ISSN 2676-9042

Vol 7, No 2, 2025.

2025, VII. évf. 2. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

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

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
Bronze Age | **Bronzkor**
painting | című festménye látható

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

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

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

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

Our journal is indexed by the following databases

Folyóiratunkat a következő adatbázisok indexelik

EBSCO

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

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

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

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

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

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

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

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

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

Published quarterly, typically in Hungarian, occasionally in a foreign language. Special and/or thematic issues related to conferences and topics are occasionally published in Hungarian or in foreign languages.

Only those papers will be published which reviewed by two independent reviewers and recommended suitable for publication in the Safety and Security Sciences Review. The submitted manuscripts must meet the requirements both of the form and the content which can be found in the journal's website. Please note: we will not return unapproved manuscripts.

The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).

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

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

A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.

Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

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

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

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

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

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

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

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

Vol 7, No 2, 2025. | **2025. VII. évf. 2. szám**

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

ANDRISKA Gergő

andriska.gergo96@gmail.com

I am Gergő ANDRISKA, a student at the Doctoral School of Safety Sciences at Óbuda University. I also obtained my pre-qualifications at the university in safety sciences, and I also have advanced training as a fire safety lecturer and occupational safety technician rela-ted to the profession. Currently, in addition to my doctoral studies, I am also completing an EHS specialist engineer training, also in connection with my university training.

ANDRISKA Gergő vagyok az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója. Előképzettségeimet is az egyetemen szereztem biztonságtudományi szakirányok-ban, emeltett a szakmához kapcsolódóan tűzvédelmi előadói és munkavédelmi technikusi képzettséggel is rendelkezem. Jelenleg a doktori tanulmányaim mellett egy EHS-szakmérnök képzést is végzek, szintén az egyetemi képzés kötelékében.

BEREK Lajos

berek.lajos@bgk.uni-obuda.hu

Prof. Dr. Lajos BEREK until 2019, he was a professor at Obuda University and the Zrínyi Miklós National Defense University, and since 2019, he has been a professor emeritus at Obuda University. He served as a colonel in the Hungarian Defense Forces between 1972 and 2006. He has been a university lecturer since 1981. He was the dean of the János Bolyai Faculty of Military Engineering at the National Defense University from 2000 to 2007. He was involved in the founding of three doctoral schools. As a university professor, his main areas of expertise are combat and operations of land forces, personal and property security and safety, and troop leadership.

Prof. Dr. BEREK Lajos 2019-ig az Óbudai Egyetem és a Zrínyi Miklós Nemzetvédelmi Egyetem professzora, 2019-től az Óbudai Egyetem pofessor emeritusa. 1972-2006 között a Magyar Honvédségben szolgált ezredesként. 1981-től egyetemi oktató. 2000-2007 a Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar dékánja. Három doktori iskola alapításában közreműködött. Egyetemi tanárként a fő szakterülete a szárazföldi csapatok harca és hadművelete, a személy- és vagyonbiztonság, a csapatok vezetése.

BRAUN András

braun.andras92@stud.uni-obuda.hu

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

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

CSERCSA Klaudia

claudiacsercsa@gmail.com

Klaudia CSERCSA is currently pursuing her doctoral studies at the Doctoral School of Security Studies at

CSERCSA Klaudia jelenleg az Óbudai Egyetemen a Biztonságtudományi Doktori Iskolában folytatja doktori ta-

the University of Óbuda. Project management, PR and press relations, and consumer behavior taught at Óbuda University. She won a MNB Scholarship in 2021 and a National Higher Education Scholarship in 2020. She won 1st place at the Scientific Student Conference in 2021 and a Special Prize in 2020. She also worked as a demonstrator and tutor at the University of Óbuda. At the Jánossy Ferenc Vocational College, she performs official duties.

nulmányait. Az Óbudai Egyetemen oktatott Projektmenedzsment, PR és sajtókapcsolatok, illetve Fogyasztói magatartás tárgyakat. 2021-ben MNB Ösztöndíjat, 2020-ban Nemzeti Felsőoktatási Ösztöndíjat nyert. Tudományos Diákköri Konferencián 2021-ben 1. helyezést, 2020-ban Különdíjat nyert. Ezenkívül demonstrátori, korrepetitori tevékenységet is végzett az Óbudai Egyetemen. A Jánossy Ferenc Szakkollégiumban tisztségviselői feladatokat lát el.

FAZEKAS Bálint

balint.fazekas@hu.bosch.com

He is a mechanical engineer and researcher specializing in constitutive modelling of largely deformable viscoelastic materials and nonlinear finite element simulations. At Bosch Hungary, he is responsible for developing new simulation methods for sealing systems and short fiber reinforced plastic parts. His work also includes static and fatigue strength analysis of e-motor components. In addition to his industrial role, he is an assistant professor at the Budapest University of Technology and Economics, where his research focuses on the mechanical modeling of rubber-like materials and fracture mechanics of polymer composites.

Okleveles gépészmérnök és kutató, szakterülete a véges alakváltozásra képes viszkoelasztikus anyagok konstitutív modellezése, valamint a nemlineáris végeselemes szimulációk. A Bosch Magyarországnál szakértőként a tömítőrendszerek és a rövid szálerősítésű polimerek szimulációs módszereinek fejlesztéséért felel. Munkája kiterjed továbbá villanymotor-alkatrészek szilárdságtani és fáradási számításaira is. Ipari tevékenysége mellett a Budapesti Műszaki és Gazdaságtudományi Egyetem adjunktusa, ahol kutatási témái közé tartozik a gumiszerű anyagok mechanikai modellezése, valamint a polimer kompozitok törésmechanikai vizsgálata.

FEHÉR Dávid János

david.janos.feher@gmail.com

I am a Chief Security Architect at a leading multinational telecommunication company, specializing in designing security systems and solutions and enhancing platform security with a focus on ISO 27001 standards. I hold a bachelor's degree in military and security engineering with a specialization in information security, a master's degree in economics specializing in business development, and an Executive MBA for IT. Additionally, I have completed a postgraduate program in engineering coaching. My certifications include Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Cloud Security Professional (CCSP), Certified Google Cloud Architect, Certified Data Privacy Solutions Engineer (CDPSE), Google Security Engineer, as well as SAFe Scrum Master and SAFe Product Owner certifications.

Chief Security Architect vagyok egy vezető multinacionális távközlési vállalatnál, ahol biztonsági rendszerek és megoldások tervezésére, valamint platformbiztonság fejlesztésére szakosodtam, különös tekintettel az ISO 27001 szabványokra. Had- és biztonságtechnikai mérnöki alapképzéssel rendelkezem információbiztonsági specializációval, vállalkozásfejlesztés szakos gazdasági mesterképzéssel, valamint IT területre szakosodott Executive MBA diplomával. Továbbá elvégeztem egy mérnöki coaching posztgraduális képzést is. Minősítéseim között szerepel a Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Cloud Security Professional (CCSP), Certified Google Cloud Architect, Certified Data Privacy Solutions Engineer (CDPSE), Google Security Engineer, valamint SAFe Scrum Master és SAFe Product Owner minősítések.

GODA Tibor János

goda.tibor@bgk.uni-obuda.hu

Prof. Dr. Tibor J. GODA is a mechanical engineer. He earned an MSc degree in 1999, specializing in machine design and mechanics of solids and a Ph.D. in 2003, specializing in numerical mechanics and tribology of polymer composites. In 2017, he earned a D.Sc from the Hungarian Academy of Sciences, specializing in contact mechanics, mechanical behavior of engineering materials and numerical modelling of dry and lubricated sliding components. Since 2022, he has been the head of the Doctoral School on Safety and Security Sciences of Obuda University.

Prof. Dr. GODA Tibor János okleveles gépészmérnök diplomáját 1999-ben géptervezés és szilárdtest mechanika szakirányon, PhD fokozatát 2003-ban polimer kompozitok numerikus mechanikája és tribológiája területen szerezte. Kontaktmechanikára, mérnöki anyagok mechanikai viselkedésére, valamint száraz és kent csúszó alkatrészek numerikus modellezésére koncentráló szakmai munkájának eredményeként 2017-ben MTA doktora címet szerzett. 2022 óta az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának vezetője.

GOMBKÖTŐ Judit

judit.gombkoto@msg-plaut.hu

Judit GOMBKÖTŐ has 25 years of experience in finance, project management, and SAP consulting in a multinational environment. She obtained her university degree at Eszterházy Károly University in Eger, where she graduated as an economist teacher. Additionally, she holds certifications in SAP Concur, SAP FI, and SAP Project Management. She is also a lecturer at Óbuda University and Budapest University of Economics and Business. Over the past ten years, she has worked at several consulting firms, gaining expertise in SAP, project management, automation, stakeholder management, and global system implementation. Prior to that, she held a leadership position at a multinational company, where she was responsible for global projects, the introduction of new programs, and global support for SAP Concur. Currently, she works as a Senior SAP Consultant at msg Plaut Hungary Kft., primarily on SAP ERP projects. Her research and professional interests include the development of enterprise resource planning (ERP) systems and the automation of business processes.

GOMBKÖTŐ Judit 25 éves pénzügyi, projektmenedzsment és SAP tanácsadói tapasztalattal rendelkezik multinacionális környezetben. Egyetemi végzettségét az Eszterházy Károly Egyetemen szerezte Egerben, ahol közgazdász tanárként végzett. Emellett SAP Concur, SAP FI és SAP Projektmenedzsment vizsgával is rendelkezik. Emellett az Óbudai Egyetem és a Budapesti Gazdaságitudományi Egyetem óraadó oktatója. Az elmúlt tíz évben több tanácsadó cégnél dolgozott, ahol SAP-val, projektmenedzsmenttel, automatizációval, stakeholder menedzsmenttel és globális rendszer implementációval kapcsolatos ismereteket szerzett. Előtte egy multinacionális vállalatnál töltött be vezetői pozíciót, ahol globális projektekért, új programok bevezetéséért és a SAP Concur globális támogatásáért volt felelős. Jelenleg a msg Plaut Hungary Kft.-nél dolgozik vezető SAP tanácsadóként, elsősorban SAP ERP projekteken. Kutatási és szakmai érdeklődési területei közé tartozik a vállalatirányítási rendszerek fejlesztése, az üzleti folyamatok automatizálása.

HUSZÁK Csenge

huszak.csenge@bgk.uni-obuda.hu

Csenge HUSZÁK is a departmental engineer at the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering. She obtained her bachelor's degree in mechanical engineering at Óbuda University and continued her studies at the Budapest University of Technology and Economics. Currently, she is a student at the Doctoral School of Safety and Security Sciences at Óbuda University. Her research area is metal-

HUSZÁK Csenge az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi gyakornoka. Gépészmérnöki alapdiplomáját az Óbudai Egyetemen szerezte, tanulmányait a Budapesti Műszaki és Gazdaságtudományi Egyetemen folytatta. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori iskolájának hallgatója. Kutatási területe a metallográfia, a hegesztett anyagok és szerkezetek.

lography and welded structures. During her doctoral research, she is working on developing the requirement system for safety-critical components.

Doktori kutatása során a biztonságkritikus komponensek követelményrendszerének kidolgozásával foglalkozik.

KISS Csaba

kiss.csaba@uni-nke.hu

Csaba KISS is a doctoral student at the Doctoral School of Military Engineering of the National Public Service University. He completed his studies in the Soviet Union at the Ulyanovsk Military Journalism University, where he graduated in 1986. In the last year of university, he graduated as a Russian military interpreter. During his years of service in the Hungarian Army from 1986 to 1996, he completed a Civil Service Officer course and obtained the "C" type intermediate level language exam with the addition of the military vocational test in German. From 1996, he worked at the Education Directorate of the Hungarian Telecommunications Company (MATÁV) in the Transmission Technology Department of the Technical Department. After obtaining his teacher's qualification, he taught technical subjects. In addition to the technical courses, he also obtained a trainer's qualification, so he held various skill-building and team-building trainings. During the trainings, he used his self-developed skills development program for the computer (Octopus-32). In 2010, he won 2nd place with his skills development software in the "smart software" competition at the European level announced by the LUDUS project.

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

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR is a communications engineer, certified communications specialist, electronic information security manager, doctor of economics (PhD), and doctor (PhD) and habilitated doctor (Dr. habil.) in military engineering. He is also a cybernetics consultant, coach, and mediator. His research interests include the social aspects and economic impacts of the digital age, with a particular focus on the human aspects of information security, information security awareness, human-robot interaction, smart cities, artificial intelligence, social credit systems, and domotics. He is a senior research fellow at Óbuda University, where he leads the specialized courses for Domotics Engineer/Consultant and Facility and Property Professional Engineer/Manager. He is also the head of the Artificial Intelligence Workshop and serves as the scientific secretary of the Editorial Board of the Safety and Security Sciences Review, which is classified by the Military Science

KOLLÁR Csaba kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), a katonai műszaki tudományok doktora (PhD) és habilitált doktora (Dr. habil.), kibernetikus, tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere, az intelligens épületek (domotika rendszerek) üzemeltetése és gazdálkodása. Az Óbudai Egyetem tudományos főmunkatársa, a domotika szakmérnök/szaktanácsadó és a létesítménygazdálkodó és -üzemeltető szakmérnök/szakmenedzser továbbképzési szakok képzésvezetője, a Mesterséges Intelligencia Műhely vezetője, az MTA IX. Osztály Hadtudományi Bizottsága által minősített Biztonságtudományi Szemle szerkesztőbi-

Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences. Csaba KOLLÁR is an expert with the Hungarian Society of Military Science and the National Association of Human Professionals, and has been a member of the Artificial Intelligence Consortium since Q4 2018.

zottságának tudományos titkára, az Egyetem Biztonságtudományi Doktori Iskolájának és a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának az oktatója, témavezetője. A Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

KOVÁCS Tünde Anna

kovacs.tunde@bgk.uni-obuda.hu

Prof. Dr Tünde Anna KOVÁCS is a full professor in the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Hungary. Member of the editorial board of the Acta Materialia Transylvania, Safety and Security Sciences Review and Security Engineering of Anthropogenic Objects. Her research interests are in materials science and technologies, as well as unique welding processes (ultrasonic and explosive welding). She is an International Welder Engineer (IWE), welder robots and collaborative welding robotics. She is a supervisor in the Doctoral School on Materials and Technologies of the Óbuda University and the Doctoral School on Safety and Security Sciences, Hungary. Author and co-author of numerous scientific publications. Member in several research projects and supervisor of doctoral students.

Prof. Dr. KOVÁCS Tünde Anna az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi tanára. Tagja az Acta Materialia Transylvania, a Biztonságtudományi Szemle, az Antropogén Objektumok Mérnöki Biztonsága folyóiratok szerkesztő bizottságának. Kutatási területe az anyagtudomány és technológia területén a különleges hegesztési eljárások (ultrahangos és robbantásos hegesztés), nemzetközi hegesztőmérnökként (IWE), hegesztő robotok és collaborative robothegesztés. Témavezetőként dolgozik az Anyagtudományok és Technológiák, valamint a Biztonságtudományi Doktori iskoláknál. Számos tudományos publikáció szerzője és társszerzője. Tagja kutatási projekteknek és doktori témák témavezetője.

KREPUSKA András István

andras.krepuska@zknet.hu

András István KREPUSKA, he is security engineer MSc and electric engineer. He studied at Budapest Tech Polytechnical Institution and Óbuda University. Since 2006 works as a designer of fire alarm and fire extinguish systems. CEO of ZKNet Kft. and technical director of Ökodómusz Hungária Kft. In his doctoral research, he examines the obsolescence of fire protection systems. He is a regular fire protection system design course instructor and a multiple invited speaker at the Fire Protection Professional Day at Lakitelek.

KREPUSKA András István okleveles biztonságtechnikai mérnök, villamosmérnök. Budapesti Műszaki Főiskolán, valamint az Óbudai egyetemen végezte tanulmányait. 2006 óta foglalkozik beépített tűzjelző és tűzoltó rendszerek rendszerek tervezésével. A ZKNet Kft. ügyvezetője, valamint az Ökodómusz Hungária Kft. műszaki igazgatója. Doktori kutatásában a tűzvédelmi rendszerek avulását vizsgálja. Rendszeres oktatója tűzoltórendszer tervezői tanfolyamoknak, valamint többszörös meghívott előadója a lakitelki tűzvédelmi szakmai napnak.

MÁRTON Zoltán

marton.zoltan@uni-obuda.hu

Zoltan MARTON is the head of the STEAM Office at Obuda University and serves as the Platform Coordinator of the Hungarian STEM Platform. He holds degrees in safety technology engineering and engineering education, and he is currently pursuing his PhD in Doctoral Shool of Safety and Security Sciences at Obuda University. His professional and research focus

MÁRTON Zoltán az Óbudai Egyetem STEAM Irodájának vezetője és a Magyarországi STEM Platform koordinátora. Biztonságtechnikai mérnöki és mérnökpedagógiai diplomával rendelkezik, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában hallgató. Szakmai és kutatási fókuszában a STEAM-alapú tananyagfejlesztés, a kibertér-alapú

centers on STEAM-based curriculum development, skill-building for cyberspace-based protection strategies, and innovative, digitally supported teaching methods. He has been actively involved in coordinating and leading several international projects, including Erasmus+ and Horizon Europe initiatives and projects focused on digital skills, STEAM education, and gamified learning experiences. Through these roles, he contributes to advancing interactive and safety-focused educational content in Hungary and beyond.

védelmi stratégiák készségfejlesztése és az innovatív, digitálisan támogatott oktatási módszerek állnak. Aktívan részt vett több nemzetközi projekt koordinálásában és vezetésében, többek között Erasmus+ és Horizon Europe kezdeményezésekben és a digitális készségekre, a STEAM-oktatásra és a játékosított tanulási tapasztalatokra összpontosító projektekben. E szerepkörök révén hozzájárul az interaktív és biztonságközpontú oktatási tartalmak fejlesztéséhez Magyarországon és azon túl is.

NAGY Rudolf

nagy.rudolf@uni-obuda.hu

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

Dr. habil. NAGY Rudolf nyugalmazott tűzoltó ezredes, jelenleg az Óbudai Egyetem adjunktusa. Külföldi oktatási intézményekben tanult. Vegyivédelmi tisztként szolgált, és részt vett iparbiztonsági feladatokban. A NATO SFOR misszióban műveleti tisztként szerzett tapasztalatokat. Ezt követően az 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. 2015 óta oktatja a biztonságtudományok tantárgyakat, a tűzvédelmi mérnöki specializáció felelőse. Habilitált doktori címet szerzett az öngyulladások tudományos vizsgálatából.

PETŐ Richárd

peto.richard@bgk.uni-obuda.hu

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

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

PINKE Péter

pinke.peter@bgk.uni-obuda.hu

Dr. Péter PINKE is an associate professor in the Department of Materials Technology at the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, Hungary. Member of the editorial board of the Acta Materialia Transylvanica. His scientific activities focus on materials science, physical metallurgy and the investigation of the limit states of materials. He has participated in several scientific research pro-

Dr. PINKE Péter az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi docense. Tagja az Acta Materialia Transylvanica folyóirat szerkesztő bizottságának. Tudományos tevékenysége az anyagtudományra, a fizikai metallurgiára és az anyagok határállapotainak vizsgálatára fókuszál. Több tudományos kutatásban is részt vett, amelyek

jects aimed at the investigation of the properties of steels and non-ferrous alloys. His areas of expertise include heat treatment, mechanical material testing, and the investigation of the microstructure of metals and alloys. He is a supervisor in the Doctoral School on Materials and Technologies of the Óbuda University and the Doctoral School on Safety and Security Sciences, Hungary.

acélok és nemvasfém ötvözetek tulajdonságvizsgálatára irányultak. Szakterülete a hőkezelés, a mechanikai anyagvizsgálatok, valamint fémek és ötvözetek mikroszerkezetének vizsgálata. Témavezetőként dolgozik az Anyagtudományok és Technológiák, valamint a Biztonságtudományi Doktori iskoláknál.

POLAT, Mehmet Alican

mehmet.alicanpolat@uni-obuda.hu

Mehmet Alican POLAT was born in Turkey, where he completed his bachelor's degree in chemical engineering. During his undergraduate studies, he participated in exchange programs and had the opportunity to study at universities across various European countries. He later pursued his master's degree at the Budapest University of Technology and Economics with the support of the Stipendium Hungaricum scholarship. Mehmet deeply appreciates Budapest and has a strong interest in materials and their mechanisms. He is also passionate about explosion safety. As hydrogen has become a priority area for the European Commission and funding opportunities continue to grow, he decided to focus his research on Hydrogen Fuel Station Safety. He is a PhD student at Óbuda University, Doctoral School on Safety and Security Sciences, specialising in Safety Science with a focus on Hydrogen Safety.

Mehmet Alican POLAT Törökországban született, ahol vegyészmérnöki diplomát szerzett. Az egyetemi tanulmányai során csereprogramokban vett részt, és lehetősége volt különböző európai országok egyetemein tanulni. Később a Stipendium Hungaricum ösztöndíj támogatásával a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerzett mesterdiplomát. Mehmet nagyon kedveli Budapestet, és erősen érdeklődik az anyagok és azok mechanizmusai iránt. Emellett szenvedélyesen érdeklődik a robbanásbiztonság iránt. Mivel a hidrogén az Európai Bizottság számára kiemelt területté vált, és a finanszírozási lehetőségek folyamatosan nőnek, úgy döntött, hogy kutatásait a hidrogén üzemanyagtöltő állomások biztonságára összpontosítja. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója, szakterülete a biztonságtudomány, különös tekintettel a hidrogénbiztonságra.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Prof. Dr. Zoltán RAJNAI is currently the National Cyber Coordinator of Hungary and professor at the Obuda University. Previously Dr. Rajnai served as Colonel in Hungarian Defense Forces (1981-2013) and was professor at the National Defense University in the field of Information, info-communication, and telecommunication systems (1993-2013). Since 2013, Dr. Rajnai also is the Dean of faculty of Mechanical and Safety Engineering, Head of Doctoral School on Safety and Security Sciences with main responsibilities in the field of Cyber Security, Information Security, info-communication, and telecommunication systems. Dr. Rajnai received education from the High School at the Hungarian Defense Forces (1981-1985), the Military Academy (1990-1993), the Doctoral School on Military Sciences (1997-2000), and the Joint Security College- Paris, France (2003-2004).

