja a 100%-os referenciaértéket. A CoA (Center of Area) módszerrel meghatározott kimeneti értékek szinte kivétel nélkül a magas veszélyszint (MV) kategóriájába estek, ami azt jelzi, hogy a rendszer a két tényező alapján helyesen ismeri fel a veszélyeztetettséget. Az eredmények tehát jól tükrözik a modell érzékenységét a kulcstényezők kombinációira.

	Kepzettseg	Kornyezet	CoA	Szint
1	38	41	67.5000	KV
2	54	47	67.5000	KV
3	54	48	67.5000	KV
4	76	47	54.8000	KV
5	50	57	83.8000	MV
6	67	57	67.5000	KV
7	45	63	89.2000	MV
8	45	63	89.2000	MV

5. Ábra A második vizsgálat eredményei Forrás: Saját szerkesztésű

Az 5. ábra a második vizsgálat eredményeit mutatja, ahol a viszonyítási alap már nem a két változó együttes maximuma, hanem a teljes baleseti szituáció komplex veszély-

szintje. Ez azt jelenti, hogy a modellnek azt kellett megbecsülnie, a „Képzettség” és a „Környezet” tényezők együtt milyen arányban járultak hozzá a ténylegesen bekövetkezett balesethez. A kimeneti értékek itt változatosabb képet mutatnak, több eset a közepes veszélyszint (KV) kategóriájába esik, ami arra utal, hogy a vizsgált tényezők az adott esetekben nem kizárólagosan determinálták a balesetek bekövetkezését. Ez a megközelítés segíti az ok-okozati viszonyok finomabb megértését, és rámutat arra is, hogy egyes szituációkban további tényezők is jelentős szerepet játszhattak.

KÖVETKEZTETÉSEK, JAVASLATOK

Az 1-5-ig az ábrák a rendszer első működési ciklusának eredményeit mutatják be. A 2. ábra a kialakított szabályhalmazt, valamint az aggregált kimeneti eredményeket jeleníti meg. A grafikus felület lehetőséget biztosít az egyes szabályok külön-külön történő tesztelésére, ezáltal nyomon követhető, hogy azok milyen kimenetekhez vezetnek. Fontos azonban hangsúlyozni, hogy ez a felület nem alkalmas a rendszer egészének működésére vonatkozó érvényességi megállapításokra, azaz nem képes visszajelzést adni a teljes logikai struktúra helyességéről.

A rendszer validálásában kulcsszerepet játszik a veszélysűrűség-vizsgálat, amelyet a 3. ábra szemléltet. Ezek az ábra a rendszer működésének minőségéről, valamint a veszélyeloszlások logikai következményeiről ad tájékoztatást. A konkrét működési helyesség alátámasztására azonban elsősorban a 4. és 5. ábrák szolgálnak, amelyek a kimeneti értékeket rendszerszintű logikai összefüggések mentén mutatják be.

A két megközelítés szerint készült eredménytáblázatok különböző értelmezési szinteket képviselnek. Az első megközelítés szerint a vizsgált veszélyszintet kizárólag a két bemeneti változó – a „Képzettség” és a „Környezet” – kombinációja idézte elő. Mivel ebben az esetben nem kerültek bevonásra további tényezők, a modell logikája szerint a két változónak együttesen közelítenie kell a 100%-os veszélylefedettséghez. A 4. ábra tanúsága szerint az eredmények 88–90% közötti tartományban mozogtak, ami azt jelzi, hogy a rendszer működése ebben az értelemben megfelelt az elvárásoknak.

A második megközelítés a két változó relatív hozzájárulását vizsgálta a balesetek során ténylegesen kialakult veszélyszinthez képest. Előzetes számítások alapján ebben az értelmezésben a várható hozzájárulás átlagosan 72% volt, amely a rendszer besorolása szerint a közepes veszélyszintnek felel meg. Ez arra utal, hogy még abban az esetben is, ha a balesethez vezető valamennyi kulcstényező a két fő szál valamelyikén megjelent, a tényleges baleseti veszélyszintnek csak körülbelül 70%-át tudták lefedni – ami azt is jelenti, hogy a balesetnek elvileg nem kellett volna bekövetkeznie. Mivel azonban minden vizsgált esetben súlyos balesetről volt szó, ez az érték elsőre alacsonynak tűnhet.

Fontos ugyanakkor megjegyezni, hogy a rendszerben megjelenő kulcstényezők súlyozása nem kizárólag a tényleges jelentőségükön, hanem a vizsgálati szálakhoz való kapcsolódásuk erősségén is múlik. Azok a tényezők, amelyek nem közvetlenül a felügyelői értékelés révén kerültek be, vagy csak gyenge kapcsolattal voltak összeköthetők a fő szálakkal, automatikusan alacsonyabb súlyozást kaptak. Ennek kiküszöbölésére a jövőbeni verziókban cél a kapcsolati súlyozás módosítása, valamint több vizsgálati szál párhuzamos alkalmazása, amely lehetővé teszi a tényezők valós értékének pontosabb visszatükrözését.