Prof. Dr. RAJNAI Zoltán Magyarország nemzeti kiberkoordinátora, az Óbudai Egyetem professzora, 2015-tól az Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának dékánja. A Biztonságtudományi Doktori Iskola alapítója, vezetője, kutatási területe a kiberbiztonság, az információbiztonság, az infokommunikáció és a távközlési rendszerek fejlesztése. Korábban (1981–2013) ezredesként szolgált a Magyar Honvédségben, 1993–2013 között a Zrínyi Miklós Nemzetvédelmi Egyetem tanáraként fő szakterülete az információs, kommunikációs és távközlési rendszerek szervezése és azok biztonsága volt. Rajnai professzor a katonai főiskolai és egyetemi tanulmányait követően a Hadtudományi Doktori Iskolában (1997–2000) és a párizsi Összhaderőnemi Védelmi Kollégiumban (Collège Interarmées de Défense – CID) tanult.

SÁNTA Róbert

santar@uniduna.hu

I am Dr. habil. Róbert SÁNTA, Associate Professor with over 20 years of experience in renewable energy research, focusing primarily on the mathematical modeling and optimization of heat pump systems and heat exchangers. My research places a strong emphasis on two-phase flow phenomena and the accurate description of both steady-state and transient thermal processes. I have published extensively and participated in numerous national and international projects, especially in the fields of industrial applications and energy efficiency. My goal is to contribute to the advancement of sustainable technologies through both theoretical and practical innovation.

Dr. habil. SÁNTA Róbert vagyok, egyetemi docens, több mint 20 éve foglalkozom megújuló energiák, különösen a hőszivattyús rendszerek és hőcserélők matematikai modellezésével és optimalizálásával. Kutatásaim során kiemelt figyelmet fordítok a kétfázisú áramlások, valamint a statikus és tranziens hőtani folyamatok pontos leírására. Számos hazai és nemzetközi publikációval, valamint kutatási projekttel rendelkezem, különösen az ipari alkalmazások és az energiahatékonyság növelése terén. Célom, hogy a fenntartható technológiák fejlesztéséhez hozzájáruljak mind elméleti, mind gyakorlati szinten.

SÁRI-BARNÁCZ Viktor

viktor.sari@hu.bosch.com

He is a mechanical engineer with over 11 years of experience in product development and applied industrial research. He currently works as a lead expert at Bosch Hungary, where his main responsibilities include the analysis of critical mechanical and mechatronic failures, coordination of related research projects, and strategic development of engineering methodologies. He is also a Bosch certified DRBDM L4 engineering method expert. His focus lies in function-based and model-based engineering, with special interest in tribology, thermal-mechanical interfaces, and failure modeling.

Okleveles gépészmérnök, több mint 11 éves termékfejlesztési és alkalmazott ipari kutatási tapasztalattal. Jelenleg a Bosch Magyarország vezető szakértőjeként dolgozik, főbb feladatai közé tartozik a kritikus gépészeti és mechatronikai meghibásodások elemzése, kapcsolódó kutatási projektek koordinálása, valamint mérnöki módszertanok stratégiai fejlesztése. Emellett Bosch DRBFM L4 szintű módszertani szakértő. Szakmai fókuszában a funkcióalapú és modellalapú mérnöki megközelítések állnak, különös tekintettel a tribológiára, thermo-mechanikai problémákra és meghibásodások analitikus modellezésére.

ZÓNAI Viktor

zonai.viktor@uni-obuda.hu

My name is Viktor ZÓNAI. I am a certified mechanical engineer specialized in building services and process engineering, managing director of ThermoSun Ltd., and a PhD student at the Doctoral School of Safety and Security Sciences at Óbuda University. My research focuses on the energy analysis of ground source heat pump systems, with particular attention to their efficiency and environmental sustainability. My goal is to improve the performance of low carbon heating systems. I also teach energy and building services engineering subjects at the University of Dunaújváros. I have published several scientific papers on the optimization of HVAC systems. I am a member of the Hungarian Chamber of Engineers, holding professional licenses for design and technical supervision. I have more than ten years of experience in the design and implementation of thermal engineering systems.

ZÓNAI Viktor vagyok, okleveles épületgépészeti és eljárástechnikai gépészmérnök, a ThermoSun Kft. cégvezetője, valamint doktorandusz az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában. Kutatási területem a talajszondás hőszivattyús rendszerek energetikai vizsgálata, különösösen azok hatékonyságára és környezeti fenntarthatóságára fókuszálva. Célom az alacsony szén-dioxid-kibocsátású hőellátó rendszerek teljesítményének növelése. Oktatási tevékenységet folytatok a Dunaújvárosi Egyetemen energetikai és épületgépészeti tárgyakban. Több tudományos publikációm jelent meg az épületgépészeti rendszerek optimalizálása témájában. Tagja vagyok a Magyar Mérnöki Kamarának, tervezői és műszaki ellenőri jogosultsággal. Több mint tízéves tapasztalattal rendelkezem hőtechnikai rendszerek tervezésében és kivitelezésében.

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

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

BORS Györgyi

borsgyorgyi77@gmail.com

She was born in 1977 in Tapolca, Hungary. The tragic early death of his mother was decisive in her life because she was then raised in state care until she was 18 years old. During her years there, she realized that she found the greatest pleasure in art. She studied graphic art for several years at the Railway School of Music and Fine Arts in Budapest with the painter and sculptor György BENEDEK, and later with Árpád "Pika" NAGY and Zoltán SEBESTYÉN. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán GASZTONYI, from whom she learned the different techniques of oil painting. She is narrative painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött rá, hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában BENEDEK György festő és szobrászművésznél, majd később NAGY Árpád „Pika"-nál és SEBESTYÉN Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere GASZTONYI Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

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

Vol 7, No 2, 2025. | 2025. VII. évf. 2. szám

CONTENT | TARTALOM

Material Safety column | Anyagbiztonság rovat

Security Systems column | Biztonságtechnika rovat

War Security and Law Enforcement column | Hadbiztonság és rendvédelem rovat

Information Security column | Információbiztonság rovat

Industrial and Operational Safety column | Ipar- és üzembiztonság rovat

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.2025.7.2.1

REVIEW OF HYDROGEN PROPERTIES, PRODUCTION, STORAGE, LOGISTICS, AND SAFETY CRITERIA

A HIDROGÉN TULAJDONSÁGAINAK, ELŐÁLLÍTÁSÁNAK, TÁROLÁSÁNAK, LOGISZTIKÁJÁNAK ÉS BIZTONSÁGI KRITÉRIUMAINAK ÁTTEKINTÉSE

POLAT Mehmet Alican[1], KOVÁCS Tünde Anna[2]

Abstract

While the physical and chemical properties of hydrogen make it an excellent energy carrier and an alternative solution to carbon-based energy sources, its colourless, odourless nature, low ignition energy, reversible Joule-Thompson effect, susceptibility to Boiling Liquid Expanding Vapor Explosion (BLEVE) and rapid phase transition (RPT) physical explosions, hydrogen damage, and hydrogen embrittlement reveal characteristics that complicate its production, storage, logistics, and pose challenges to safety in end-user applications. This study explores both the advantages and disadvantages presented by hydrogen's physical and chemical properties, discussing its production, storage, logistics, and overall economic aspects. Furthermore, it emphasises the essential safety standards that must be considered in handling hydrogen throughout these processes.

Keywords

hydrogen, green hydrogen, metal hydrides, hydrogen damages, embrittlement

Absztrakt

Míg a hidrogént fizikai és kémiai tulajdonságai kiváló energiahordozóvá és a szénalapú energiahordozók alternatívájává teszik, színtelen, szagtalan természete, alacsony gyulladási energiája, reverzibilis Joule-Thompson-effektusa, forrásban lévő folyadékot kitágító gőzrobbanásra és a gyors fázisátalakulás okozta fizikai robbanásokra való érzékenysége, a hidrogén betegséget és hidrogén ridegedést okozó hatásai, megnehezítik a hidrogén előállítását, tárolását, logisztikáját, és kihívást jelentenek a végfelhasználói alkalmazások biztonsága szempontjából. Ez a tanulmány a hidrogén fizikai és kémiai tulajdonságaiból adódó előnyöket és hátrányokat vizsgálja, kitérve a hidrogén előállítására, tárolására, ennek logisztikájára és általános gazdasági szempontjaira. A tanulmány továbbá a hidrogén kezelésénél figyelembe veendő alapvető biztonsági előírások hangsúlyozásával zárul, amelyeket e folyamatok során végig figyelembe kell venni.

Kulcsszavak

hidrogén, zöld hidrogén, fémhidridek, hidrogén betegség, ridegedés

[1] mehmet.alicanpolat@uni-obuda.hu | ORCID: 0009-0008-7322-9697 | PhD student, Óbuda Uniersity Doctoral School on Safety and Security ScienceS| PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kovacs.tunde@bgk.uni-obuda.hu| ORCID: 0000-0002-5867-5882| professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering| egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

The increasing population and the rising increase in energy demand are unquestionable. As humanity continues to elevate its luxuries daily, the energy need is escalating day by day like never before (Figure 1.) [1].

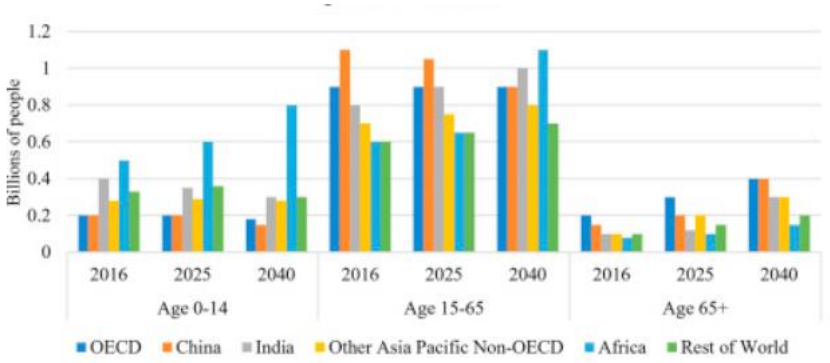


Figure 1: Population Increase of the World in different age groups [1]

The increasing demand for energy raises the carbon footprint from energy consumption (Figure 2.). This extraordinary energy need also leads to a global increase in CO_2 concentration. Efforts worldwide to promote and use alternative energies aim to reduce emissions of non-renewable gases and help decrease our footprint on this planet. However, new energy fields occasionally emerge due to technological advances and growing human luxuries, with ongoing studies in areas such as hydrogen.

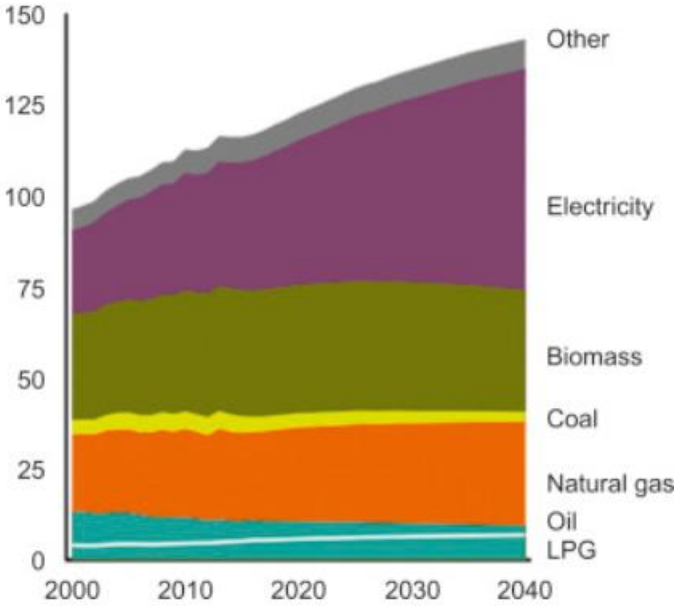


Figure 2. Increase in the consumption of the various energy fuels in the world by 2040 [1]

HYDROGEN

Hydrogen has become one of the most widely used chemicals globally because of its high energy density, lightweight, and clean burning characteristics of it. Some of the sectors that hydrogen is used the most are the chemical, refinery, metallurgy, food, glass, and electronic industries. Moreover, the high energy density, meaning high energy per unit mass, and the emission of only water vapour have fastened increased academic studies in recent years [2]. The aim of these studies is to reduce carbon emissions and enhance the calorific value of other energy sources, such as natural gas. Hydrogen is in molecular form in its natural form. It is a colourless, tasteless, and odourless gas. It can be changed from a gas to a liquid state at -252°C. It can dissolve in water and alcohol. It is the least dense gas with a density of 0.08999 g/L. The energy required for converting molecular hydrogen to atomic hydrogen is approximately 435 kJ/mol. Atomic hydrogen is highly reactive, and it can create covalent or ionic bonds with other atoms. During this formation, it follows the duet rule rather than the octet rule. In its molecular state, hydrogen exists as either para or ortho hydrogen. At -273°C, the ratio of para-hydrogen is higher. The bonding of hydrogen atoms in a hydrogen molecule changes its physical properties [3]. Hydrogen is the lightest, simplest element, quickly forming combinations with other elements, and it is the most abundant element on Earth. However, it's essential to note that hydrogen is not a primary energy source; it exists in compound states with other elements, such as oxygen in water, carbon, nitrogen, and fossil fuels. This circumstance allows hydrogen to function as an energy carrier [4]. The need for hydrogen in various sectors over the years is projected to increase, and it is estimated that the demand will go up to 519 million metric cubic meters by the year 2070. Figure 3 projects this growth in different sectors [5].

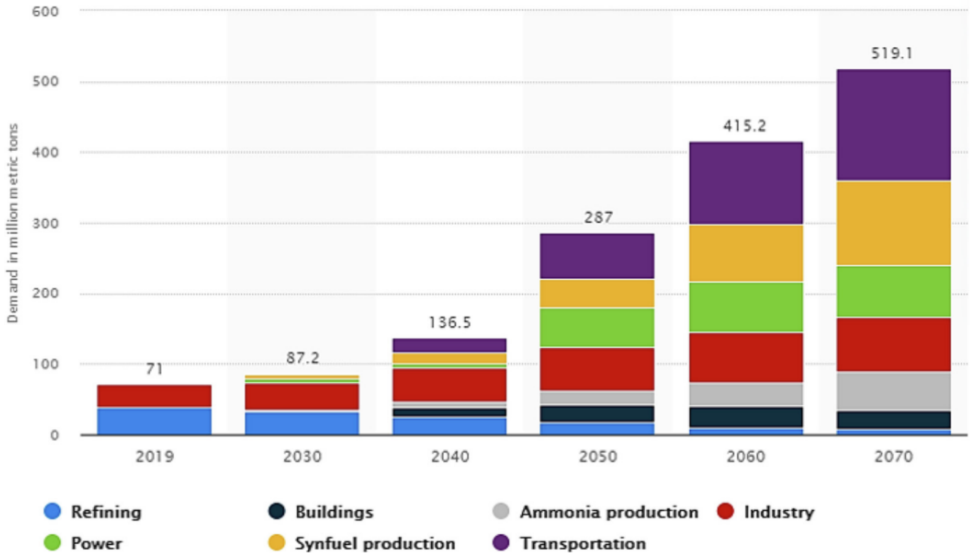


Figure 3: From 2019 to 2070, H_2 demand forecast [5]

In addition to the advantages of hydrogen, there are disadvantages that lead to the research and efforts worldwide to get focused. One of the points that makes hydrogen an ideal fuel is its high combustion energy release, but this feature, combined with its ability

to be stored at high pressures, also brings up safety concerns due to the low ignition energy of hydrogen. The hydrogen density in different storage methods can be seen in Table 1 [6].

Storage form	Energy density		Density (kg/m^3)
	kJ/kg	MJ/m^3	
Hydrogen gas (0.1 MPa)	120,000	10	0.090
Hydrogen gas (20 MPa)	120,000	1900	15.9
Hydrogen gas (30 MPa)	120,000	2700	22.5
Hydrogen liquid	120,000	8700	71.9
Hydrogen in metal hydrides	2000–9000	5000–15,000	–
Hydrogen in metal hydrides typical	2100	11,450	5480
Methane (natural gas) at 0.1 MPa	56,000	37.4	0.668
Methanol	21,000	17,000	0.79
Ethanol	28,000	22,000	0.79

Table 1. Energy density by weight, volume, and mass density for various hydrogen forms.

HYDROGEN PRODUCTION

Hydrogen can be produced with many methods, such as steam reforming, partial oxidation, methane pyrolysis, coal gasification, and electrolysis. A significant portion of hydrogen production these days comes from steam reforming and coal gasification; these two techniques cover almost the entire production of Hydrogen in the world. The production of hydrogen from natural gas or coal is referred to as grey hydrogen. The distinction between grey hydrogen and blue hydrogen lies in the absence of carbon capture and storage in grey hydrogen production. In blue hydrogen, the process includes decarbonisation technology for the emitted CO_2. Green hydrogen is produced through water electrolysis. To mitigate carbon emissions, increasing the production of green hydrogen is essential. Figure 4 provides a schematic overview of hydrogen production techniques.

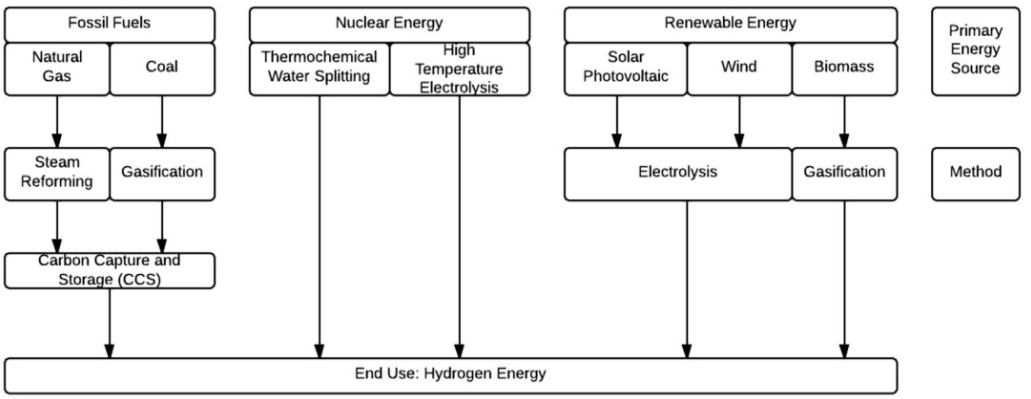


Figure 4: Hydrogen Production Methods [4]

As can be seen, alternative energy sources such as solar energy and wind turbines can be used to produce green hydrogen. The important fact here is the ability to integrate alternative energy with hydrogen production.

Steam Reforming of Natural Gas is still the most widely used technique among these techniques today. Petroleum Recovery and Refining is the most common application of hydrogen use today. Table 2 illustrates the technology of different hydrogen methods, the energy source used in this technique, the resulting product, the production cost, and the carbon emission value [5, 7].

Hydrogen Color	Technology	Source	Products	Cost ($ kg/H_2)	CO_2 emissions
Brown Hydrogen	Gasification	Brown coal (Lignite)	$H_2 + CO_2$	1.2–2.1	High
Black Hydrogen	Gasification	Black coal (Bituminous)	$H_2 + CO_2$	1.2–2.1	High
Grey Hydrogen	Reforming	Natural gas	$H_2 + CO_2$ (Released)	1–2.1	Medium
Blue Hydrogen	Reforming + carbon capture	Natural gas	$H_2 + CO_2$ (Captured 85-95%)	1.5–2.9	Low
Green Hydrogen	Electrolysis	Water	$H_2 + O_2$	3.6–5.8	Minimal

Table 2. Energy density by weight, volume, and mass density for various hydrogen forms [5]

Steam Reforming

Steam reforming is still the most widely used method for hydrogen production. The process basically involves the conversion of fossil fuel (methane) into CO and H_2 at temperatures of 700-900 °C of water steam, and 3-35 bars of pressure, using a nickel catalyst (Figure 5).

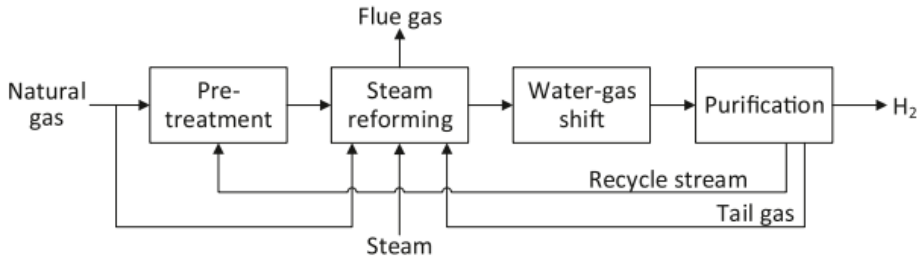


Figure 5: Primary Process Steps of Hydrogen production by steam methane reforming *[8]*

$$CH_4 + H_2O \leftrightarrow 3H_2 + CO \quad (1)$$

$$CO + H_2O \leftrightarrow H_2 + CO_2 \quad (2)$$

Coal Gasification

As Natural gas, coal is also easily accessible, and it is known as being cheap. The production of hydrogen by gasification of coal can be a bit more expensive compared to

natural gas steam. Even though it is cheap as a raw material, the technology itself can be more expensive [9].

The process of coal gasification basically involves the partial oxidation of coal with steam at high temperature and pressure. CO and H_2 are produced at the end of the reaction as a result. CO is later again reacted with steam, which leads the production of H_2 and, additional CO_2. One significant problem of this technique is the high level of CO_2 emissions. Therefore, day by day, Carbon Capturing technologies are advancing to address this concern.

$$3C + O_2 + H_2O \rightarrow H_2 + 3CO \tag{3}$$

$$CO + H_2O \rightarrow CO_2 + H_2 \tag{4}$$

Electrolysis

Electrolysis is an electrochemical separation method of hydrogen and oxygen using electrical energy applied to water. This method has become one of the most researched hydrogen separation techniques in recent years, primarily used to obtain green hydrogen since it is entirely carbon-free.

$$1\ H_2O + Electricity\ (237.2\ kJmol^{-1}) + Heat\ (kJmol^{-1}) \rightarrow H_2 + \frac{1}{2}O_2 \tag{5}$$

Cathode: $$2H_2O + 2e^- \rightarrow H_2 + 2OH^- \tag{6}$$

Anode: $$2OH^- \rightarrow \frac{1}{2}O_2 + H_2O + 2e^- \tag{7}$$

Equation 3-5. needs cell voltage of 1.23 V to achieve the separation of water into oxygen and hydrogen, 0.4 V is needed for oxidation and 0.83 V is for reduction. However, an effective cell voltage of 1.48 V is needed for efficient water electrolysis. Even though water electrolysis is well-known technology for a long time currently only 4% of hydrogen can be obtained from water. The four well know technology of electrolysis are Alkaline Water Electrolysis, Anion Exchange Membrane Electrolysis, Proton Exchange Membrane Electrolysis, and Solid Oxide Water Electrolysis. These electrolysis methods are distinguished based on their working principles, the electrolyte used, and the ionic agents (OH^-, H^+, O^{-2}) employed. Each technology has its own advantages and disadvantages [7].

HYDROGEN STORAGE

Hydrogen storage technology can be categorized based on factors such as pressure, temperature, safety criteria, energy density, and volume. Depends on the types of hydrogen storage, the physical or chemical properties of hydrogen can change. Hydrogen can be stored as molecular form as a liquid or gas, or it can be adsorbed to the materials through very light van der Waals bonds. Atomic hydrogen also can be absorbed chemically into metal hydrides. Figure 6 illustrates different storage types both physically and chemically.

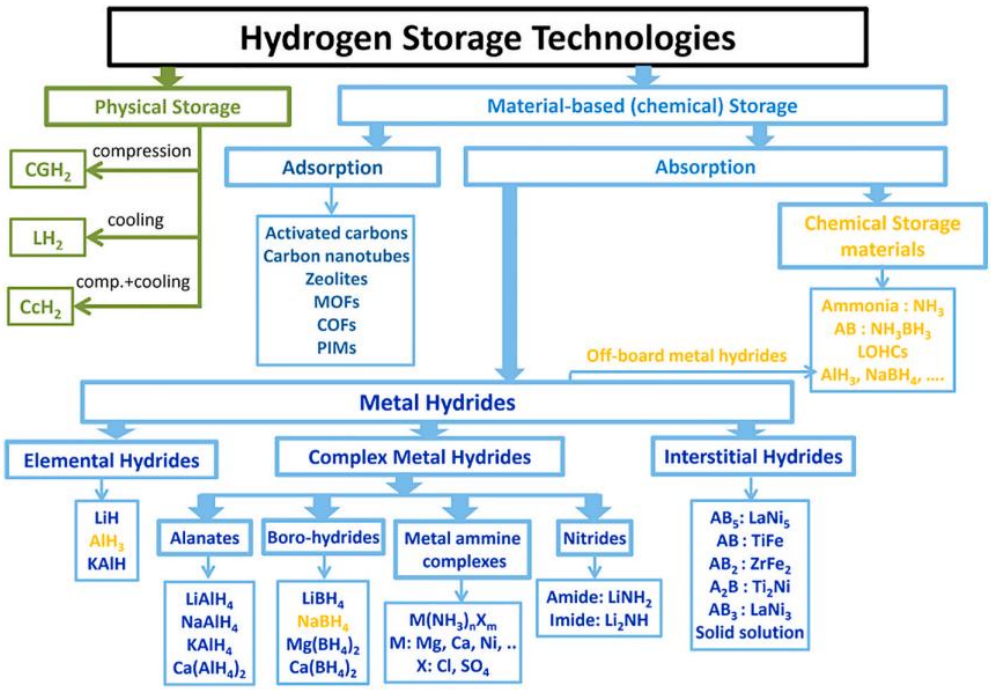


Figure 6: Hydrogen Storage Technologies [10]

Taking LPG as an example, the liquefaction of propane occurs at around -42°C or at pressures of approximately 2-3 bar. LPG tanks in cars are typically made of steel with a thickness of 3-4 mm, and the material of the tank, which operates at around 7 bars inside the car, is not critically essential. Similarly, natural gas can be compressed as a gas at pressures of 200-250 bar at 20°C, or it can be liquefied by cooling down to -162°C at atmospheric pressure. When stored in liquid form, natural gas occupies twice the volume compared to its gaseous state.

The literature explores various storage methods for hydrogen, as hydrogen gas storage requires reaching pressures up to 800 bars. Studies are conducted to reduce this pressure or to develop materials capable of withstanding such pressure.

Compressed Hydrogen

Compressed Hydrogen is a method of storing hydrogen in gas form at high pressure. This technique is still the most used in the world and can increase the density of hydrogen from 0.1 g/L to up to 40 g/L by pressurizing hydrogen to 700 bars from 1 bar [10].

To go up to these pressures and withstand these intense pressures, materials need to be designed accordingly. The material design options are metallic (1), metal with fiber resin (2), carbon fiber composite (3), composite (4), space-filling skeletons (5). And the pressures they can handle are approximately 30, 100, 450, 700, and 800 bars, respectively [11]. As is evident, a tank going up to these pressures to store hydrogen in a car will

always cause safety concerns, and these safety considerations should always be kept in mind.

Liquid Hydrogen

Storing a substance in liquid form is more advantageous in terms of volume. When hydrogen is liquefied at -253 °C, it becomes highly advantageous in volume. However, issues such as temperature insulation arise in this type of storage, and current research is focused on minimising hydrogen efficiency losses and developing lightweight and stronger composite tanks capable of isolating temperature [12].

Material-Based Hydrogen Storage

Metal-based hydrogen storage is based on the principles of either adsorption or absorption of hydrogen. The varying parameters in these two techniques depend on the energy required for hydrogen to be adsorbed or absorbed by the metal and the energy and temperature needed during desorption. The advantages and disadvantages of metal-based storage generally revolve around these principles. Adsorption is on the van der Waals bonds formed between molecular hydrogen and the material, leveraging selected materials' large, based surface area. On the other hand, absorption technology utilizes ionic, covalent, and complex hybrids for hydrogen storage and relies on the principles of both storing and desorbing hydrogen during separation [10].

One of the examples of these techniques is ammonia. While ammonia is the second-most-produced chemical in the world, it can be found in liquid form, not too far from atmospheric temperature and pressure. It can be changed to hydrogen under the same parameters. While this technology is advantageous for not causing CO_2 emissions, it faces some economic uncertainties considering the conversion expenditures [12].

Metal hydrides, on the other hand, are advantageous because they can absorb and release hydrogen at room temperature. However, the economic viability of metal hydride technology varies depending on the materials' structure.

The required amount of hydrogen for a regular car to cover 400-500 km is 5-8 kg [13]. The Metal Hydride tank needed to store this amount of hydrogen weighs around 500-600 kg, creating a weight disadvantage for cars.

Figure 7 indicates that an economic comparison has been made among different storage types in terms of storage, transportation, and conversion [14]. Even though NH3 is very advantageous and can store much hydrogen compared to other storage techniques, the conversion rate is very expensive. We can decide which storage method is needed depending on the usage area of hydrogen and logistical values (such as how long it will be transported, etc.). For example, ammonia can be advantageous for long distances as it has low transportation costs.

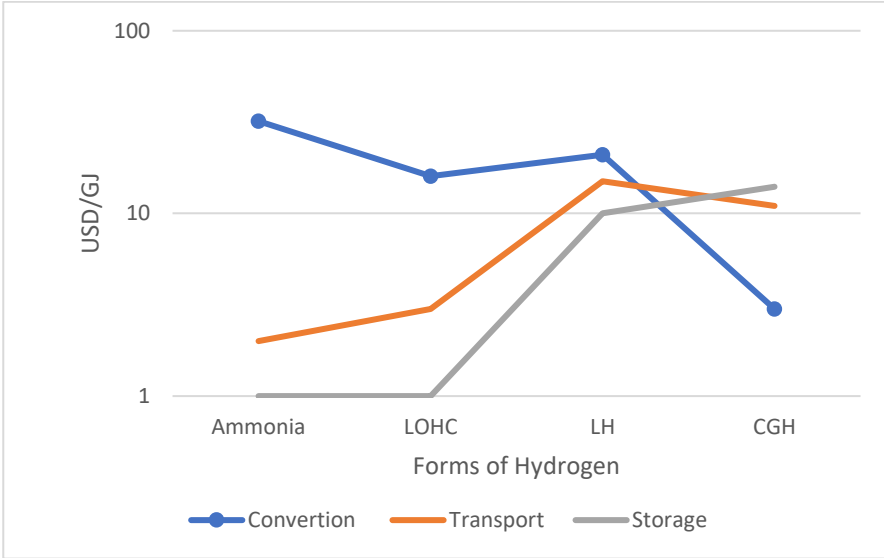


Figure 7: Cost of hydrogen value chains

As you can see from the storage methods, even though new materials are being studied or improved to keep the pressure low or the temperature near room temperature, most of the hydrogen is still being stored using conventional methods, which are physical storage.

HYDROGEN TRANSPORTATION

Hydrogen transportation can be done by road, railway, and ship. These transportation methods include compressed or liquefied hydrogen by roads, compressed hydrogen by pipeline, and compressed, liquid, ammonia or liquid organic hydrogen carriers from hydrogen by ships. Each has advantages and disadvantages depending on the distance, weight, or volume. Figure 8. shows the transportation techniques briefly [15].

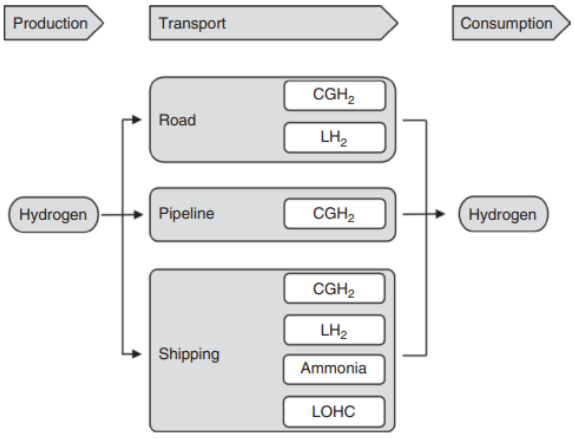


Figure 8: Hydrogen Transportation Methods [15]

Pipeline Transportation

Hydrogen transportation by pipes might be very advantageous in terms of economics and by volume if the high amount of hydrogen transportation is the topic, but embrittlement of hydrogen, permeation and leaks and the cost that can protect from these problems are the point of question. It is well known that hydrogen is very small, and the diffusion efficiency of hydrogen is 4 times higher than natural gas; therefore, the components of pipelines must be designed for this purpose [15]. The transportation distance can go up to hundreds of km and there are examples of these all around the world, especially from source to end users, but meanwhile pressure goes up to 100 bar, meaning all the mentioned safety problems are being raised as a question [16].

Road Transportation

Road transportation allows gaseous and liquid hydrogen to be carried. The gaseous hydrogen can be carried in vessels, can be filled in a production plant and carried to the end user, and empty bottles can be changed there. 200 to 1000 kgs of Hydrogen can be carried with 200 to 500 bar pressure, but this has limitations, for example, in the USA, the maximum is 250 bars. It can also be carried in Liquid form; it has advantages when it comes to volumetric storage density, around 4000 kg of hydrogen can be carried at -253°C with cryogenic tanks [15].

This high pressure for compressed hydrogen brings limitations all around the world, safety issues are big concern, therefore the distance, speed, volume and even acceleration or brakes of the truck should be considered. And we should not forget that these applications are advantageous only for short and middle range of transportation.

Ship Transport

Hydrogen can be transported by ships in compressed, liquid or ammonia form. For compressed form, again, high pressure for the cylinders will be needed. For liquid form cryogenic technologies, a low temperature will be needed. One advantageous carry method by ships is in the compound form as ammonia. -33°C and 8 to 10 bar pressure are the parameters of ammonia transportation, which is promising in terms of safety and brings this method up considering the safety criteria (Figure 9, 10) [17].

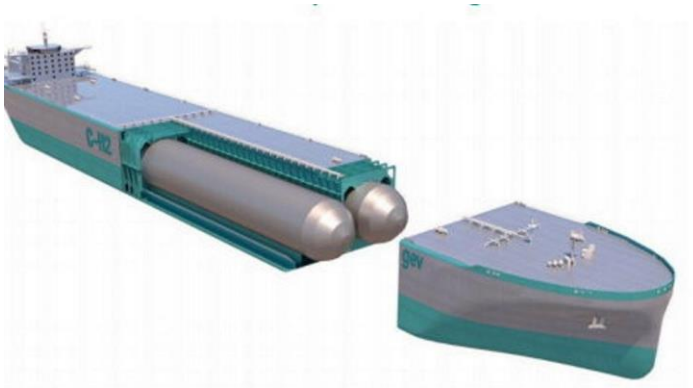


Figure 9: Compressed Hydrogen Transportation

Figure 10: Liquid Hydrogen Transportation By Ships

SAFETY OF HYDROGEN

As previously noted, hydrogen production and storage typically require either high pressure or extremely low temperatures. These demanding conditions naturally lead to concerns about safety. With the growth in hydrogen production, there is an increasing focus on safety protocols, prompting some countries to revise their legislation accordingly. Research efforts are expanding in areas such as operational safety, appropriate equipment selection, and personnel training. If hydrogen use in vehicles continues to rise, the safety standards for refuelling stations should be incorporated into this framework, and corresponding regulations and safety norms ought to be formally established.

It was mentioned that hydrogen is the lightest element in the world, meaning it is lighter than air, which means it goes up in case of release. Even though it is said that hydrogen is neither toxic nor harmless, the fact that it is colourless and odourless makes it hard to detect. Also, it should not be forgotten that hydrogen has a reverse Joule-Thompson effect, meaning that pressure drop increases the temperature. International Electrotechnical Commission and ATEX directives in Europe consider that the ignition energy of hydrogen is 0.017 MJ. Considering that a person cannot feel below MJ, the hydrogen with 0.017 MJ can be ignited, and even touching the t-shirt can cause it to be ignited.

There is also one more phenomenon, which is called Hydrogen Embrittlement. Hydrogen is compatible with organic materials but can cause embrittlement when metal or alloys are used for storage or transportation. The interaction of atomic hydrogen with the crystal lattice of the metal is quite possible because hydrogen atoms weaken the lattice [18-20].

When a gas mixture, or dust, self-propagates its flame and creates high-pressure waves, it is called an explosion reaction. The size of the pressure wave determines the degree of the explosion. If it is small, it is called deflagration; if it is big, it is called detonation.

Physical Explosion

There can also be physical explosions in the form of BLEVE (Boiling Liquid Expanding Vapour Explosion) or RPT (Rapid Phase Transition). A BLEVE is a physical explosion due to an immediate vessel rupture, including superheated liquids inside [21]. RPT is a physical explosion as well, and this should be considered when LH2 is close to the water source because this explosion happens when heat transfer happens between the cryogenic fluid and water, and it creates a vast explosion [16]. That's why installation systems of H_2 should consider these phenomena.

Hydrogen Damages

Besides the models of the explosion, it is worth talking about Hydrogen Damage; hydrogen is well known for its corrosion, and this corrosion can be classified by environment, appearance, and mechanism. All these forms of damage result from the diffusion of atomic hydrogen into the metal. This diffusion can cause a High-Temperature Hydrogen Attack, Hybrid/Hydrogen Embrittlement, Hydrogen Blistering, and Cracking [22]. Equation (8) shows that when steel or carbon is exposed to hydrogen for a long time under high pressure or temperature, it undergoes hydrogen attack over time, and hydrogen, reacting with carbon, forms methane.

$$8H + C + Fe_3C \rightarrow 2CH_4 + 3Fe \quad (8)$$

Hydrogen Safety: Considering the Standards

There are various standards to guide the training of people, installation, maintenance, design, repair, and inspection of the equipment used in hazardous areas and classification of environments with flammable gases, liquids, and dust, which poses a risk of fire or explosion. The most well-known standards are IECEx standards, NFPA codes and ATEX directives. IECEx is an international standard for explosive areas. The 60079 series covers the design, installation, repair, maintenance, inspection, marking, and classification of the equipment used in explosive atmospheres. NFPA is the American code, and ATEX is not a standard but a European directive covering essential health and safety requirements. Therefore, hydrogen also falls into these standards depending on the location. Also, there are ISO standards such as ISO/TR 15916 for essential consideration for the safety of hydrogen systems, ISO 16111:2018 for metal hydride storage devices and systems, ISO TC 197 for hydrogen fueling stations, and NFPA 2 for hydrogen technologies code.

An explosion occurs when the concentration of flammable gas in the air is between the lower flammable limit (LFL) and the upper flammable limit (UFL). For hydrogen, this is between 4% and 77%. This means that when the hydrogen concentration is more than 77% or less than 4% against air, it is not going to explode [23].

In any industry where explosive gas is present in the atmosphere (it can be dust too), the area is classified as Zone 0, Zone 1 and Zone 2 after calculations are made. Zone 0 indicates a continuous presence of explosive gas; Zone 1 indicates an occasional presence and Zone 2 is not likely to occur. Once this Zone area is classified, all the equipment selection, safety measures, maintenance and repair activities must be done according to this.

After the Zone is selected, the selection equipment for that Zone should have appropriate specifications. Each piece of equipment has a label that includes its explosive atmosphere, gas group, and temperature range. International standards define these values, and the ignition temperature for hydrogen is determined to be 560°C, which is why hydrogen has a T1 temperature classification as per the IECEx standards. It is important to remember that these values may have a slight difference from one standard to another; for the best value, a test might be needed. However, IECEx 60079 standards accept hydrogen as temperature class T1.

The temperature classification ranges from T1 to T6, and T6 is the most conservative one. Hydrogen's ignition temperature of 560°C is classified as T1, but it is essential not to forget that it is 0.017 MJ, which is very low.

Moreover, universal standards ensure each piece of equipment has a specific gas/dust group for explosive gases/dust. For gases, the groups are IIA, IIB, and IIC. IIC is the most conservative gas group, and hydrogen, along with acetylene, falls into this group.

Considering these standards, careful consideration is crucial when Hydrogen is present in the area.

CONCLUSION

Focus on logistics rather than hydrogen production. Therefore, proper storage, whether in batteries, underground, or integrated with natural gas, is essential. The key is to produce hydrogen from alternative sources with zero carbon emissions and integrate it into the system. Hydrogen filling stations utilizing excess electricity from solar or wind energy are a smart option.

While there is an increasing focus on storage advancements, traditional methods are still widely used. This raises safety concerns due to the increased pressure associated with hydrogen compression, necessitating extra safety measures. Although standards in this field are growing, there is a need for clearer guidelines and academic research regarding distance evaluations, zoning, hazardous area classification, equipment selection, and employee training in filling stations.

REFERENCES

[1] Victor Chombo, Pius, Yossapong Laoonual, and Somchai Wongwises. "Lessons from the electric vehicle crashworthiness leading to battery fire." Energies 14.16 (2021): 4802.

[2] Q. Hassan, A. Z. Sameen, H. M. Salman, M. Jaszczur, and A. K. Al-Jiboory, “Hydrogen energy future: Advancements in storage technologies and implications for sustainability,” J Energy Storage, vol. 72, p. 108404, Nov. 2023, doi: 10.1016/J.EST.2023.108404.

[3] H. Idriss, M. Scott, and V. Subramani, “Introduction to hydrogen and its properties,” Compendium of Hydrogen Energy: Hydrogen Production and Purification: Volume 1, vol. 1, pp. 3–19, Jan. 2015, doi: 10.1016/B978-1-78242-361-4.00001-7

[4] J. Arrillaga and B. Giessner, “Limitation of short-circuit levels by means of HVDC links,” presented at the IEEE Summer Power Meeting, Los Angeles, CA, USA, Jul. 12–17, 1990, Paper 70 CP 637.

[5] Zhang, Junyuan, et al. "Topology optimisation for crashworthiness and structural design of a battery electric vehicle." International journal of crashworthiness 26.6 (2021): 651-660.

[6] Jones, Andrew Zimmerman. "The Physics of a Car Collision." ThoughtCo, Aug. 27, 2020, thoughtco.com/what-is-the-physics-of-a-car-collision-2698920.