Összességében a várható eredmények a közepes veszélyszint tartományába estek, és a tényleges kimenetek ezt többnyire megerősítették. A 5. ábra szerint az esetek többsége

valóban ebbe a kategóriába esett, ugyanakkor az esetek 37%-ában magas veszélyszintet mutatott a rendszer. Bár a korábbi matematikai előrejelzések alapján nem lett volna várható ilyen magas kategória, azok csak az átlagértékekre vonatkoztak. Egyedi esetek szintjén korábban is megfigyelhetők voltak hasonló eltérések.

Mindezek alapján kijelenthető, hogy a rendszer működése megfelelőnek tekinthető, azonban a kapott eredmények részletesebb értelmezése és a vizsgálatok bővítése több baleseti eset bevonásával elengedhetetlen a végleges következtetések megalapozásához

ÖSSZEFOGLALÁS

A balesetvizsgálat eredményessége nem kizárólag a tudás mennyiségén vagy a szakemberek felkészültségi szintjén múlik, hanem azon is, hogy a meglévő ismeretek és gyakorlati tapasztalatok miként illeszkednek az adott kivizsgálási helyzet sajátos körülményeihez. Ez különösen igaz a hatóságok által végzett helyszíni vizsgálatokra, amelyek során pszichés nyomás, időkorlátok és számos egyéb akadályoztató tényező mellett kell objektív és megalapozott döntéseket hozni. E körülmények között jelentős támogatást nyújthat egy olyan döntéstámogató rendszer, amely képes a már rendelkezésre álló adatok alapján meghatározni a további szükséges információkat, irányt mutatni a vizsgálat folytatásához, illetve a teljes adathalmaz birtokában elősegíteni az objektív tényfeltárást.

A jelen tanulmány célja egy ilyen rendszer alapjainak lefektetése volt. A kidolgozott megközelítés ötvözi a munkavédelmi szakértők gyakorlati tapasztalatait, a súlyos és halálos munkabalesetekből levonható tanulságokat, valamint a fuzzy logikai rendszer rugalmasságát. Az így kialakított modell a vizsgált nyolc baleseteset elemzése során két fő vizsgálati szál – a munkavállalók képzettsége, illetve a környezeti tényezők – mentén haladva átlagosan a releváns szempontok 72%-át volt képes feltárni és fuzzy modellben értékelni.

Ez az eredmény különösen biztató annak fényében, hogy a modellbe a jövőben további vizsgálati szálak is integrálhatók, amely még tovább növelheti az értékelés hatékonyságát. Fontos azonban hangsúlyozni, hogy a rendszer nem az emberi döntés kiváltására, hanem annak támogatására szolgál. Már a jelenlegi eredmények is bizonyítják, hogy hasznos kiegészítő eszközként szolgálhat a balesetvizsgálatok során.

Bár a rendszer mindhárom pillére – a kivizsgálási módszertan, a baleseti tanulságok, valamint a fuzzy megközelítés – külön-külön is bizonyították létjogosultságukat, a mostani konfiguráció hatékonysága és gyakorlati alkalmazhatósága csak további esettanulmányok és validációs folyamatok révén nyerhet teljes megerősítést.

FELHASZNÁLT IRODALOM[2]

[1] I. C. Baierle, M. A. Sellitto, R. Frozza, J. L. Schaefer, and A. F. Habekost, "*An artificial intelligence and knowledge-based system to support the decision-making process in sales*," South African Journal of Industrial Engineering, vol. 30, no. 2, pp. 17–25, Aug. 2019. [Online]. Available: https://doi.org/10.7166/30-2-1964

[2] M. Tanque, "*Knowledge Representation and Reasoning in AI-Based Solutions and IoT Applications,*" in Artificial Intelligence to Solve Pervasive Internet of Things Issues,

[2] példák hivatkozásokra | REFERENCES examples of references

Elsevier, 2021, pp. 13–49. [Online]. Available: https://doi.org/10.1016/B978-0-12-818576-6.00002-2

[3] N. Tamascelli, A. Campari, T. Parhizkar, and N. Paltrinieri, "*Artificial Intelligence for safety and reliability: A descriptive, bibliometric and interpretative review on machine learning*,"Journal of Loss Prevention in the Process Industries, vol. 90, art. 105343, 2024. [Online]. Available: https://doi.org/10.1016/j.jlp.2024.105343

[4] [5] LumApps, "*Exploring knowledge-based systems: Enhancing decision-making with AI.*" [Online]. Available: https://www.lumapps.com/insights/blog/exploring-knowledge-based-systems-enhancing-decision-making-ai. [Accessed: Jun. 10, 2025].