[7] isaac Physics - https://isaacphysics.org/concepts/cp_collisions?stage=all, 2022.11.15.

[8] Stabile, Pietro, et al. "An ultra-efficient lightweight electric vehicle—Power demand analysis to enable lightweight construction." Energies 14.3 (2021): 766.

[9] Aalund, Ryan, et al. "Understanding the non-collision related battery safety risks in electric vehicles: a case study in electric vehicle recalls and the LG Chem battery." IEEE Access (2021).

DOI: https://doi.org/10.12700/btsz.2025.7.2.15

CHALLENGES OF MODERN SECURITY TECHNOLOGY: EQUIPMENT LIFESPAN AND TECHNOLOGICAL DEVELOPMENT

A MODERN BIZTONSÁGTECHNIKA KIHÍVÁSAI: ESZKÖZÉLETTARTAM ÉS TECHNOLÓGIAI FEJLŐDÉSE

ANDRISKA Gergő[1]

Abstract

This study aims to explore the relationship between the lifespan of security technology systems, their technological advancement, and the economic return on investment. Due to rapid innovation, both hardware and software developments significantly impact the efficiency and applicability of these systems. The increasing use of artificial intelligence opens new possibilities, though concerns remain regarding its reliability and autonomous operation. Hardware advancements – such as sensors, image processing units, and control systems – represent progress, but their economic justification is not always evident. The research emphasizes that implementing technological innovations must be based on a thorough cost-benefit analysis, with attention to the full lifecycle of the systems.

Keywords

security technology, service life, obsolescence, technological development, investment return, life cycle management

Absztrakt

A tanulmány célja a biztonságtechnikai eszközök élettartama, technológiai fejlődése és a beruházások gazdasági megtérülése közötti összefüggések vizsgálata. A gyors technológiai fejlődés következtében mind hardveres, mind szoftveres téren folyamatosan jelennek meg új fejlesztések, amelyek hatással vannak a biztonságtechnikai rendszerek hatékonyságára és alkalmazhatóságára. A mesterséges intelligencia egyre szélesebb körű alkalmazása új lehetőségeket kínál, ugyanakkor kérdéses a megbízhatósága és önálló alkalmazhatósága. A hardverfejlesztések – mint az érzékelők, képfeldolgozó egységek és vezérlőrendszerek – jelentős előrelépést jelentenek, ám gazdaságossági szempontból nem minden esetben indokoltak. A kutatás rávilágít arra, hogy a technológiai újítások bevezetésének költség-haszon elemzésen kell alapulnia, figyelembe véve a rendszerek teljes életciklusát.

Kulcsszavak

biztonságtechnika, élettartam, elavulás, technológiai fejlődés, megtérülés, életciklus-menedzsment

[1] andriska.gergo96@gmail.com | ORCID: 0000-0002-6318-4084 | University student, Obuda University Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi hallgató, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A biztonságtechnikai rendszerek alkalmazása az elmúlt évtizedekben jelentős technológiai fejlődésen ment keresztül, amelynek eredményeként nőtt a védelmi rendszerek hatékonysága és bővültek a technológiai lehetőségek. Az olyan rendszerek, mint a megfigyelő kamerák, beléptető rendszerek, valamint tűz- és behatolásjelző berendezések, nemcsak a fizikai biztonság szavatolására szolgálnak, hanem adatokat is biztosítanak az események elemzéséhez és a preventív intézkedések kidolgozásához. Az eszközök műszaki paraméterei és élettartama azonban jelentős eltéréseket mutat, és a gyors technológiai innovációk következtében gyakran az eszközök fizikai elhasználódása előtt technológiailag meghaladottá válnak.

Gazdasági szempontból kulcsfontosságú az eszközök megtérülési mutatóinak vizsgálata. Egy biztonságtechnikai beruházás akkor tekinthető eredményesnek, ha az eszköz teljes élettartama alatt a befektetett költségek és az elért biztonsági szint közötti arány optimális. A technológiai elavulás ugyanakkor rendszeres frissítéseket vagy teljes rendszer cseréjét teszi szükségessé, ami növeli a fenntartási költségeket. Ezért a vállalatok és intézmények számára elengedhetetlen, hogy stratégiai megközelítést alkalmazzanak a biztonságtechnikai rendszerek életciklus-menedzsmentjében.

Jelen kutatás célja a biztonságtechnikai eszközök jellemző élettartamának átfogó elemzése, az elavulás különböző formáinak azonosítása, valamint a technológiai fejlődés eszközcserékre és megtérülési ütemezésre gyakorolt hatásainak vizsgálata. A tanulmány arra törekszik, hogy feltárja, miként egyeztethetők össze a műszaki, biztonsági és gazdasági szempontok egy hosszú távon fenntartható biztonságtechnikai stratégia kialakítása érdekében.

TÖRTÉNETI ÁTTEKINTÉS (1970–2025)

A biztonságtechnikai eszközök fejlődését az elmúlt öt évtizedben jól körülhatárolható technológiai ugrások jellemezték, amelyek jelentősen befolyásolták az eszközök alkalmazhatóságát, elavulását és cseréjének ütemezését.

- **1973 – CCTV-rendszerek bevezetése a londoni metróban**
  A londoni metróvonalakon 1973-ban telepítettek először analóg zártláncú kamerarendszert (CCTV), amely fekete-fehér képet rögzített videokazettára. A rendszer célja kezdetben kizárólag a megfigyelés volt, automatizált funkciók vagy távoli hozzáférés nélkül.
- **1984 – HID első elektronikus beléptető rendszer**
  A HID Corporation ekkor vezette be első nagyszabású mágneskártyás beléptető rendszerét vállalati környezetben. Ez forradalmasította az azonosítástechnikát, és kiváltotta a mechanikus kulcsokat az érzékeny objektumoknál.
- **1996 – Axis NetEye 200, az első IP-kamera**
  Ebben az évben dobta piacra az Axis Communications a világ első IP-alapú kameráját, a NetEye 200-at. Ez a lépés alapozta meg a mai hálózati megfigyelőrendszerek elterjedését, amelyeknél már nem volt szükség közvetlen kábeles összeköttetésre a kamerák és a rögzítő között.

- **2008 – Milestone XProtect NVR-rendszer széles körű bevezetése**
  A dán Milestone Systems 2008-tól kezdve ipari szinten is elérhetővé tette XProtect nevű, skálázható hálózati videómenedzsment szoftverét. Ez lehetővé tette az IP-alapú kamerák központosított, szoftveralapú kezelését, akár több ezer eszköz integrációjával.
- **2016 – Hikvision DeepinView: mesterséges intelligencia videóanalitikában**
  A Hikvision 2016-ban jelentette meg DeepinView kameracsaládját, amely képes arcfelismerésre, viselkedéselemzésre és tömegszámlálásra. A mesterséges intelligencia ekkor kezdett gyakorlati jelentőséggel bírni a valós idejű incidensészlelésben.
- **2023 – Verkada: felhőalapú, IoT-integrált biztonsági platformok**
  A Verkada és hasonló gyártók olyan felhőalapú megfigyelő rendszereket kínálnak, amelyek IoT-eszközöket (pl. szenzorok, beléptetők, videómodulok) egyetlen webes platformon kezelnek, prediktív riasztásokkal és teljesen távoli menedzsmenttel. Ez radikálisan csökkenti az on-site IT szükségletet.

Mint látható, a technológiai váltások (pl. analógról digitálisra, lokálisról hálózati vagy felhőalapú rendszerekre) kb. 10–12 évente új korszakot nyitottak a biztonságtechnikában.

A TÉMA ELMÉLETI ALAPJAI

A biztonságtechnikai rendszerek típusai és szerepük

A biztonságtechnikai rendszerek olyan komplex műszaki megoldások, amelyek célja az emberek, eszközök és adatok védelme különféle fenyegetésekkel – például illetéktelen behatolással, tűzzel, lopással vagy szabotázzsal – szemben. E rendszerek különösen kiemelt jelentőséggel bírnak a kritikus infrastruktúrák (KI) védelmében, ahol egy esetleges működésképtelenség nemcsak gazdasági, hanem társadalmi és nemzetbiztonsági következményekkel is járhat [1].

A biztonságtechnikai rendszerek az alábbi fő kategóriákba sorolhatók:

- **Megfigyelőrendszerek (CCTV/IP alapú):** Lehetővé teszik a folyamatos vagy eseményvezérelt vizuális megfigyelést. A modern rendszerek képesek mesterséges intelligencia alapú videóanalízisre, mozgásérzékelésre, arcfelismerésre, viselkedéselemzésre.
- **Beléptető rendszerek:** Feladata a hozzáférés szabályozása fizikai terekhez (pl. kártyás, biometrikus vagy PIN alapú rendszerek). Ezek kulcsszerepet játszanak a területre belépő személyek azonosításában és nyomon követésében.
- **Behatolásjelző rendszerek (IAS):** Olyan érzékelők összessége (pl. mozgás-, rezgés-, üvegtörésérzékelők), amelyek az illetéktelen behatolásokat detektálják és riasztást indítanak.
- **Tűz- és füstjelző rendszerek:** Elsődleges céljuk a korai észlelés és az életmentés, valamint az anyagi kár minimalizálása. Automatikus tűzjelzés, evakuációs irányítás és oltóberendezések aktiválása kapcsolódhat hozzájuk.
- **Integrált rendszerek:** Ezek a különféle rendszerek (pl. CCTV, beléptetés, IAS) egy közös platformon, egy egységes felügyeleti szoftveren keresztül működnek együtt, javítva a reakcióidőt és az adatfelhasználást.

Ezeknek a rendszerek hatékony működtetése és folyamatos fejlesztése elengedhetetlen a kritikus infrastruktúrák megbízható és biztonságos üzemeltetése érdekében. A nemzetközi szakirodalom is hangsúlyozza, hogy a biztonságtechnikai rendszerek integráltsági foka és technológiai színvonala közvetlenül befolyásolja az adott infrastruktúra kockázati kitettségét [2].

Az említett rendszerek nem csupán detektálnak, hanem adattárolási és -elemzési funkciókat is betöltenek. Ezáltal a biztonságtechnikai rendszerek az incidens utáni nyomozások, statisztikai elemzések és megelőző stratégiák kidolgozásának is alapját képezik.

AZ ESZKÖZÖK ÉLETTARTAMÁNAK MEGHATÁROZÓ TÉNYEZŐI ÉS AZ ELAVULÁS ELMÉLETE

A biztonságtechnikai rendszerek élettartama és elavulása szorosan összefüggő jelenségek, amelyek alapvetően befolyásolják a rendszerek megbízhatóságát, biztonsági szintjét és gazdasági fenntarthatóságát. Az élettartam alatt azt az időtartamot értjük, amely során az eszköz rendeltetés szerűen, biztonságosan és hatékonyan működik, míg az elavulás a fizikai, technológiai vagy funkcionális alkalmatlanság különböző formáit öleli fel. Az alábbiakban részletesen bemutatjuk az élettartamot meghatározó tényezőket, majd az elavulás elméletét, típusait és hatásait, hogy átfogó képet nyújtsunk e két terület kölcsönhatásáról és stratégiai jelentőségéről.

Az eszközök élettartamának meghatározó tényezői

A biztonságtechnikai eszközök élettartamát számos tényező befolyásolja, amelyek technológiai, környezeti, üzemeltetési és gyártói szempontból is megközelíthetők. Ezek pontos ismerete elengedhetetlen a fenntartási és fejlesztési döntések meghozatalához, valamint az optimális csereidőpont meghatározásához.

- **Műszaki paraméterek és beépített technológia:** Az eszközök élettartamának alapvető meghatározója a beépített technológia fejlettsége és a gyártási minőség. A korszerűbb, például IP-alapú rendszerek – amelyek önellenőrző funkciókkal, redundáns adatkezeléssel vagy szoftverfrissítési lehetőséggel rendelkeznek – általában hosszabb ideig képesek hatékonyan működni [1]. A hardveres elavulás jellemzően 5–10 év alatt következik be, míg a teljes funkcióvesztés többnyire 10–15 évnél jelentkezik [2]. Az olyan eszközök, mint az intelligens kamerák vagy tűzérzékelők, amelyek szoftveresen frissíthetők, hosszabb ideig maradhatnak relevánsak, mivel a szoftverfrissítések képesek lépést tartani a technológiai fejlődéssel.
- **Környezeti tényezők:** Az üzemelési környezet – például a hőmérséklet, páratartalom, por vagy korrózió – jelentős hatással van az eszközök élettartamára. Kültéri rendszerek, például térfigyelő kamerák, ki vannak téve szélsőséges időjárási viszonyoknak, UV-sugárzásnak és mechanikai behatásoknak, amelyek gyorsítják az anyagfáradást és az alkatrészek elhasználódását. Ezzel szemben a beltéri rendszerek stabilabb körülmények között hosszabb ideig maradnak üzembiztosak, különösen megfelelő karbantartás mellett. A környezeti tényezők figyelembevétele ezért kulcsfontosságú a rendszertervezés és az eszközválasztás során.

- **Karbantartás és használati gyakoriság:** A rendszeres karbantartás, például a megelőző ellenőrzések, tisztítás és szoftverfrissítések, jelentősen meghosszabbíthatja az eszközök élettartamát [3]. Az intenzív használat, például a 24/7 működés, gyorsíthatja az alkatrészek elhasználódását, különösen a mozgó elemek, mint például a kamerák forgatómotorjai vagy a beléptető rendszerek mágneszárjai esetében. Ezzel szemben a túlritkán használt eszközök elöregedése is problémát jelenthet, például az akkumulátorok kapacitásvesztése vagy az érintkezők oxidációja miatt. A karbantartási stratégia és az üzemeltetési szokások tehát közvetlenül befolyásolják az élettartamot.
- **Gyártói támogatás és frissítési ciklusok:** A gyártók által biztosított firmware- és szoftvertámogatás időtartama gyakran rövidebb, mint az eszköz fizikai élettartama. Különösen azoknál a rendszerknél amelyek hálózati kapcsolattal rendelkeznek. Az elavult szoftverek kiberbiztonsági kockázatokat hordoznak, mivel nem képesek megfelelni a legújabb biztonsági protokolloknak. A gyártói támogatás megszűnése után az eszköz technológiailag elavulttá válik, még ha fizikailag működőképes is. A frissítési ciklusok nyomon követése és a gyártói támogatási periódusok figyelembevétele ezért elengedhetetlen a hosszú távú működés biztosításához.

Az elavulás elmélete: típusok és hatások

Az elavulás a biztonságtechnikai rendszerek esetében nem csupán a fizikai elhasználódást jelenti, hanem egyre gyakrabban technológiai és funkcionális tényezőkben nyilvánul meg. Az elavulás mértéke és üteme közvetlenül befolyásolja az eszközök megbízhatóságát, biztonsági szintjét és gazdaságos üzemeltethetőségét, ezért elemzése kulcsfontosságú az életciklus-alapú tervezésben.

- **Fizikai elavulás:** A fizikai elavulás az anyagok természetes öregedéséből, mechanikai kopásából vagy elektronikai alkatrészek meghibásodásából fakad. Tipikus példái a szenzorok érzékenységének csökkenése, a kamerák képminőségének romlása vagy a mozgó alkatrészek – például motorok vagy relék – meghibásodása. Ez a folyamat különösen szembetűnő kültéri rendszereknél, ahol az időjárási viszonyok gyorsítják az elhasználódást. A fizikai elavulás fokozatos, és karbantartással – például alkatrészcserével vagy tisztítással – időlegesen mérsékelhető, de az élettartam vége felé a karbantartási költségek jelentősen megnőhetnek.
- **Technológiai (erkölcsi) elavulás:** A technológiai elavulás során az eszközök ugyan még működőképesek, de funkcionalitásuk, kompatibilitásuk vagy biztonsági szintjük elmarad az aktuális iparági sztenderdektől [4]. Ez gyakran a szoftveres támogatás megszűnéséből, új szabványok bevezetéséből vagy a kiberbiztonsági követelmények szigorodásából ered. Például egy tíz évvel ezelőtti analóg CCTV-rendszer nem nyújt megfelelő képfelbontást vagy hálózati integrációt a mai igényekhez képest. Az olyan technológiák, mint az AI-alapú videóanalitika vagy a biometrikus azonosítás, különösen gyors elavulási ütemmel rendelkeznek, mivel az új algoritmusok és protokollok akár 3–4 év alatt elavulttá tehetik a rendszert.
- **Funkcionális elavulás:** A funkcionális elavulás akkor lép fel, amikor egy eszköz már nem képes kielégíteni a megváltozott működési vagy szervezeti igényeket [5]. Ez például akkor fordul elő, amikor egy vállalat új biztonsági protokollokat vezet

be, amelyekhez a meglévő rendszerek nem alkalmazkodnak, vagy amikor egy integrált platform bevezetése miatt a régebbi rendszerek kompatibilitási problémákkal szembesülnek. Egy beléptető rendszer, amely nem támogatja a többfaktoros azonosítást, funkcionálisan elavulttá válhat egy szigorúbb biztonsági környezetben, még ha technikailag működőképes is. A funkcionális elavulás szorosan összefügg a technológiai elavulással, de a kiváltó ok itt a használati kontextus változása.

- **Az elavulás hatása a rendszerbiztonságra és gazdaságosságra:** Az elavulás különböző típusai jelentős hatással vannak a biztonságtechnikai rendszerek teljesítményére és költséghatékonyságára. Az elavult rendszerek gyakran sebezhetőbbek, nem támogatják az új protokollokat, és nem képesek hatékonyan integrálódni más alrendszerekkel, például tűzvédelmi vagy IT-biztonsági platformokkal, ezáltal növelve a rendszerszintű kockázatot [6]. Különösen a kritikus infrastruktúrák esetében súlyos gazdasági, társadalmi vagy nemzetbiztonsági következményekkel járhat egy elavult rendszer meghibásodása.
  Gazdasági szempontból az elavulás növeli az üzemeltetési és karbantartási költségeket. A fizikai elavulás miatt gyakoribbá válik az alkatrészcsere vagy javítás, míg a technológiai és funkcionális elavulás gyakran a teljes rendszer cseréjét teszi szükségessé [7]. Az elavult rendszerek kevésbé hatékonyak, ami közvetett költségeket – például hosszabb reakcióidőt vagy alacsonyabb kockázatészlelési pontosságot – eredményez. Az élettartam és az elavulás közötti összefüggések elemzése ezért kulcsfontosságú a gazdasági és biztonsági szempontok összehangolásához.
- **Az élettartam és elavulás kölcsönhatása:** Az élettartamot befolyásoló tényezők és az elavulás típusai szoros kölcsönhatásban állnak. Például a környezeti tényezők gyorsíthatják a fizikai elavulást, míg a gyártói támogatás hiánya a technológiai elavulást erősíti. A karbantartás elhanyagolása mind a fizikai, mind a technológiai elavulást felgyorsíthatja, mivel a szoftverfrissítések elmaradása kiberbiztonsági kockázatokat, míg a mechanikai karbantartás hiánya az eszköz meghibásodását okozhatja. A funkcionális elavulás gyakran a technológiai elavulás következménye, de a szervezeti igények változása önmagában is indokolhatja a rendszer cseréjét, még ha az eszköz fizikailag és technikailag működőképes is.

A döntéshozatal során az élettartam és az elavulás közötti egyensúly megtalálása kulcsfontosságú. Az optimális csereidőpont meghatározása nem csupán az amortizációs szabályokon, hanem a kockázatértékelésen, a technológiai trendeken és a szervezet specifikus igényein is alapul [8]. Az életciklus-alapú tervezés, amely figyelembe veszi az élettartamot befolyásoló tényezőket és az elavulás különböző formáit, lehetővé teszi a fokozatos fejlesztések bevezetését, csökkentve a pénzügyi terheket és biztosítva a technológiai relevancia fenntartását.

ROI; TCO; CBA – AVAGY A MEGTÉRÜLÉS MATEMATIKÁJA

A biztonságtechnikai beruházások hatékonyságának vizsgálata a döntéshozatali folyamat elengedhetetlen eleme. Az értékelés során különböző gazdasági módszerek állnak rendelkezésre, melyek közül a leggyakrabban alkalmazottak: a megtérülési mutatók (ROI), a teljes élettartamköltség (TCO), valamint a költség–haszon elemzés (CBA). Ezek célja, hogy objektív alapot biztosítsanak a rendszerfejlesztési és csereidőzítési döntésekhez.

ROI (Return on Investment) - Beruházás-megtérülés

A ROI a beruházásból származó nettó nyereséget viszonyítja a beruházási költségekhez. A képlet a következő:

$$ROI = \left(\frac{B - K}{K}\right) * 100\%$$

ahol:

- B: a biztonságtechnikai rendszer által generált haszon (pl. csökkentett kárérték, biztosítási díjkedvezmény),
- K: a teljes beruházási költség.

A ROI egyszerű és gyors összehasonlítást tesz lehetővé, ugyanakkor nem veszi figyelembe az időértéket és a működési költségeket [7].

TCO (Total Cost of Ownership) - Teljes élettartamköltség

A TCO a rendszer teljes életciklusa során felmerülő összes költség számszerűsítésére szolgál. A képlet:

$$TCO = K_b + K_t + K_m + K_o + K_e$$

- K_b: beszerzési költség,
- K_t: telepítési és beüzemelési költség,
- K_m: működtetési költség (pl. energiafogyasztás, munkaerőköltség),
- K_o: karbantartási és javítási költség,
- K_e: selejtezési, csere- és leszerelési költség.

A TCO különösen alkalmas hosszú távú rendszerfejlesztések és integrált biztonságtechnikai beruházások gazdasági értékelésére [8].

CBA (Cost-Benefit Analysis) - Költség–haszon elemzés

A CBA a beruházás összes hasznát és költségét összeveti, figyelembe véve azok időbeli értékét. A nettó jelenérték (NPV) kiszámításának képlete:

$$NVP = \sum_{t=1}^{n} \frac{B_t + K_t}{(1 + r)^t}$$

ahol:

- B_t: a t-edik évben várható haszon,
- K_t: a t-edik évben felmerülő költség,
- r: diszkontráta,
- n: a projekt időtartama években.

Pozitív NPV esetén a beruházás gazdaságilag indokolt, míg negatív érték gazdaságtalanságra utal [9].

Technológiai innovációk hatása a megtérülésre

Az olyan új technológiák, mint a mesterséges intelligencia, prediktív analitika, IoT vagy felhőalapú rendszerek, rövid távon növelhetik a beruházási költségeket, azonban hosszú távon csökkenthetik az üzemeltetési és karbantartási kiadásokat. Ez befolyásolja a TCO

és ROI számításokat, így új számítási modellek és szimulációk alkalmazását teheti szükségessé a pénzügyi tervezés során [9].

Összehasonlító táblázat

	Jellemző élettartam	Technológiai elavulás	Karbantartási igény	ROI (becsült)	TCO szint (relatív)
Analóg CCTV kamera	6–8 év	Gyors	Alacsony	Alacsony (~3%)	Alacsony
IP-alapú kamera	7–10 év	Közepes	Közepes	Közepes (~7%)	Közepes
AI-alapú videóanalitika	4–6 év	Nagyon gyors	Magas	Magas (~12%)	Magas
Beléptető rendszer (RFID)	10–12 év	Lassú	Közepes	Közepes (~6%)	Közepes
Biometrikus beléptető	6–8 év	Közepes–gyors	Magas	Közepes (~8%)	Magas
Tűzjelző rendszer (optikai)	12–15 év	Lassú	Alacsony	Alacsony (~4%)	Közepes
Behatolásjelző rendszer	8–10 év	Közepes	Közepes	Közepes (~6%)	Közepes

1. táblázat Különböző biztonságtechnikai rendszerek élettartam-elavulás összegzése (saját szerkesztés)

Elemzés és értelmezés

Az egyes eszköztípusok közötti különbségek nemcsak műszaki paramétereikben, hanem működtetési és gazdasági szempontjaikban is jelentősek. A saját elemzésem során négy fő kategóriát határoztam meg: műszaki időtállóság, technológiai elavulás, karbantartási igény, valamint beruházási megtérülés (ROI) és teljes élettartamköltség (TCO).

- **Műszaki időtállóság:** A tűzjelző rendszerek és RFID-alapú beléptetők kiemelkednek a hosszú élettartamukkal, amelyet egyszerű, jól bevált technológiájuknak és alacsony szoftverfüggőségüknek köszönhetnek. Az ilyen eszközök gyakran több mint egy évtizeden keresztül használatban maradnak, különösebb fejlesztés vagy korszerűsítés nélkül. Ezzel szemben a gyorsan fejlődő területeken – például a képfeldolgozás vagy biometrikus azonosítás – használt eszközök rövidebb időn belül morzsolódnak le technológiai szempontból, még ha fizikailag tovább is működőképesek.
- **Technológiai elavulás:** A technológiai avulás a mesterséges intelligencia alapú eszközöknél a leggyorsabb. Az új algoritmusok, szabványok és hálózati követelmények akár 3–4 év alatt elavulttá tehetnek egy korábban korszerű rendszert. Az IP-alapú eszközök esetében az erkölcsi elavulás általában 6–8 év között következik be, míg az analóg rendszerek már gyakorlatilag elavultnak tekinthetők. Saját értékelésem szerint ez az egyik legfontosabb tényező, amit a beszerzési döntések során figyelembe kell venni.
- **Karbantartási igény:** A kevésbé bonyolult rendszerek – mint például a passzív tűzjelzők vagy az analóg kamerák – karbantartási igénye alacsony, rendszerint csak alapvető működésellenőrzésre, tisztításra és tesztelésre van szükség. Ezzel szemben a szoftverintenzív rendszerek (pl. AI, biometria) rendszeres frissítést, konfigurálást,

esetenként rendszeres újratanítást igényelnek, ami szakemberi jelenlétet, magasabb költséget és szervezési ráfordítást jelent.

- **Megtérülés és költséghatékonyság:** A példaszámítás alapján kimutattam, hogy az AI-alapú rendszerek ugyan rövidebb élettartammal és magasabb TCO-val rendelkeznek, mégis nagyobb megtérülést biztosíthatnak, ha helyesen vannak beillesztve a védelemi struktúrába. Ez azonban csak akkor igaz, ha a működési környezet lehetővé teszi az automatizált kockázatészlelések tényleges kihasználását.

Az egyszerűbb rendszerek gazdaságilag kedvezőbbek rövid és középtávon, de hosszú távon nem feltétlenül támogatják az összetett fenyegetésészlelést és hálózati integrációt. Éppen ezért a gazdasági mutatók – különösen a TCO és az NPV – rendszeres felülvizsgálata elengedhetetlen a stratégiai döntésekhez.

A kutatásom során arra a megállapításra jutottam, hogy a biztonságtechnikai rendszerek élettartama, elavulása és technológiai fejlődése szoros kölcsönhatásban állnak egymással. A fizikai élettartam ugyan továbbra is meghatározó, de a technológiai elavulás – különösen a digitális, hálózatra kapcsolt eszközök esetében – gyakran hamarabb indokolja a cserét, mint a műszaki meghibásodás. Ez a felismerés fontos hatással van arra, hogyan kell tervezni és üzemeltetni egy korszerű biztonságtechnikai rendszert.

A különböző eszköztípusok élettartama jelentősen eltér, különösen a szoftveresen komplex rendszerek esetében, ahol az erkölcsi elavulás gyakran 4–6 éven belül bekövetkezik. A gazdasági megtérülés nem csupán a beruházási költségektől függ, hanem szorosan kapcsolódik az üzemeltetési költségekhez, a karbantartási igényekhez és a rendszer funkcionalitásához. A TCO és ROI mutatók összehangolt alkalmazásával hosszú távon fenntartható és hatékony beruházási döntések hozhatók. Az új technológiák bevezetése akkor éri meg, ha az adott védelmi célrendszer képes kihasználni az általuk nyújtott előnyöket, például az AI-alapú elemzéseket vagy a hálózati integrációt.

KONKLÚZIÓ

A kutatás tapasztalatai alapján több gyakorlati javaslatot fogalmazok meg.

Először is, érdemes életciklus-szemléletű tervezést alkalmazni, amely már a biztonságtechnikai rendszerek kiválasztásának a fázisában figyelembe veszi a várható élettartamot, a technológiai fejlődést és a gyártói támogatási időszakot.

Másodszor, a rendszeres TCO és ROI elemzések támogatják az eszközök állapotának és költséghatékonyságának időszakos értékelését, különösen nagyobb léptékű infrastruktúrák esetében, így elősegítve a tudatos döntéshozatalt.

Harmadszor, a gyorsan elavuló technológiák kezelésére célszerű 3–5 éves frissítési ciklust bevezetni, amely lehetővé teszi a fokozatos fejlesztést a teljes rendszer lecserélése nélkül.

Negyedszer, előtérbe kell helyezni az integrációs képességeket, olyan rendszereket választva, amelyek könnyen összekapcsolhatók más alrendszerekkel, például tűzjelző vagy épületfelügyeleti rendszerekkel, ezzel növelve az adatáramlás és a döntéstámogatás hatékonyságát.

Végül, a modern technológiák alkalmazása megköveteli a kezelőszemélyzet rendszeres képzését és a gyártói vagy szolgáltatói támogatás aktív igénybevételét.

Ezek a javaslatok hozzájárulnak ahhoz, hogy a biztonságtechnikai beruházások hosszú távon fenntarthatók, költséghatékonyak és technológiailag korszerűek maradjanak. A tudatos döntéselőkészítés és az életciklus-alapú szemlélet nemcsak a költségvetés hatékonyságát növeli, hanem a védelmi szint fenntartását is biztosítja.

FELHASZNÁLT IRODALOM

[1] Enisa, „Security of Industrial Control Systems," European Union Agency for Cybersecurity, online, 2020.
[2] B. T. Bognár Balázs, KRITIKUS INFRASTRUKTÚRÁK VÉDELME I., Budapest: Dialóg Campus Kiadó, 2019.
[3] Keenfinity-group, „Product Life Cycle Planning Guide," 2022. [Online]. Available: https://www.boschsecurity.com/xe/en/support/product-security/.
[4] „IEC 62820-1:2016: Video surveillance systems for use in security applications – General requirements," 2016.
[5] Z. Zsolt, „A biztonság és abiztonságmenedzsment vizsgálata vállalati nézőpontból," Hadmérnök, %1. kötet15, %1. szám1, pp. 19-29, 2020.
[6] Security Science: The Theory and Practice of Security, Butterworth-Heinemann, 2013.
[7] Isaac Kohen, „How to calculate your return on security investments," online, 2019.
[8] T. L. Néma Szabolcs, „Gazdasági optimalizáció az objektumvédelemben," Magyar Rendészet, %1. kötet24, %1. szám4, p. 121–144, 2024.
[9] R. Naegle, „Strategic IT Cost Optimization That Goes Beyond Slashing Spend," gartner, online, 2025.
[10] „A karbantartás szerepe a vagyonvédelmi rendszerek életciklusában," 2021.
[11] „UL 2800-1 Standard: Performance and Reliability of Security Equipment," UL, 2021.
[12] Koorsen Fire & Security, „How Important Is Regular Maintenance for Commercial Security Systems," Koorsen Fire & Security, online, 2024.

DOI: https://doi.org/10.12700/btsz.2025.7.2.25

ASPECTS OF OBJECTS AND FACILITIES INTERFERING WITH SURVEILLANCE

OBJEKTUMOK, LÉTESÍTMÉNYEK LÉGTÉRFELDERÍTÉST ZAVARÓ ASPEKTUSAI

BRAUN András[1] – PETŐ Richárd[2]

Abstract

In Hungary, military installations equipped with radars can be found in several settlements in different parts of the country. These radars can reveal azimuth, distance and altitude of detected air targets. In the course of the study, besides the operation and application of radars, the general rules of their installation and terrain requirements are described. Separately, the RAT-31DL three-dimensional radar is shown, which has a fixed location, but a mobile transportable version, the RAT-31DL/M has also become available. However, regardless of whether the radars in question are mobile or fixed, they must comply with almost the same rules and terrain requirements in order to create a clear and acceptable air situational picture.

Keywords

Object, RAT-31DL Radar, Airspace Reconnaissance, Military Technology

Abstract

Magyarország több településén, az ország különböző pontjain, található radarokkal felszerelt katonai létesítmény. Ezen radarok különböző oldalszögeken, különböző magasságokon és távolságokon képesek a légi célokat felderíteni. A tanulmány során ismertetésre kerül a radarok működése és alkalmazása mellett azok telepítési helyeinek általános szabályai, terep követelményei. Külön szemléltetésre kerül a RAT-31DL három dimenziós radar, mely nagyrészt fix települési hellyel rendelkezik, ugyanakkor az idők során a mobil, szállítható verziója, a RAT-31DL/M is megjelent. Mindazonáltal, attól függetlenül, hogy a kérdéses radarok mobil vagy fix településűek szinte ugyanazon szabályoknak és terep követelményeknek kell eleget tenniük a tiszta és elfogadható légihelyzetkép felderítése érdekében.

Keywords

Objektum, RAT-31DL Radar, Légtérfelderítés, Haditechnika

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

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

INTRODUCTION

When installing radars and their associated communication equipment, be it civil or military use, the requirements for the installation site must primarily take into account the usability of the given equipment. Including its operational properties, communication capabilities, and other requirements. Of course, health and nature consideration aspects must also be taken into account, but from the point of view of utilizing the effectiveness of the devices, the most important thing is to provide a clear line of sight, i.e. a free radio horizon. In general, the installation rules prescribed for structures and objects to be installed in the vicinity of the radar serve environmental and health purposes as well. Therefore, if a tall structure, residential building or multi-storey house cannot be built in the immediate vicinity of the radar. This prohibition is not only intended to maintain detection or communication capabilities, but also to protect the environment and health of the people living there. Compared to the installation location of radars, in the direction or in the directions on which the objects listed above are located, a significant decrease in capability, usability may occur or may occur if some basic rules regarding the installation of the objects are not observed. In order to maintain the usability of civil and military radars and related communications technical devices, as well as to preserve the reconnaissance and communication capabilities required for these equipment, it is necessary to preserve their environment in the state in which it was deployed. [1]

OPERATION AND SUB-OPERATION OF RADARS

„Radar, as a radio detection and determining tool, became widely used in the Second World War. The radar detects the target with the help of radio waves and plots the spatial position of objects like a map. Radio waves travel through smoke, clouds, fog, even walls, they can see excellently even on objects impenetrable to light. The antenna emits radio waves and then waits for reflected waves from the target. It radiates several signals simultaneously to scan in as many directions as possible in a short time, while the antenna rotates continuously. The pulses emitted by the radars must be timed so that there is time for the signal already sent to return before the next pulse is sent by the antenna. From the reflected signal, the distance of a target can be measured, and in different radars, its height can also be measured.

Radio locators are classified as:

- By operation: continuous or pulsed.
- Used by wavelength: meter, decimeter, millimeter wavelength.
- By primary task: tracking, searching.
- By installation location: ship, ground, aircraft, etc.

The basic elements of active radars are the antenna and power line system, indicator, transceiver, antenna control system, as well as power source. Passive radars do not have transmitting equipment. Continuous radars are suitable for determining the radial velocity of the selected target using the Doppler effect. The Doppler effect is a change in wave frequency and thus wavelength due to the fact that the wave source and observer move relative to each other. The high-frequency energy radiated into the air by the antenna, produced by the transmitter, travels at a speed of $3x10^8$ m/s. Then the signal reflected from a

target or target is picked up by the receiving antenna, amplified by the receiver, and then transmitted to the indicator screen, where it is transformed into visible information.

Application of radio location in civilian life:

- In industry: research and fault positioning, monitoring.
- In meteorology: determining coordinates, measuring wind speed and forecasting the weather, observing cloud migration.
- In transport: search and control of ground, water and aircraft vehicles, determination of speed and other coordinates, possible prevention of accidents.
- In agriculture: crop estimation.

Application of radio location in the army:

- Recognition and distraction.
- Target detection, target tracking, target identification and fire control, target interception.
- Control of aircraft take-off and landing, determination of target coordinates and orientation to enemy targets.
- Remote control by command, depth measurement and entry into port, guidance of missiles and torpedoes." [2, pp. 2-3.]

RAT-31 DL three-dimensional radar

"The RAT-31 DL[3] is a long-range three-dimensional radar that provides surveillance and reconnaissance over aircraft. State-of-the-art radar system operated in military air defense. Its antenna is a phased array of broadband dipoles and has a detection range of 470 km. The radar provides survivability as well as versatile operational flexibility against various enemy disturbances. Full solid-state, remotely controllable, transmitting power 84 kW, D/L band 1215-1400 MHz, IFF[4] system Mode 4 and Mode S and Mode 5. In some cases, it can also be used by air traffic control. It enables early warning and situational recognition for the timely use of weapon systems in addition to air surveillance. Its feature is to map the electromagnetic environment for ECM[5] and clutters[6] , to more reliably detect flying aircraft within radar detection range, and to determine spatial coordinates, distance, azimuth and altitude.

The RAT-31 DL radar has all the modern data processing capabilities such as adaptive disturbance maps and all modern interference suppression techniques for known land objects. Its angular rotation is mechanical, while the angular height of the main beam is electronically determined on a phase-controlled principle, i.e. with phase shifters. The antenna surface of the radar is tilted back by about 10° in order to achieve the lowest possible radar beam angle value. Over time, they created the DL/M version of the RAT-31, a mobile,

3 RAT31-DL - Italian-made three-dimensional reconnaissance radar

4 IFF – Identification Friend or Foe, a radio recognition system designed for command and control. It allows military and civil air traffic control systems to identify aircraft, vehicles or forces as friends and determine their direction and distance from the interrogatory.

5 ECM – Electronic Countermeasure.

6 Clutter – Confusion, distraction.

transportable version of this state-of-the-art three-dimensional radar system. They are almost identical in parameters and properties, the biggest difference is in mobility." [2, pp. 3-4.]

GENERAL RULES AND TERRAIN REQUIREMENTS

The objects and facilities listed below, depending on the distance and height of their location relative to the electromagnetic center line of the antenna of the radar station, greatly negatively affect or even completely impair the basic detection properties of the radar equipment examined or affected:

- taller buildings, structures,
- high-power electrical transformers,
- high-voltage lines,
- electrical wiring and their supporting columns,
- wind farms, wind farms,
- high-frequency or microwave towers, repeater stations,
- plant populations, forests.

By following the general rules, detection capabilities of the currently installed, already operating radio technology and radar equipment, and in the case of military radars, their operational capabilities and the communication coverage of the associated radio communication devices can be preserved. General rules:

- The directional characteristics of the radio-locator (radar) antenna are shaped by the terrain conditions of the settlement location.
- The degree of influence of the terrain depends on the altitude of the radar antenna above the surrounding terrain or landmarks.
- The formation of the antenna beam is influenced by unevenness of the terrain (protrusions), which create a so-called cover angle[7] in the direction of free propagation of electromagnetic energy. The part of the space behind the cover angle remains unirradiated, so the signals reflected from that part of the space cannot be detected, i.e. so-called dead zones or blind spots are formed for the radar.
- Depending on the intensity of the energy reflected from different sections of the terrain, moving away from the antenna of the radar station, the area forming the antenna characteristics can be divided into two main parts. These areas are near space (0-1000 m) and far space, outside a radius of 1000 meters measured from radar.
- In order to ensure the tactical capabilities of radio locator stations, the so-called cover angles closed by the radio horizon and local landmarks should not exceed 20 arcminutes in any direction. At cover angles greater than 20 arcminutes, the detection distance specified in the radio-locator station pedigree will be significantly reduced, and the ability to detect and track devices flying at low altitude in that direction will be degraded or, in worse cases, may disappear.

7 Cover angle – The angle between the tangent drawn to a feature at a height other than the horizontal and the antenna plane. [minutes]

- An ideal settlement location can be considered a settlement site on the prevailing elevation with negative angles of cover. [3] [4]

Radar Near Space (0-1000 m) terrain requirements

When assessing terrain, both natural and artificial landmarks and structures should be taken into account. The radar near-space (0-1000 m) has the most significant influence on the formation of the radar vertical plane antenna radiation diagram.

- The height of the settlement, radar is close to the area, the height of its unevenness, including topography and artificial structures and buildings, within a radius of 1000 meters measured from the antenna, must not exceed the height of the antenna platform.
- A dense forest located at or close to the height of the radar antenna greatly reduces the detection distance, therefore, within a radius of 1000 meters around the settlement site, dense vegetation that rises above the antenna platform should not be.
- Artificial structures extending or located at radar antenna height, such as buildings, radio transmission or relay towers, TV transmitters or repeater towers, radiotelephone masts and other antenna poles. Masts and other high points such as wind farms, wind farms and observation towers may not be built.
- The radar station must be installed at a minimum distance of 1000 meters from densely populated areas. It is forbidden to build any structure in the etheric radius of the radar already installed, whatever its material or consistency, for any purpose or use - reaching above the radar platform1000 m.
- It is forbidden to construct any building or structure with a roof of metal construction or a total roof surface exceeding 50 square meters in the vicinity of the radar platform within a radius of 1000 meters, the roof of which exceeds half the height of the radar platform.
- Within a radius of 1000 meters of the radar, there must be no tall reinforced concrete and brick structures, buildings with metal roofs, metal masts, bridge structures, high-voltage transmission lines, or wired communication or telecommunications lines or cables that reach beyond the height of the radar platform.[4] [5]

Radar Far Space (outside a radius of 1000 meters from radar) terrain requirements

The design of the radar detection diagram is basically determined by the angles of cover of landmarks in the distant space. In connection with the above, Figure 1 below illustrates the limitations of building structures around radars.

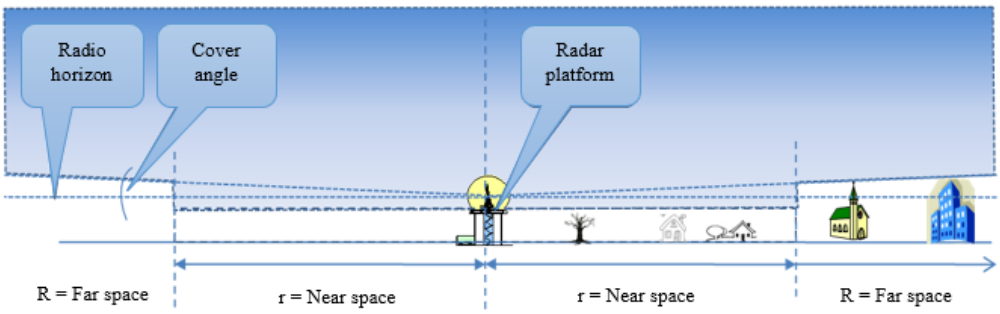


Figure 1: Illustration of radar detection, Near space, Far space, author's edit

The licensing of the construction plans of various structures and objects is approved by the competent authority. The authority may approve the construction and design documentation of the structure based on the height and distance from the radar of the structure to be constructed. The distance and height of the object to be constructed from the radar determines whether or not a building permit can be issued for the construction of the object. The administration is obliged to examine, on the basis of the submitted plans, whether the structure to be constructed corresponds to the radar cover angle or not, using the following mathematical relationship. In the distance of the radar, i.e. beyond the radius of 1000 m from the radar, only structures may be built which satisfy the values given by the following relationship. [5] [6]

$$R_{object} = 3605 * \sqrt{H_{object\,[m]}}\ [m]$$

R_{object}: The distance of the object or structure to be built from the radar, expressed in meters as the crow flies, where the result is obtained in meters after the calculation is completed.