[5] Brain Pod, "*Exploring knowledge-based agents in AI: Real-world examples and applications*," [Online]. Available: https://brainpod.ai/exploring-knowledge-based-agents-in-ai-real-world-examples-and-applications/. [Accessed: Apr. 20, 2025].

[6] EU-OSHA, "*Digitalisation and occupational safety and health: EU-OSHA research programme,*" [Online]. Available: https://osha.europa.eu/hu/publications/digitalisation-and-occupational-safety-and-health-eu-osha-research-programme. [Accessed: Apr. 20, 2025].

[7] European Commission, "*Strategic policy documents*," [Online]. Available: https://employment-social-affairs.ec.europa.eu/policies-and-activities/rights-work/health-and-safety-work/strategic-policy-documents_de. [Accessed: Apr. 20, 2025].

[8] Ministry for Innovation and Technology, "*Digital Labour Protection Strategy*," Hungarian Government, [Online]. Available: https://cdn.kormany.hu/uploads/document/4/48/48c/48c0999a11d2e7741d110165f40505ec9d341513.pdf. [Accessed: Apr. 20, 2025].

[9] A. Correia, A. B. Barr, T. Malone, P. Dillenbourg, and G. Fischer, "*Designing for Hybrid Intelligence: A Taxonomy and Survey of Crowd-Machine Interaction*," Applied Sciences, vol. 13, no. 4, p. 2198, Feb. 2023, doi: 10.3390/app13042198.

[10] European Agency for Safety and Health at Work, "OSH strategies," [Online]. Available: https://osha.europa.eu/hu/safety-and-health-legislation/osh-strategies. [Accessed: Apr. 20, 2025].

[11] European Union, Council Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work, Available: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex:31989L0391. [Accessed: Jun. 10, 2025].

[12] European Union, Directive 2009/104/EC concerning the minimum safety and health requirements for the use of work equipment by workers at work, Available: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32009L0104. [Accessed: Jun. 10, 2025].

[13] European Union, Directive 2006/42/EC on machinery, and amending Directive 95/16/EC (recast), Available: https://eur-lex.europa.eu/legal-content/hu/ALL/?uri=CELEX%3A32006L0042. [Accessed: Jun. 10, 2025].

[14] 1993. évi XCIII. törvény a munkavédelemről, NetJogtár, Available: https://net.jogtar.hu/jogszabaly?docid=99300093.tv. [Accessed: Jun. 10, 2025].

[15] 16/2008. (VIII. 30.) NFGM rendelet a gépek biztonsági követelményeiről, [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a0800016.nfg

[16] "*Sicherheit und Gesundheitsschutz am Arbeitsplatz - Europäische Kommission*," Accessed: Apr. 17, 2025. [Online]. Available: https://employment-social-affairs.ec.europa.eu/policies-and-activities/rights-work/health-and-safety-work_de
[17] "*Strategiepapiere - Europäische Kommission*," Accessed: Apr. 17, 2025. [Online]. Available: https://employment-social-affairs.ec.europa.eu/policies-and-activities/rights-work/health-and-safety-work/strategic-policy-documents_de
[18] Digitalisation and occupational safety and health – EU-OSHA research programme, [Online]. Available: https://osha.europa.eu/hu/publications/digitalisation-and-occupational-safety-and-health-eu-osha-research-programme
[19] Gy. Szabó, "*Az ergonómiai funkciók szerepe a digitalizált termelési folyamatokban, a digitalizált iparban*," Gép, vol. 69, no. 1, pp. 78–82, 2018. [Online]. Available: https://epa.oszk.hu/03300/03334/00041/pdf/EPA03334_gep_2018_1_078-082.pdf
[20] E. González-Sarmiento, J. Roa-Perez, and L. Ortiz-Ospino, "*Big Data and Artificial Intelligence in the Development of Industry 4.0: A Bibliometric Analysis*,"IOP Conference Series: Materials Science and Engineering, vol. 1154, art. 012008, Jun. 2021, doi: 10.1088/1757-899X/1154/1/012008.
[21] Cs. Kollár and B. Nagy, "*A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (első rész),*" Biztonságtudományi Szemle, vol. 3, no. 1, pp. 123–140, Mar. 2021. [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/126
[22] Cs. Kollár and B. Nagy, "*A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (második rész),*"Biztonságtudományi Szemle, vol. 3, no. 2, pp. 115–129, Jun. 2021. [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/160
[23] M. H. Lehoczky and C. Kollár, "*On the road to human-scale artificial intelligence, as seen by our experts,*" Biztonságtudományi Szemle, vol. 4, no. 1. Ksz., pp. 5–21, Oct. 2022. [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/254
[24] M. H. Lehoczky and C. Kollár, "*A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből (1. rész)*,"Biztonságtudományi Szemle, vol. 4, no. 1, pp. 117–129, Mar. 2022. [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/208
[25] M. H. Lehoczky and C. Kollár, "*A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből (2. rész),*" Biztonságtudományi Szemle, vol. 4, no. 2, pp. 87–101, Jun. 2022. [Online]. Available: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/231
[26] A. Kelemen-Erdős and É. Beke, "*A mesterséges intelligencia az oktatásban – lehetőségek és korlátok,*" Iskolakultúra, vol. 33, no. 8, pp. 52–66, 2023, doi: 10.14232/iskkult.2023.8.52.
[27] J. Liu, X. Kong, F. Xia, X. Bai, L. Wang, Q. Qing, and I. Lee, "*Artificial Intelligence in the 21st Century,*" IEEE Access, vol. 6, pp. 34403–34421, 2018, doi: 10.1109/ACCESS.2018.2819688.
[28] J. Sevilla, L. Heim, A. Ho, T. Besiroglu, M. Hobbhahn, and P. Villalobos, "*Compute trends across three eras of machine learning*," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Padua, Italy, Jul. 2022, pp. 1–8, doi: 10.1109/IJCNN55064.2022.9891914.