H_{object}: The height of the highest point of the object or structure to be built expressed in meters, the data must be expressed in meters.

Figure 2 below depicts, with the help of two red marker lines, based on the coordinates of their intersections, that objects or structures up to 30 meters high can be built at a distance of 20 km from the radar.

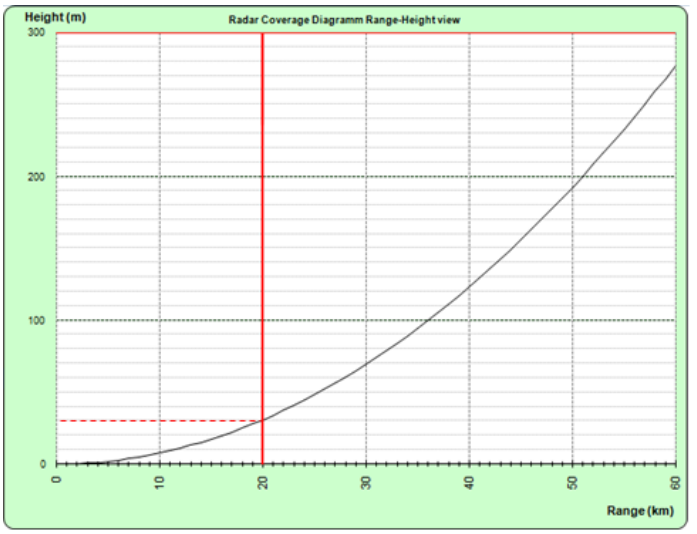


Figure 2: Radar coverage chart, distance-altitude view, author's edit

REQUIREMENTS FOR SETTLEMENT SITES

When choosing a settlement location, it should be taken into account that the terrain conditions of the settlement location play a key role in the development of the directional characteristics of the radar station. The dimensions of the terrain that affect the directional characteristics depend on the height of the radar station's antenna above the terrain, the operating frequency, and the antenna's angle of location. The location of the radar station must first be selected on a map, followed by a visual inspection of the terrain. The best possible

settlement place is straight open ground with a radius of 800-1000 meters. It is not always possible to find such a settlement place, therefore, in each case, it is necessary to choose a place suitable for the combat task of the radar station to be solved.

Near Space (0-1000 m) has the most significant influence on the design of the vertical plane radiation diagram. When assessing the zone of the presumed settlement site, the following shall be taken into account:

- disparities in settlement location must not exceed 3 m within a radius of 100 m from the antenna and 6 m within a radius of 1000 m,
- a uniform slope or rise of the terrain significantly affects the formation of vertical characteristics,
- if the settlement site has a uniform slope at some angle, the radiation diagram is inclined towards the ground at approximately the same angle in a vertical plane and has deeper incidences, the angle of slope must not exceed 2°,
- if the settlement site rises uniformly at a small angle, then the radiation diagram rises by the same angle in a vertical plane, as a result of which the detection distance decreases, the angle of rise should not exceed 0,5°,
- dense forest greatly reduces the detection distance, therefore the settlement site should be chosen at least 1000 meters from the forest, some trees and thickets do not affect the characteristics of the radar station,
- on mountainous terrain, where the choice of settlement site is difficult, the radar station should be located primarily on a plateau with a flat area with a radius of 500-1000 meters, if necessary, it can also be located on a slope or at the foot of the mountain,
- if the radar station is to be installed near built-up areas, it shall be at least 1000 m from built-up areas, and if there are buildings with high metal roofs in built-up areas, at least 2000 m,
- the water surface is advantageous for the development of direction characteristics, increases the range, therefore it is advisable to choose the settlement location on an island, cliff, sloping sea or river bank, in case of a river wider than 400 meters, so that the water surface falls into the main sector and the radar station is no more than 100 meters from the shoreline.

When choosing a place for settlement, it is also necessary to evaluate the surface of the remote zone. In order to increase the range, the cover angle shall not exceed 15'. The choice of settlement place should begin with the study of the map. Designating some possible settlement sites, it is necessary to evaluate the remote zone of each settlement site as follows:

- draw a vertical section of the terrain from the assumed settlement point, especially in critical directions,
- for each direction, the profile of the terrain must be edited in a Cartesian coordinate, where the distance from the antenna is applied to the abscissa axis, the height is applied to the ordinate axis, the resulting points are connected by a continuous line,
- using terrain sections, the settlement location should be evaluated in terms of covering angles and local landmarks on the basis of the above considerations,

- choosing the two or three best of the indicated places of settlement, you need to go out to the site to evaluate and study the nearby zone.

If at different side angles the slope and ascent angles of the terrain are different, then the settlement site should be divided into sectors with homogeneous terrain. If the settlement site has more than two or three sectors with homogeneous terrain, it is not suitable. When assessing the settlement site, access roads, drinking water supply, mains feeding, communications and radar station camouflage against air and ground surveillance shall be taken into account. Within a radius of 100 meters of the selected settlement site, there should be no high reinforced concrete and brick structures, buildings with metal roofs, metal masts, bridge structures, high-voltage power lines, multi-wire news lines. For the placement of cars and trailers, it is advisable to designate a place with hard ground. [4] [5] [6]

SUMMARY

When installing radars, whether for civilian or military purposes, the most important aspect is to ensure the operability and efficiency of the devices. To this end, a location should be chosen which guarantees a free radio horizon and helps to establish and maintain a clear air situational picture. When choosing a site, it is necessary to take into account the detection and communication capabilities of radars, as well as environmental and sanitary regulations. The latter aspects not only serve to protect the environment and human health, but also contribute to optimizing the operation of the radar. The impact of structures and landmarks is extremely important in the vicinity of radars. Taller structures, electrical equipment, wind farms and dense vegetation can significantly reduce radar's range and detection capability. To avoid them, in close space with a radius of 1000 meters, landmarks and structures that rise above the antenna platform cannot be placed. Also, in distance space (beyond 1000 meters), the height and distance of objects from radar are limited according to strict rules. Terrain conditions are also decisive in determining radar directional characteristics. In uneven terrain, the cover angle increases, which can lead to blind spots, reducing radar's ability to detect. Ideally, radars should be installed at prevailing heights with negative cover angles. If this is not possible, the unevenness and gradient/ascent angles of the terrain must be strictly controlled. Unevenness of terrain within a radius of 1000 m should not exceed the height of the antenna, dense forests and tall buildings should be avoided. The location of the radar installation must first be marked on a map, and then checked on the ground, taking into account accessibility, power supply and camouflage options. When choosing a site, priority is given to proper preparation of the environment for optimal radar operation. This includes assessing terrain conditions in near and far zones, minimizing coverage angles, as well as limiting objects in the radar environment. Overall, choosing the right installation site is key to ensuring long-term effective radar operation and minimizing environmental impact.

REFERENCES

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

[2] BRAUN A., *Szélerőművek hatása a radarokra*. Biztonságtudományi Szemle, Vol 6, No 3, pp. 59-69, 2024. [Online] https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/482
[3] EUROCONTROL, *Guidelines on Assessing the Potential Impact of Wind Turbines on Surveillance Sensors*, 2014. [Online] https://www.eurocontrol.int/publication/eurocontrol-guidelines-assessing-potential-impact-wind-turbines-surveillance-sensors
[4] WOODFORD, C., *Radar*, 2015. [Online] https://www.explainthatstuff.com/radar.html
[5] BARTON D. K – LEONOV S. A., *Radar technology encyclopedia*. Artech House, Boston, Mass., 1997. [Online] https://us.artechhouse.com/Radar-Technology-Encyclopedia-P594.aspx
[6] SELLER R., *Radarmérés alapjai*. Nemzeti Közszolgálati Egyetem, 2016. [Online] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://vik.wiki/images/2/27/Radarmeres_alapjai.pdf

DOI: https://doi.org/10.12700/btsz.2025.7.2.35

MILITARY SECURITY IN THE PRICE OF STRESS

KATONAI BIZTONSÁG A STRESSZ ÁRNYÉKÁBAN

KISS Csaba[1]

Abstract

The Law on Surry was passed in Hungary in 1868, and from 1869 the Hungarian Army, which was suspended on November 3, 2004. This said that after the suspension, only the Hungarian army consists of professional and contractors. This can also be interpreted as the fact that in 2025, those under the age of 38 did not serve as a Sorka Tone in the Hungarian Defense Forces. During the past time, military technology has undergone a rapid development, which is also due to the opportunity for artificial intelligence. The world tendency says that armed conflict explodes more and more places and the fighting parties use the latest military tools to win. With the development of Haditech-Nika, there is a narrow layer who is in professional and contractual staff. Serving in the army always meant stress. The publication explains how artificial intelligence can help citizens invited from military service civilians to overcome stress.

Keywords

soldier, stress, artificial intelligence, military training

Absztrakt

A sorkatonaságról szóló törvényt 1868-ban fogadták el Magyarországon s ezt követő évtől 1869-től működött a sorozott magyar hadsereg, amit 2004. november 3-án felfüggesztettek. Ez azt jelentette, hogy a felfüggesztést követően csak hivatásosokból és szerződésesekből áll a magyar hadsereg. Ezt úgy is értelmezhetjük, hogy 2025-ben a 38 évnél fiatalabbak nem szolgáltak sorkatonaként a Magyar Honvédségben. Az eltelt idő alatt a haditechnika rohamos fejlődésen ment keresztül, ez köszönhető a mesterséges intelligencia alkalmazásának is. A világ tendenciája azt mutatja, hogy egyre több helyen robban ki fegyveres konfliktus és a harcoló felek a legújabb technikai eredményekkel felszerelt katonai eszközöket használnak a győzelem elérésére. A haditechnika fejlődésével egy szűk réteg foglalkozik, akik hivatásos és szerződéses állományban vannak. A hadseregben szolgálni mindig stresszet jelentett. A publikáció kifejti, hogy hogyan segíthet a mesterséges intelligencia a katonai szolgálatot teljesítő civilből behívott polgárokat a stressz leküzdésében.

Kulcsszavak

katona, stressz, mesterséges intelligencia, katonai kiképzés

[1] kiss.csaba@uni-nke.hu |ORCID:0000-0002-7265-8704| PhD student, National University of Public Service, National, Doctoral School of Military Engineering| doktorandusz, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

BEVEZETÉS

A sorkatonaságról szóló törvényt 1868-ban fogadták el Magyarországon s ezt követő évtől 1869-től működött a sorozott magyar hadsereg, amit 2004. november 3-án felfüggesztettek. Ez azt jelentette, hogy a felfüggesztést követően csak hivatásosokból és szerződésesekből áll a magyar hadsereg.

Ezt úgy is értelmezhetjük, hogy 2025-ben a 38 évnél fiatalabbak nem szolgáltak sorkatonaként a Magyar Honvédségben. Az eltelt idő alatt a haditechnika rohamos fejlődésen ment keresztül, ez többek között köszönhető az MI látványos alkalmazásának a katonai eszközökben.

A világ tendenciája azt mutatja, hogy egyre több helyen robban ki fegyveres konfliktus és egyre több embert érint, mint civil, mint katonai szempontból. A harcoló felek az újabb fegyveres konfliktusokban a legújabb technikai eredményekkel felszerelt katonai eszközöket használnak a győzelem elérésére.

Látható, hogy a haditechnika fejlődésével egy szűk réteg, akik hivatásos és szerződéses állományban vannak, képesek lépést tartani s készségszinten nekik is évekbe telik azok alkalmazásának a megtanulása.

„Az egyik legnagyobb kihívás az lesz, hogyan tudjuk radikálisan újra gondolni az egyéni és szervezeti tanulási folyamatainkat - hangsúlyozta dr. Porkoláb Imre dandártábornok a Honvédelmi Minisztérium Védelmi Innovációs és Képességfejlesztési Főosztályának miniszteri biztosa a Trend FM „A Nap Vendége" című műsorában 2022. december 13-án." [1].

„A Magyar Honvédségben zajló digitális transzformációval kapcsolatban Porkoláb Imre kiemelte a digitális katona programot, amelynek két iránya van. Az egyik, hogy kognitív módon miként lehet felkészíteni a katonákat a digitális technológiákra, a másik pedig az energiabiztosító rendszerek kérdése." [1].

A tanulás nem csak a katonai eszközök működésének megértését és azok használatát jelenti, hanem az eszközök rendszerben történő üzemeltetésének a megtanulását is. Ide tartozik még a saját csapataink és az ellenséges csapatok jelzésének a megkülönböztetése, a technikai eszközök megkülönböztetése a katonai szín és formavilágban történő eligazodás.

„A társadalom és a gazdaság folyton változása nyomot hagy a mindennapjainkban, ami növelheti a szorongást az aggodalmakat és a stressz nyomását." [2]. Ennek kezelésére szükségünk van helyzetfelismerésre, és szociális ügyességre. A civil területen megszerzett képességek a túlélésre sokszor nem elegendőek a katonai szolgálat alatt ért hatások leküzdésére. A civil területen megszokott biztonság, kényelem a katonai életben csak nyomokban található meg vagy egyáltalán nincsenek is meg.

Klinikai érvelések szerint, az agy középső részéhez közel elhelyezkedő hippokampusz szervünk felelős az olyan kognitív funkciókért, mint az olvasás, a memória, vagy a viselkedés szabályozása. „Felmérések bizonyítják, hogy a krónikus stressz hosszú távon károsítja a hippokampuszt és csökkenti annak méretét." [3]. Ilyen körülmények között a tanuláshoz szükséges olvasási és memória képességek csökkenése várható, ami csökkentheti az elsajátított anyagmennyiségét és annak megértését.

A hosszan tartó stressz jelen lehet a katona életében, amikor a katona a katonai hadműveleti területről nem tud szabadságra menni és a váltás is hónapokat késik. A katona

egyben bízhat a saját túlélőképességében, ami nagyban függ a katona kreativitásától. Sajnos a stressz csökkenti a kreativitást, néha teljesen elfojtja.

Ha olyan környezetben dolgozunk vagy tanulunk, ahol véget nem érő tennivalókkal és problémákkal találjuk szembe magunkat, akkor az agyunkban lévő neurotranszmitterek nem kapják meg azt az időt, amelyre szükségük lenne a kreativitást megalapozó kapcsolatok létrehozására.

A véget nem érő feladat vagy probléma lehet az a nagy anyagmennyiség is, amit rövid idő alatt kell elsajátítani a katonai kiképzésen. A szoros kiképzési napirend is csökkentheti azt az időt, amit a katona magára tud fordítani. Sokszor nincs idő meditálni vagy átgondolni a kapott információkat. Albert Einstein zenéléssel töltött rengeteg időt, hogy elősegítse gondolkodása számára oly fontos kreatív folyamatokat.

Lesznek, akik bátran néznek szembe a katonai szolgálattal s lesznek, akikben a szorongás érzet az izgalom a félelem fog nőni a sorkatonai szolgálat hallatán. Ez a feszültség kihatással lehet a beilleszkedésre az új viselkedési normáknak történő megfelelésre és a katonai kiképzésre tanulásra.

STRESSZ

A stressz már ismert az ókor óta, ahol feljegyzést készítettek a harctéri stressz hatásairól. A jelen hadviselésben „gránátnyomás", „harci kimerültség" és „harctéri idegsokk" névvel illették [9]. A tény, hogy a harcban álló felek évszázadokon át elismerték, hogy a katona számára emberfeletti megterhelés lehet a háború borzalmait elviselni.

A ma aktív szolgálatot teljesítő katonákat is megviseli a hosszú munkaidő, a fárasztó küldetések és a szeretteiktől távol töltött idő, ami különösen a külföldi missziók idején felerősödik. Ezért sokszor mentális vagy érzelmi problémák sújtják őket, amiket elnyomnak vagy feldolgozatlan formában együtt élnek vele.

De nem csak a szolgálati időben aktív katona van kitéve a stressznek, hanem a háborúból hazatérő vagy leszerelt katona is. A katonákat ilyenkor a pszichiáterhez küldik, ahol diagnózist állítanak ki, amit nem lehet semmilyen vérvizsgálattal, röntgennel vagy az agyról végzett képalkotó vizsgálattal igazolni.

A világ egyik vezető nemzetközi pszichiátere John Rawlings Rees brit dandártábornok 1945-ben a hadseregre, mint a pszichiátria kutatási labor tekintett.

John Rawlings Rees mondása: „A szárazföldi erők és a többi haderőnem különleges kísérleti csoportok, mivel zárt közösségeket alkotnak, és lehetséges olyan kísérletek elvégzése is, amelyek a civilek körében nagyon nehezek lennének." [4].

Az Amerikai Egyesült Államokban a lelki betegségben szenvedő katonák komoly vizsgálata csak a koreai és a vietnami háborút követően kezdődött meg. Az amerikai hadseregben ekkor néztek szembe azzal a ténnyel, hogy egyre több katonájuknál jelentkeznek a már jól ismert tünetek. A betegséget elnevezték a ma is ismert nevén: poszttraumás stressz-szindróma, angolul: posttraumatic stress disorder (a továbbiakban: PTSD). A PTSD nem csak katonákat érintő betegség, sok esetben megfigyelhető a szindróma tünetei olyan civileknél is, akik nagyon súlyos stresszhelyzeten mentek keresztül, éltek át.

A helyzet annyira összetett, hogy a Pentagon mai napokban is 2 milliárd dollárt költ csak a mentális egészségügyre. Ez a költségvetés a Veteránügyi Minisztérium mentális egészségügyi költségvetése szerint a 2007-es 3 milliárd dollárról 2014-re elérte a 7 milliárd dollárt.

A statisztikák azt mutatják, hogy a brit katonák és veteránok öngyilkossági száma 2012-ben nagyobb, mint ahányan csatában elestek. Az ausztrál statisztikák is azt mutatják, hogy a védelmi erők dolgozóinak az öngyilkossági száma az elmúlt évtizedben meghaladja a frontvonalon elesettek számát. Az amerikai hadseregben 2001 és 2009 között 2100 öngyilkosság volt, ez háromszorosa az Afganisztánban meghalt katonák számának, és fele az Irakban elesett összes amerikai áldozat számának. Az amerikai veteránoknál még rosszabb a helyzet, minden 65 percben megöli magát egy amerikai veterán katona – ez 22 fő naponta.

Az MH Egészségügyi Központ pszichológusa Györffy Ágnes szerint „a katonáknál sokkal gyakrabban alakul ki a betegség úgynevezett késleltetett változata". A tünetek várhatóan fél-egy évvel a stresszet kiváltó eseményt követően jelennek meg. Ez azzal magyarázható, hogy a katonák a stresszes események bekövetkeztekor tovább folytatják a katonai műveletet, még akkor is, ha az megviselik őket. Ugyanis a katonai kiképzésen megtanulják, hogy mindenáron helyt kell állniuk, végezniük kell a munkát. Ez viszont nem jelenti azt, hogy később ne legyen problémájuk a feldolgozással.

A tudományos kutatások ebben a témában megállapították, hogy a győztes háborúkat követően radikálisan kevesebb a PTSD-s katona. Ezt úgy magyarázzák, hogy a PTSD könnyebben jelenik meg, ha egy katonában ott van a tehetetlenségélmény. A pszichológusok azt tapasztalták, hogy a falklandi hadjárat után szinte alig jelentkezett poszttraumás stresszben szenvedő katona, míg a koreai, illetve a vietnami háborúkat követően rengeteg mentálisan beteg katona fordult segítségért a szakemberekhez.

Az Amerikai Egyesült Államokban a 2000-es évek két nagy fegyveres konfliktusa után, az iraki és az afganisztáni háborút követően, korábban soha nem tapasztalt számban jelentkezett PTSD-ben szenvedő katona.

Ugyanakkor a szakemberek annak a megakadályozására törekednek, hogy valaki eljusson a PTSD szintig, hiszen belátható, hogy nem minden traumatizáció vezet feltétlenül a PTSD kialakulásához. Figyelve a korai jeleket igyekeznek segítséget nyújtani a páciensnek, ha zavart észlelnek az élményfeldolgozásban.

Ha sikerül a korai szakaszban beavatkozni és segíteni a feldolgozást, akkor ez egy megelőzés lehet a PTSD kialakulásának. Györffy Ágnes szerint: „A közhiedelemmel ellentétben a betegség még akkor is gyógyítható, amikor az már kialakult”. Ugyanis bármilyen traumát fel lehet dolgozni szakemberek segítségével úgy, hogy azzal együtt tudjanak élni a katonák vagy a veteránok.

A stressz nem csak a harcban s utána van jelen a katona életében, hanem a kiképzés során is. A kiképzés során megpróbálnak olyan körülményeket teremteni, ami nagyban hasonlít a harctéren található körülményekhez. Ebben a helyzetben legjobban a fegyelem tudja segíteni a katonát.

A fegyelem pedig nagyban függ az alkalmazkodó képességtől. Vannak, akik nehezen tudnak alkalmazkodni s azoknak minden perc egy küzdés a beilleszkedés szempontjából. Ebben az időben a katona személyiségére komoly lélektani teher nehezedik, amit fokozhat a folyamatos kialvatlanság és a fizikai erőterhelés. Ilyenkor megjelenik az elfogadás a belátás mozzanata, ami azt eredményezi, hogy a katonák belátják nem lehet ezt másképp csinálni s ezt végig kell csinálni.

A belátás nélkül nem lehet a katonai szolgálatot végrehajtani. A gond akkor kezdődik amikor a belátás nem jelentkezik s az előre nem látható események mozgósítják az

egyén elhárító mechanizmusát. Ennek a helyzetnek a kimenetele nem kiszámítható nagyban függ a katona stressz tűrő képességétől, igy a reagálása lehet akár az öngyilkosságig befolyólag minden rendzavarás. Mivel a katona nem tudja feldolgozni az általa átélt sérelmet így megakar szabadulni a feszültségtől, ami nem mindig kiszámítható.

A másik fontos tényező a stresszel kapcsolatban, amikor a bevonult találkozik az első felettesével, aki rögtön utasításokat osztogat neki. A vezetőt vagy parancsnokot nem lehet megválasztani azt kapja az ember, azaz a bevonult rögtön beosztott lesz. A helyzetet súlyosbítja, hogy a katonai ranglétrán a legalsó fokon bevonult állománynak szinte mindenki elöljárója, azaz felettese lesz.

Ilyenkor előjön az empátia, ha szimpatikus a vezető, amit első látásra rögtön megállapíthatunk, akkor könnyebben megy az együtt dolgozás a parancsok elfogadása. Az elfogadás egyes pszichológiai vizsgálatok szerint könnyebb, ha az elfogadni kívánt személy kellemes külsejű.

A kellemes külsőhöz rögtön rokonszenvesebb karaktert gondolunk ehhez hozzátehet még a rendezett környezet is, ami a fegyelmet és áttekinthetőséget sugallhatja. A szabályzatban megadott külső megjelenés a ruha a kulturált hajviselet az alakias mozgás mögött egy határozott vezetőt sejtünk, ami kivívhatja a szimpátiánkat. Ezek fontos tényezők, akkor amikor az életünket bízzuk a másikra mert hisszük, hogy amit megtanít az segít túlélni a lehetetlent a háborút.

Egy szimpatikus vezetőről büszkén beszélünk a barátainknak s megnyugvással tölti el a bevonult állományt, hogy jó kezekben van. Viszont, ha nem sikerül kivívni a szimpátiát, ami gyakran a találkozás első perceiben kialakul az további passzivitást vagy legrosszabb esetben kétkedést szül a vezetővel szemben.

Ilyenkor megkérdőjelezhetik a vezető döntéseit, a parancsok végrehajtása vontatottan történhet, szervezkedhetnek a vezető ellene, vagy másik tiszt, felettes oltalmát közelségét keresik. A parancsnok ebben az esetben azt veheti észre, hogy nehezebb a katonák érdeklődését fenntartani, nehezebb őket motiválni.

A kiképzendő katona kerülhet olyan helyzetbe, ami meghaladja az ő tűrési határát s elképzelhető, hogy ilyenkor pánikba esik. A pánik a legveszélyesebb lélektani helyzet, ami előfordulhat az egyén és a közösség szempontjából. A pánikba esett személy és közösség nem tudja kontrolálni magát mert megszűnik az értelem irányító szerepe és a menekülés a helyzetből lép első helyre, így az események irányítása lehetetlenné válik.

A történelem során katonai jellegű pánikot például 1915-ben és 1945-ben jegyeztek fel. 1915-ben Ypern belga falu mellett egy meglepetés szerű gáztámadást hajtottak végre, ami során a védekezésben lévő katonák 6 km széles vonalon a fegyvereiket eldobálva elmenekültek. 1945 tavaszán a Balaton és Vértes között a németek ellentámadást hajtottak végre a szovjet csapatok ellen s a támadó ék gyorsabban nyomult előre, mint a hadtáp, így közöttük akadozott az információ áramlás. Valami oknál fogva elterjedt a leszakadt hadtáp egységeknél, hogy a szovjetek körbe kerítik őket, ami nagy pánikot okozott a katonák között és ott hagyva állásaikat visszavonultak. A helyzetet nem tisztázta senki, a katonák információ nélkül maradtak, ami tovább növelte a pánikban résztvevők számát.

A pánik helyzetet megelőzi általában egy hosszabb terhes időszak, ami lehet egy katonai hadművelet előtti várakozás, ez kiválthat az érintetteknél egy szorongást a fenyegetéstudatuk miatt.

A pánik reakcióhoz mindenképpen kell egy személy, aki elindítja ezt a folyamatot a tömeg pedig követi őt. A pánikba esett katona a pánik végén kimerült lesz, és ilyenkor válik közönyössé, elveszti az energiáját. Ez az állapot pont akkor éri el a katonát, amikor a tényleges veszélyt kéne leküzdeni.

A kiképzés során kell megtanulni a katonáknak az elfogadást, ami nincs időkorlát-hoz kötve, mindenkinél a saját ritmusa szerint alakul ki. Ezért a kiképzési folyamat sem stressz mentes igy ez befolyásolja a tanulást is.

TANULÁS A FÉLELEM ÁRNYÉKÁBAN

A félelem általában egy jövőbeli eseményhez, eseményekhez kapcsolódik, jelen esetben egy katonai bevetésen való részvétel vagy a bevetés alatt szerzett sérülés elszenvedése. A félelemmel gyakran együtt jár az érzelmi szorongás állapota, amelyre jellemző, hogy általában külső fenyegetés nélkül lép fel. „A félelem kapcsolatban van a menekülési és az elkerülési viselkedéssel, míg a szorongás a veszélyek eredménye.” [8].

A félelem az enyhe figyelmeztetéstől egészen a fóbiáig vagy paranoiáig terjedhet. A félelem kapcsolatban áll több érzelmi állapottal, mint például az aggódás, szorongás, rémület, a horror a pánik és a rettegés. Az alábbi két oszlopban megtalálhatók azok a félelmet kiváltó okok, amik jelentkezhetnek egy újoncnál.

tapasztalatok hiánya	kiképzők
saját fantáziám	fegyverhasználat
leszerelt katonák meséi	éjszakai szolgálat
bizonytalanság	ügyelet
öreg katonák	felelősség vállalás
megfelelés	katonai technika
fizikai megterhelés	megszégyenülés
tanulás	beilleszkedés
kiképzés	elfogadás
szülői szeretet hiánya	család hiánya
magány	komfortzónából kilépés
fegyelem	stressz
alkalmazkodás	érzelmi teher
változás	büntetés
gyakorlatokon részvétel	döntéshozatal
kialvatlanság	korlátozások
erőpróbák	beosztottak vezetése
szokások elhagyása	egészségre káros dolgok

A feljebb felsorolt félelmet kiváltó okok nem teljesek hiszen ez nagyban függ az egyéntől is. A bevonult katonák hozzák magukkal az otthoni kultúrát, szokásokat, szocializációt, amihez hozzájön az életben személyesen megtapasztalt dolgok.

A félelemnél kapcsolatban fontos tisztázni, hogy a félelem reális-e, vagy esetleg irreális. A veszélyforrás, ami kiváltotta a félelmet megtalálható a környezetünkben vagy nem létezik. Ezek nehezen eldönthető kérdések. A személyiségünk folyamatosan működtet

egy realitáskontroll-funkciót, ami folyamatosan vizsgálja a belső világunk értékelő folyamatait és az általuk létrehozott értékeléseket és viselkedéses reakciókat azért, hogy összhangban legyenek a külvilág eseményeivel. Sajnos a szorongás vagy a hosszan tartó stressz ezeket a realitáskontroll-funkciókat károsítja. Ez azt jelenti, hogy a félelmeink megmagyarázhatatlanul naggyá növekedhetnek, vagy a félelmeink a valóságban nem is létező tárgyat, személyt találnak maguknak. Ilyen esetben az irreális félelmeket csak úgy lehet kontroll alatt tartani, ha a realitáskontroll-funkciót helyreállítjuk. A bizalmatlanság is lehet egy irreális veszélyforrás.

A bizalmatlanság jelenléte általában egy ismeretlen szituáció vagy személlyel szemben alakulhat ki, azaz. bekövetkezhet, mint egy veszélyérzet. A bizalmatlanság megjelenése felfogható egy korai figyelmeztető jelzésnek olyan szituációkkal kapcsolatban, amik tragikusabb félelemre vagy veszélyre mutatnak. A megnyugtatás általában csökkenti vagy eltünteti a félelmet, mint például, ha ismételten többször csinálunk valamit. A békeidőben történő katonai kiképzés lehetővé teszi a folyamatok ismétlését, igy az esetleges félelmek elkerülhetőek.

A félelem oka lehet például egy személyesen átélt nyomasztó esemény megélése. Néhány kutatás rámutatott, hogy a félelem megtanulása független attól, hogy mi magunk élünk át egy traumát, vagy mások félelmeit figyeljük. Ez azt jelenti, hogy egy leszerelt katona is átadhatja félelmeit egy még be nem vonult leendő katonának csupán egy ártatlan beszélgetés folyamán.

„A memória szorosan összefügg a tanulással” [5]. A tanulás szorosan összefügg a figyelemmel a koncentráció képességével. Ezen kívül a felejtés is fontos tényező a tanult dolgok megtartásában. Hermann Ebbinghaus kidolgozott egy felejtési görbét a kutatásai nyomán, amit 1885-ben publikált az -Über das Gedächtnis- név alatt. Az 1.ábra sematikusan ábrázolja a felejtés görbét.

1. Ábra: Felejtés görbe, [101].

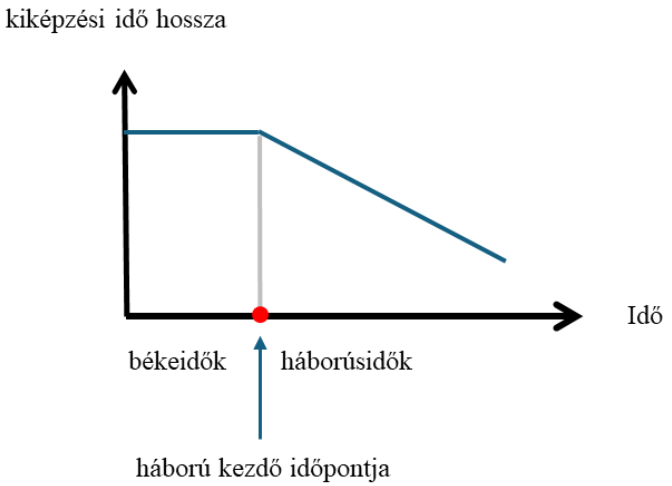
Az 1.ábra szerint a felejtés a tanulás után rögtön megkezdődik és az első nap végén már csak a 80%-ra emlékszünk a megtanultaknak. A negyedik nap végére pedig csak az

50%-t vagyunk képesek felidézni. Ez egy kiegyensúlyozott stressz mentes környezetben történő felmérés szerint, ahol minden körülmény közelíti az optimálisat.

Azonban, ha a körülmények nem optimálisak például az egyén frusztrált, ideges, feszült és nem tud koncentrálni, mint ahogy elvárnánk tőle, igy az eredmény is elmaradhat. Ha az oktatás alatt az anyag 80%-án volt képes figyelni úgy egy nap után a leadott anyag már csak a 64%-ra fog emlékezni. A negyedik nap végére a leadott anyag már csak a 40%-t képes felidézni.

A gondot fokozza az is, hogy a figyelés az órai anyagra nem folyamatos, hanem megszakításokkal teletűzdelt, igy az egésznek csak részei maradnak meg, amiből nehéz kikövetkeztetni az egészet és sokszor nem is lehet pótolni a hiányokat, igy egy használhatatlan tudás marad az oktatáson résztvevő fejében.

A tanult anyag hosszútávú eltárolását segíti az ismétlés mert az ismétlés során újból kezdődik a felejtés folyamata csak lassabban. Béke időben van lehetőség ismétlésre gyakorlásra viszont háborús időben a kiképzésre szánt idő drasztikusan rövidülhet hiszen a veszteségek pótlása a lehető leggyorsabban kell, hogy végbe menjen. A csökkent kiképzési idő csökkent átadott tudásanyagot jelent, aminek a megtanulását csökkenti az a stressz is, ami abból adódik, hogy a kiképzett állomány rögtön katonai bevetésre megy. A 2. ábra szemlélteti a békeidő és a háborúsidő közötti oktatásra fordított kiképzési időkülönbséget.



2. Ábra: Kiképzési idő, saját szerkesztés.

A 2.ábra nem tartalmaz pontos időintervallum számokat mert ez nagyban függ a háború menetétől és az adott ország kiképzési struktúrájától. A háborús időben a kiképzésre szánt idő töredéke lehet a békeidőben elvégzett kiképzési hossznak, amit jól szemléltet a 2. ábra.

A katonai kiképzés során a megtanultak között vannak saját és ellenséges csapatokról adatok, mint például rangjelzések, térképjelek, katonai felségjelzések, zászlók, címerek és a katonai lőszereken használt szín jelölések.

Az a civil, aki nem foglalkozott a katonai szín és formavilággal egy rövid intenzív katonai kiképzésen való részvétel után a kapott sok információ miatt reménytelennek találhatja helyzetét.

AZ MI SEGÍT

A szorongás a katonai szolgálattal szemben sokszor nem a szolgálat nehézsége adja, hanem azok a faktorok, amiket még nem ismerünk. Ilyen faktor lehet rögtön a bevonuló állománnyal szemben a katonai rendfokozatok ismeretének a hiánya.

A rendfokozatok látható helyen színes vállappal és csillagokkal teletűzdelt forma, ami különböző színben fordul elő a gyakorló, hétköznapi és az ünnepi viseleten. Ezt nehezíti, hogy 2025-ben már 32 Észak Atlanti Szövetség (a továbbiakban: NATO) tagország létezik s mindegyiknek egyedi rangjelzése van. A katonai szolgálat során alkalom nyílik a NATO tagországokkal közös gyakorlatokon reszt venni, ezért fontos felismerni a baráti hadseregek rendfokozati jelzését.

A NATO katonai rendfokozatai igen változatos képet mutatnak, ami több mint 1500 egyenruhából és rendfokozati jelzésből áll. „Megkülönböztetünk jelzést, amit rávarrnak a ruhára és megkülönböztetünk jelvényt, ami fémből készül és azt az egyenruhára felfüggesztve vagy feltűzve viselik.” [6].

A katonai rendfokozatok és jelvények szín és forma felismerésére legalkalmasabb a gépilátás. Egy ilyen eszközzel, ami a gépilátás alapján működik, segíteni lehetne a sorkatonát a tanulásban az ismétlésben. Egy ilyen eszköz gyakorlatilag részben átvenné az oktató szerepét és mindegy katonai fordító gép segítené a sorállományt a számukra új katonai információ befogadásában.

Nem csak katonai rendfokozatokban vannak színek és formák, hanem más katonai eszközöknél is mint például a fegyvereknél és a lőszereknél. A 2019-ben megjelenő katonai fegyvereket bemutató enciklopédiában több mint 800 különböző típusú és alakú fegyvert ismertetnek [105].

A modern kori háborúkban keverednek a legújabb fegyverek a régebbivel a keleti fegyverek a nyugati fegyverekkel. Egy ilyen harctéren a talált fegyverek azonosításához jó segítséget jelenthet egy gépilátással működő eszköz, ami alakról felismeri és kiegészítő adatokkal ellátja a fegyver találóját.

Továbbá színekkel találkozhatunk a katonai járművek felség jelzésénél is. A katonai jelképeket és jelzéseket a 5/2021. (VIII. 11.) HM rendelet a katonai jelképekről és jelzésekről, valamint a Magyar Honvédséghez köthető megjelölésekről és használatuk engedélyezéséről szóló rendelet szabályozza [7].

Az országok zászlajaiban is egyedi színek jelölik az országot. Sokszor ugyan az a szín kombináció más országot jelöl. Például a piros, kék, fehér szín 11 NATO ország zászlajában is szerepel. Stresszes helyzetben csak a biztos tudás és a tapasztalat nyújt segítséget a zászlók és formák felismerésében.

Az MI ma már nem csak a tudományos-fantasztikus irodalom és filmek része, hanem megjelent a hétköznapjainkban is és egyre inkább kikerülhetetlen. A továbbiakban áttekintek néhány MI lehetséges alkalmazást, amit a katonai területen egy kiképzendő is tudna használni.

Információkeresés

Az MI fejlődése lehetővé teszi, hogy a keresőmotorokba ne csak merev kulcsszavakat gépeljünk, hanem a virtuális asszisztenseknek köszönhetően az MI képes megérteni a komplex kérdéseket, amik katonai tartalomra is mutathatnak. A kérdésre adott válasz nem

csak linkek listáját adja vissza, hanem egy összefoglalt válaszokat szintetizálnak több katonai forrásból. Igy a természetes nyelven megfogalmazott kérdésre katonai szakanyaggal és terminológiával kibővített választ kaphatunk. A katonai szakszavakat nem ismerő is rá tud keresni katonai tartalmakra, ami az ismeretszerzést könnyíti meg.

Szövegösszefoglalás, lényegkiemelés

A keresés során megtalált katonai anyagok akár hosszú cikkek, tanulmányok, publikációk vagy könyvek átolvasása sok időt igényelhet, ami egy feszült stresszes állapotban lévő újoncnak igen megterhelő. Az MI már bizonyított abban, hogy ezeknek a terjedelmes katonai szövegeknek a lényegét kiemelje, és egy lényeget kiemelő összefoglalót készítsen belőlük. Az MI észreveszi a főbb pontokat, kulcsérveket és következtetéseket, emellett viszont figyelmen kívül hagyja a kevésbé releváns részleteket. Ez rendkívül praktikus lehet a katonai adatok feldolgozása során, minden olyan katonának, aki koncentráció zavarral küzd és hosszan tartó figyelemre képtelen. Az automatizált összefoglalást kérhetjük különböző szóterjedelemben, ami jelentősen hozzájárul az információfeldolgozás hatékonyságához.

Nyelvi akadályok leküzdése

Magyarország a NATO tagja, ahol az angol, német és a francia nyelvek az elfogadott beszélt nyelvek. A tapasztalat azt mutatja, hogy a bevonultatott állomány egy kis része beszél valamilyen idegen nyelven. Ezért fontos lehetne egy gépi fordítást végző eszköz, ami a katonának bármikor és bárhol a rendelkezésére állna. A modern MI alkalmazásokban már elérhető a gépi fordítás, ami az egyik legismertebb és leggyakrabban használt alkalmazás. A modern MI programok nagy pontossággal képesek fordítani katonai szövegeket és akár beszédet is tucatnyi nyelv között. Ez igen fontos lehet a NATO-n belüli gyakorlatokon és együttműködéskor, ami lehetővé teszi a globális kommunikációt és a csapatok közötti együttműködést. Ezek a fordítóprogramok használhatóak egy külföldi weboldal katonai tartalmának megértésére, egy NATO partnerrel folytatott e-mailezésre vagy egy NATO partnertől kapott idegen nyelvű dokumentum lefordítására. A nyelvi tudás növelné a katona biztonságérzetét.

Szöveggenerálás

Sorkatona is kerülhet olyan szituációba, ahol jelentést kell írnia az átélt vagy tapasztalt eseményekről, ilyenkor a fogalmazási képessége előtérbe kerül. Ilyen esetben fontos a fogalmazás stílusa a katonai szakszavak használata és a lényegre törő magyarázat. Az MI itt is tud segíteni ugyanis az egyik leglátványosabb képessége az MI-nek a szöveggenerálás. Képes különböző stílusú és formátumú szövegeket létrehozni az egyszerű e-mailektől a különböző jelentésekig vagy akár a komplexebb technikai dokumentációkig. A katona megadhat bizonyos kulcsszavakat, egy témát és a kívánt hosszúságot, az MI pedig ezek alapján generál egy releváns szöveget vagy jelentést. A szöveggenerálásával csökkenthetjük azt a stresszt, amit a katona átélt az iskolában fogalmazás alkalmával, így az akkor átélt szorongás vagy félelem jelentősen csökkenhet.

Képgenerálás

Az MI képes kép generálására is néhány szöveges információ megadása alapján. Ez hasznos lehet előadások megtartásakor illusztrálni az elmondottakat vagy a katonai technikai leíráskor ábrák készítésénél. Nem mindenki tud rajzolni így ez a képesség az MI részéről igen hasznos tud lenni a vizuális katonai tartalom készítésekor.

Virtuális asszisztensek

A katonai technikák megtanulásakor jól alkalmazható egy virtuális asszisztens, ami lépésről lépésre bemutatja és nyomón kíséri a technika megtanulásának a folyamatát. Az MI alapvetően segít az ember-gép kommunikációban, így az összetett katonai technikák alkalmazásának a megtanulásában is tud segíteni mivel nem kell hozzá kiképző jelenléte és a magyarázat az elsajátításig újra játszható. Ez azt jelenti, hogy nem kell félnie a kiképzendőnek a kiképző büntetésétől vagy a gyakorlat helytelen elvégzéséből fakadó szégyenérzettől.

Nyelvtanulás

Az MI funkcionálhat beszélgetőpartnerként és ez a tulajdonsága teszi lehetővé nyelvtanulásra. A katona szabadidejében interaktív beszélgetőpartnerként használhatja ezt a funkciót anélkül, hogy félnie kellene a hibázástól. Beszédfelismerés és beszédszintézis segítségével képes a nyelvtant elmagyarázni, szókincset bővíteni, kiejtést javítani és katonai beosztástól függően gyakorló feladatokat generálni a katona aktuális tudásszintjének megfelelően. Ez azt jelenti, hogy a katonának nem kell a többiek előtt szégyenkeznie a rosszul kiejtett szavak és a nem pontosan megfogalmazott mondatok miatt.