[29] "*Can AI actually increase human productivity? | World Economic Forum*," World Economic Forum, May 2023. Accessed: Apr. 17, 2025. [Online]. Available: https://www.weforum.org/stories/2023/05/can-ai-actually-increase-productivity/
[30] "*Regulation - 2023/1230 - EUR-Lex*," EUR-Lex. Accessed: Jun. 01, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/1230/oj?locale=hu
[31] "*Directive - 73/361 - EUR-Lex*," EUR-Lex, Accessed: Jun. 01, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A31973L0361
[32] "*EU AI Act: The First Regulation on Artificial Intelligence*," European Parliament, Accessed: Jun. 01, 2025. [Online]. Available: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[33] A. Kułakowska, E. Frankowska, and B. Sadzińska, "*Implementation of the Behavioural Observation Programme as Part of the Work Safety Strategy*," Safety & Fire Technology, vol. 56, no. 2, pp. 156–175, 2020, doi: 10.12845/SFT.56.2.2020.10.
[34] B. U. Ayhan and O. B. Tokdemir, "*Safety assessment in megaprojects using artificial intelligence*," *Saf Sci*, vol. 118, pp. 273–287, Oct. 2019, doi: 10.1016/J.SSCI.2019.05.027.
[35] M. Pishgar, S. F. Issa, M. Sietsema, P. Pratap, and H. Darabi, "*REDECA: A novel framework to review artificial intelligence and its applications in occupational safety and health*," Int. J. Environ. Res. Public Health, vol. 18, no. 13, p. 6705, Jun. 2021, doi: 10.3390/ijerph18136705.
[36] G. Kostopoulos, G. Davrazos, and S. Kotsiantis, "*Explainable artificial intelligence-based decision support systems: A recent review,*"Electronics, vol. 13, no. 14, p. 2842, Jul. 2024, doi: 10.3390/electronics13142842.
[37] M. Gul, "*A review of occupational health and safety risk assessment approaches based on multi-criteria decision-making methods and their fuzzy versions,*"Human and Ecological Risk Assessment: An International Journal, vol. 24, no. 7, pp. 1723–1760, Oct. 2018, doi: 10.1080/10807039.2018.1424531.
[38] M. Tiikkaja, M. Mäkiaho, M. M. Leppänen, P. Kivistö-Rahnasto, and T. Seppälä, "*AI-supported safety management – analysing occupational safety data using machine learning within the framework of human factors*," SSRN Electronic Journal, 2024, doi: 10.2139/SSRN.4879013.
[39] A. Y. Ng and M. Hauskrecht, "*Informed Machine Learning – A Taxonomy and Survey of Prior Knowledge Integration into Learning Systems,*" IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 5, pp. 4504–4525, May 2023, Accessed: Apr. 21, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/9429985
[40] P. Venkatachalam and S. Ray, "*How do context-aware artificial intelligence algorithms used in fitness recommender systems? A literature review and research agenda*,"International Journal of Information Management Data Insights, vol. 2, no. 2, p. 100139, Nov. 2022, doi: 10.1016/j.jjimei.2022.100139.
[41] W. Jin, R. Xu, S. Lim, D. H. Park, C. Park, and D. Kim, "*Dynamic inference approach based on rules engine in intelligent edge computing for building environment control,*" Sensors, vol. 21, no. 2, p. 630, Jan. 2021, doi: 10.3390/s21020630.

[42] J. Corbin and A. Strauss, Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory. Apr. 2008, doi: 10.4135/9781452230153.

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