Komplex problémák elemzése

A katonák gyakran néznek szembe komplex problémákkal. Az MI segítségével ezek a komplex problémák szétszedhetőek kisebb részekre, azonosítani lehet a kulcsténye-zőket, fel lehet tárni az ok-okozati összefüggéseket. Az MI képes strukturálni az információkat, és segít a probléma mélyebb megértésében. Például egy katonai logisztikus használhatja az MI-t a katonai utánpótlás tervezésére, elemzésére, figyelembe véve a szükségletet, az eljuttatási útvonalakat, az infrastrukturális korlátokat.

Alternatív megoldások keresése

Stresszes állapotban egy probléma megoldása nagy kihívás lehet mindenkinek nem beszélve az esetleges alternatív megoldások kereséséről. Ilyenkor segíthet az MI. Ha a probléma egyértelműen definiált, az MI felajánlhat különböző megoldási javaslatokat. Az MI képes kreatív és akár nem konvencionális megoldásokat is felvetni, amelyekre stresszes állapotban nem gondoltunk volna. A javaslatait értékelheti megmutatva a különböző opciók előnyeit és hátrányait.

Optimalizálás

Katonai életben a folyamatok vagy rendszerek folytonos optimalizálására a hatékonyság növelésére, a költségek csökkentésére vagy az erőforrások jobb kihasználására van szükség. Az MI alapokon nyugvó algoritmusok teljes mértékben megfelelnek az optimalizálási problémák megoldására. Jó példa erre a katonai logisztika, ahol a legrövidebb vagy leggyorsabb szállítási útvonalak megtalálása emberéleteket menthet.

Oktatás

Katonai kiképzés egy sor oktatási anyagból áll különböző témákból, aminek a megtanulása odafigyelést és gyors memorizálást igényel. Az MI képes személyre szabott tananyagot és feladatokat generálni ezért a legjobb mértékben alkalmazkodik a felhasználó igényeihez. Felismeri a tanulók egyéni tudásszintjét, tanulási stílusát és tempóját. Képes interaktívan a kérdéseket megválaszolni. és azonnali visszajelzést adni a teljesítményről.

Ennek köszönhetően minden diák a saját tempója szerint tud haladni, és ott kap kiegészítő segítséget, ahol a tananyag elsajátításában nehézsége van.

ÖSSZEFOGLALÁS

A stressz egyre inkább a mindennapjaink része. A stresszből eredeztethető betegségek egyre több embert érintenek, nemcsak a civil, de a katonai életben is. A stressz nemcsak a katonai szolgálatra behívottakat érinti, hanem azok hozzátartozóit is, hiszen ki ne aggódna, ha gyermekét egy veszélyes tevékenység elvégzésére kérnék fel.

A stressz a katonai kiképzésre is rányomja bélyegét. A stressz hatására a katonák koncentrációs képessége csökkenhet, ami a tanulás egyik kiemelten fontos eleme. Ha kiképzés során nincs idő ismétlésre az az elsajátított anyag megértésének a romlását okozhatja.

A stressz leküzdésében nagy segítséget adhat a társas kapcsolataink, mint például a barátok, a család, akik növelhetik az önértékelésünket vagy felvilágosításokat és tanácsokat adhatnak és elvonhatják figyelmünket a szorongásról.

Az MI fejlettsége már alkalmassá teszi a különböző adatok feldolgozására, kiértékelésére, összegzésére, így egy igazi társa lehet a katonának, akit elláthat kiegészítő adatokkal, fordítással és akár katonai szakszavak értelmezésével.

Az MI képes a katonai életben használt szín és formavilág felismerésére, értelmezésére, ami nem csak a kiképzés során, hanem a hadműveleti területen is nagy segítség lehet a katonának.

Az MI-vel felszerelt eszköz kezelése hozzájárulhat a digitális kompetenciák növeléséhez, ami elvárás az Európai Unióban. A katonák, akik a civil életben nem foglalkoztak mélyebben a digitális kultúrával azok most rákényszerülnek használni egy ilyen katonai fordító gépet mert az életüket könnyíthetik meg vele. Gyorsabb lesz a tanulás és magabiztosságat adhat.

FELHASZNÁLT IRODALOM

[1] Trend FM „A Nap Vendége” című műsora 20022. december 13, [Online]. Elérhető: https://trendfm.hu/musor/a-nap-vendege-10

[2] Nagy Ervin, *Fegyelem, stressz, közösség*, Budapest, Zrínyi Katonai Könyv- és Lapkiadó, 1989.

[3] Mark Simmonds, *Siker&Szorongás*, Budapest, Partvonal könyvkiadó, ISBN: 978-963-609-029-6, 2024.

[4] Állampolgári Bizottság az Emberi Jogokért, *Katonákon végzett kísérletek*, 2024, [Online]. Elérhető: https://www.cchr.org.hu/documentaries/the-hidden-enemy/experimenting-on-troops.html#footnote1

[5] Peter Hollins, *Szupertanulás*, Budapest, GLB Könyvkiadó, ISBN: 978-963-630-172-9, 2024.

[6] Brian L. Davis, *Egyenruhák és rendfokozatok a NATO-ban*, Budapest, Zrínyi Kiadó, ISBN: 963 327 322 6, 1999.

[7] 15/2021. (VIII. 11.) HM rendelet a katonai jelképekről és jelzésekről, valamint a Magyar Honvédséghez köthető megjelölésekről és használatuk engedélyezéséről, [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a2100015.hm

[8] Öhman, A., Fear and anxiety: Evolutionary, cognitive, and clinical perspectives., In M. Lewis & J. M. Haviland-Jones (Eds.). Handbook of emotions. (pp.573–593). New York: The Guilford Press, 2000.
[9] Bódizs B. (ford.), *Stressz*, Budapest, Glória Kiadó, 2000.
[10] K Srí Dhammánanda, *Miként éljünk Félelem és aggodalom nélkül*, Budapest, Kelemen Kiadó, 2009.
[11] Belső Nóra, *Félelem, szorongás, pánik*, Budapest, Hvg Könyvek, 2022.
[12] Jonathan Davidson, *A szorongás öt arca*, Budapest, Alexandra Kiadó, 2005.

DOI: https://doi.org/10.12700/btsz.2025.7.2.49

DIGITAL DATA PROTECTION AND INFORMATION SECURITY: SOURCES OF DANGER IN THE ONLINE SPACE, METHODS OF PHISHING (SOCIAL ENGINEERING)

ADATVÉDELEM ÉS INFORMÁCIÓBIZTONSÁG: AZ ONLINE TÉRBEN FELLELHETŐ VESZÉLYFORRÁSOK, ADATHALÁSZATI-MÓDSZEREK (SOCIAL ENGINEERING)

CSERCSA Klaudia[1] – RAJNAI Zoltán[2]

Abstract

Enhanced protection of data and information security are areas of high importance these days. The misuse of data that has fallen into the hands of unauthorized persons has reached unprecedented proportions. In the online space, we can face many phishing techniques, so conscious use and up-to-date information and device protection are essential in our daily lives. Social engineering techniques are diverse and creative, so constant vigilance is essential when logging into each application. Cyber attacks are a threat to an individual's life in the same way as they are to a small or medium-sized company, a multinational company or a country or nation.

Keywords

data protection, information security, social engineering, phishing

Absztrakt

Az adatok fokozott védelme és az információbiztonság kiemelt fontosságú terület napjainkban. Korábban sosem látott méreteket ölt az illetéktelen személyek kezébe került adatokkal való visszaélés. Az online térben számos adathalászati technikával szembesülhetünk így a tudatos felhasználás és a naprakész információ és eszköz védelem elengedhetetlenül fontos a mindennapi életünk során. A social engineering technikák sokrétűek és kreatívak, így elengedhetetlen a lankadatlan éberség minden alkalmazásba történő bejelentkezés során. A kibertámadások veszélyt jelentenek egy magánszemély életében ugyanúgy, ahogyan egy kis vagy középvállalat esetében, egy multinacionális cégnél vagy egy országnál, nemzetnél.

Kulcsszavak

adatvédelem, információbiztonság, social engineering, adathalászat

[1] claudiacsercsa@gmail.com | ORCID: 0000-0003-2800-9106 | PhD student, Obuda University | doktorandusz hallgató, Óbudai Egyetem

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

BEVEZETÉS

A bűnözés ezerarcú szörnyeteg, kiismerhetetlen, megfoghatatlan, napról napra megújul, alakot vált. Ebből a jellegéből fakadóan válik annyira nehézkessé a prevenció. Mikor megtanulunk védekezni valamely formája ellen, rögtön megjelenik új alakban. Ez hatványozottan igaz az online térben történő visszaélésekkel kapcsolatban. Az elkövető arcát, legtöbb esetben még a hangját sem tudjuk azonosítani, sőt olyan is megtörténhet, hogy tudatában sem vagyunk annak, hogy kiberbűnözők áldozataivá váltunk. Az elkövetések módja olyannyira változik, mondhatjuk olyannyira naprakészek a tettesek, hogy komoly kihívást jelent a hétköznapi állampolgárok védelme. Minden online platformon, minden egyes linken, melyre kattintani lehet, ott leselkedik a veszély a gyanútlan felhasználókra, melyek gyakran nagy áldozatot követelnek. Az oktatás és a tudatos jelenlét az online térben korábban sosem tapasztalt fontosságú területté vált napjainkra. Minden felületen komoly károkat tudnak okozni az illetéktelen behatolók. A védelem minden platformon indokolt, de vannak kiemelt súllyal bíró területek. Az is veszteséggel jár, ha jogosulatlanul használják fel vagy tárolják a személyes adatainkat, fényképeinket, social media felületeken fellelhető adatainkat, de az online térben történő károkozás banki tevékenységünket még hatványozottabban fenyegeti, gazdasági helyzetünket, egzisztenciális állapotunkat szüntelenül veszélynek kitéve. A bankokra és pénzintézetekre nagy nyomás nehezedik, hogy védje a partnereik adatait és biztonságát.

Napjainkban igen használatos kifejezéssé vált a social engineering. Széles körben elfogadott, egzakt definiálása még várat magára, több kutató is vizsgálat tárgyává tette már a jelenséget. A közös metszet, hogy kibertámadási technikák gyűjtőfogalma, azonban a social engineering fogalmán belül többféle elnevezéssel is találkozhatunk egy-egy technika bemutatása során és a technikákat különböző szempontok alapján csoportosították az egyes kutatók. Ezeket kerülnek ismertetésre a továbbiakban.

SOCIAL ENGINEERING

A social engineer tükörfordításban társadalmi mérnökök, egy kifejezés, mely arra utal, hogy néhány ember a társadalmi manipulációikat mérnök szintre fejlesztette fel. Ugyanakkor a magyarosított kifejezést nem használjuk, így az angol megfelelőjét alkalmazzuk a továbbiakban. A social engineer-ek ugyanazokat a meggyőzési technikákat alkalmazzák, mint mi hétköznapi emberek a mindennapjaink során. Szerepeket játszunk, igyekszünk hitelességet teremteni, viszonozzuk a szívességeket. A social engineer-ek azonban manipulatív, megtévesztő, erősen etikátlan módon használják ezeket a technikákat, gyakran elsöprő sikerrel. [1]

Bár a pénzügyi bűnözés motivációja magától értetődőnek tűnhet, nem ez az egyetlen motiváció. Sok esetben kiderül, hogy egyes elkövetőket nem a haszonszerzés, az anyagi javak növelése, hanem a szakmai kíváncsiság és a kalandvágy, vagy valamilyen (vélt vagy valós) sérelem vagy személyes bosszúvágy motivál. Emellett egyes országok nemzeti érdekből, más esetben terrorista szervezetek vagy bűnszövetkezetek politikai célok elérésére irányulva hajtanak végre kibertámadást a védett infrastruktúrák –például a pénzügyi szektor – ellen.” [2]

A legjobb példa erre a social engineering egyik legkiemelkedőbb egyénisége Kevin Mitnick, aki az amerikai FBI egyik legkeresettebb ifjú bűnelkövetője volt az 1980-as években. Több nagyvállalat informatikai rendszerébe hatolt be illetéktelenül, anyagi, illetve bármilyen egyéb haszonszerzési cél nélkül. Kizárólag az izgalom, a hecc kedvéért. Az ifjú kiberbűnöző, büntetőjogi felelősségre vonása után, 2023. júliusban bekövetkezett haláláig harcolt a kiberbiztonság megerősítése érdekében. [3] [4] [5]

Munkássága sokat hozzátett az online tér biztonságosabbá tételéhez. Sok hiányosságra és veszélyre hívta fel a közvélemény figyelmét a rablóból lett pandúr. Könyvében úgy határozza meg a social engineering fogalmát, hogy az adathalász meggyőzi az áldozatát arról, hogy ő valaki más, akinek éppen eljátssza a szerepét attól függően, hogy milyen szerepre van szüksége ahhoz, hogy a hőn áhított információt megszerezze. Nagyon jól ért a manipuláláshoz és az emberek megtévesztéséhez. Az adathalász kialakít egy bizalmas légkört az áldozatával és a bizalmába férkőzik. [6]

A social engineering fogalmát megfeleltethetjük magyarul pszichológiai manipuláció vagy pszichológiai befolyásolás gyanánt is. Ezen támadások ellen elsősorban nem technikai eszközök alkalmazásával kell védekezni, hanem a felhasználói ismeretek széles körben kiterjesztett oktatása és ismeretnövelése által. Ezekben az incidensekben nagy hangsúly van az emberi természet megismerésén, az emberek megtévesztésén és nem a technológiai eszközök sebezhetőségével él vissza a támadó. A módszer lényege, hogy több esetben egy bizalmi viszony alakul ki az elkövető és az áldozat között, mely során értékes információkat nyer meg a támadó és ezt saját érdekére fordítja és kihasználja az áldozat óvatlanságát, jóhiszeműségét. Más helyzetben pedig a célszemély vagy inkább kiszemelt áldozat figyelmetlenségéből fakadhat a károkozás.

FOGALMAK AZ IT ALAPÚ TUDÁST NEM IGÉNYLŐ ADATHALÁSZATI TECHNIKÁKKAL KAPCSOLATBAN

Ezek az adathalászati módszerek igen hétköznapiak és ezek a legveszélyesebbek az elkövetők szempontjából, hiszen ezekkel a módszerekkel a legnagyobb a lebukás veszélye. Jellegükből fakadóan többnyire fizikai jelenlétet is igénylő információ szerzésre irányuló technikák, de némelyik adathalász módszer elkövetése során csak a hangját használja a támadó. De ez is egy közvetlen kapcsolatot alakít ki a támadó és az áldozat között. Ezek a módszerek komoly felkészülést és lélekjelenlétet követelnek az alkalmazásuk során.

Az első taktikai lépés a környezet felderítése a lehető legrészletesebb módon. Minden jelentéktelennek tűnő információt meg kell jegyezni. Meg kell ismerni, hogyan veszik fel a telefont, hogyan köszönnek egymásnak, vannak-e sajátos nyelvi fordulatok, frázisok, milyen szakmai nyelvezetet használnak a kiszemelt egységnél, hogyan működnek a napi rutinok és hol lehet elérni a különböző osztályokat. Van-e beléptető rendszer, hogyan működik, mikor vannak a szünetek, kik és mikor mennek el dohányozni és hová. Ezeknek az információknak a birtokában már sokkal könnyebb észrevétlenül elvegyülni és beépülni egy cég életébe. [7]

Vishing: A támadó telefonhíváson keresztül igyekszik az áldozat bizalmába férkőzni és megszerezni a számára értékes információt. Ehhez a módszerhez gyakran üzletkötőnek adják ki magukat az adathalászok és így próbálják meg elérni céljukat. Ehhez a módszerhez is tanácsos már előre informálódni az áldozatról. Gyakori eset, hogy banki vagy valamilyen egyéb pénzintézet alkalmazottjának adják ki magukat a csalók és a gyanútlan

áldozatok megadják a bankkártya adataikat. Emellett személyes adatokat is könnyedén meg tudnak szerezni a támadók, ha sikerül egy bizalmas légkört kialakítaniuk. Mitnick például egy magasan védett intézmény rendszerébe tudott betörni annak a módszerének köszönhetően, hogy telefonos adategyeztetés keretében felhívta a kiszemelt áldozatot és helytelenül adta meg a kódot, amit az ügyintéző rögtön kijavított a helyesre. Így sikerült is hozzáfernie a bizalmas információhoz, hiszen az emberek ilyen esetben nem gyanakodnak. [7]

Dumpster diving (Kuka búvárkodás): Többször előfordul, hogy nem kellő körültekintéssel semmisítik meg az emberek a dokumentumokat mielőtt kidobnák a szemetesbe. A támadó kereskedelmi vagy lakossági szemét tárolókban keresgél. Először információt gyűjt a kukák tárolásáról, elszállításáról majd a kuka tartalmát átvizsgálva kerül értékes információk birtokába, amelyek alapján a későbbiekben csalást vagy lopást tud elkövetni. A módszer egyszerű és hatásos, a támadó időről időre átnézi a kiszemelt áldozata kidobott hulladékait. Ajánlatos minden dokumentumot megfelelő körültekintéssel megsemmisíteni.

Pretexting: A támadás olyan formája, amelyben a támadó előzetesen információkat készít az áldozatról akár nyílt forrásból, akár adathalászatból, és többnyire legtöbbször telefonon próbál meg minél több információt megszerezni.

Eavesdropping – vagyis a hallgatódzás: Egy régi, jól bevált módszer amikor mások beszélgetésére figyel valaki jogosulatlanul. Ha egy illetéktelen harmadik fél lehallgatja két fél beszélgetését, akár személyesen, akár telefonon, akkor gyakran fontos adatok gyűjthetők össze. Ha a lehallgatást számítógéppel végzik, a támadó kihasználhatja a hálózati kommunikáció bizonytalanságát, hogy hozzáférjen a küldött és fogadott adatokhoz. Az ilyen támadásokat nehéz észlelni, mert nem okoznak hálózati átviteli rendellenességeket. Kiemelendő, hogy milyen környezetben kivel, mit beszélünk meg. Az igazán bizalmas információk közlése során még hangsúlyosabb tényező a körültekintés.

A shoulder surfing – vagyis a váll feletti leskelődés: Egy igen egyszerű módja valamilyen PIN-kód vagy jelszó megszerzésének. Az adathalász személynek nincs közvetlen kapcsolata az áldozattal, de közel van az áldozatához. Mögé áll, és közvetlenül az áldozat válla fölött néz, hogy megfigyelje, amint az áldozat melyik billentyűket gépeli be az adott felületen. Közben természetesen viselkedik, úgy tesz, mintha valami fontos dolga volna és észre sem venné az áldozat gépelését. A legelterjedtebb esetek a PIN kódok lelesése például a pénzkiadó automatáknál, de gyakori incidensek a beléptető rendszerek, kaputelefonok kódjai. Az is előfordulhat, hogy valamilyen szerkezet segítségével (például távcső vagy kamera esetleg jól beállított tükör) messziről próbálják megszerezni a PIN kódot. A legegyszerűbb módja annak, hogy megvédjük magunkat ettől a fajta támadástól, ha figyeljük a mögöttünk álló személyt, és a kód beírása közben letakarjuk a kijelzőt. [8]

Segítségkérés-segítségnyújtás: A támadó az emberek segítőkészségére támaszkodva csal ki információkat. A hibát maga a támadó is okozhatja, így ő teremti meg a helyzetet, ahol segítségét felajánlva szerez meg bizalmas információkat.

Tailgating-besurranási módszer: Ezen technika alkalmazása során a támadó besurran egy épületbe. Ehhez használhat hamis beléptetőkártyát, megtévesztheti a beléptetésért felelős személyeket vagy besurranhat egy belépésre jogosult személy mögött az automata ajtózáródásig. Értékes információkhoz juthat az irodákba való bejutás során, ahol számítógépekhez és nyomtatott dokumentumokhoz is hozzáférhet. [7]

Jelszavak kitalálása: Itt kifejezetten a nem megfelelő erősségű jelszavak kitalálásáról van szó, ahol a támadó egyszerűen próbálkozik különböző jelszavak használatával.

Gyakran a felhasználók megadják egymásnak a jelszavaikat, illetve mások által hozzáférhető helyen tárolják.

ÖSSZEGZÉS

Ezeknek az adathalászati technikáknak az eredménye általában olyan információ, melyet a későbbiekben fel lehet használni más jellegű, technikai támadások kivitelezéséhez. Ezek az egyszerűnek tűnő technikák nem kívánnak IT alapú tudást, csupán rátermettséget és bátorságot. A későbbiek folyamán azonban az ilyen jellegű támadások tekintélyes anyagi károkat tudnak okozni mindenféle a felhasználónak és szervezetnek. Ezért nagyon fontos a tudatos felhasználás és az odafigyelés a leghétköznapibbnak tűnő szituációkban is.

Az összes eddig bemutatásra került adathalászati technika szerves része volt az emberi manipuláció alkalmazása, ennek okán technikai intézkedésekkel szinte lehetetlen ezeket kivédeni. A leghatékonyabb védelem ezekkel a támadásokkal szemben tudatos felhasználás kialakítása és a hatékony adatvédelmi tudatosság felépítése lehet.

IT ALAPÚ TUDÁST IS IGÉNYLŐ ADATHALÁSZATI TECHNIKÁK

Ezek közé tartoznak a valamilyen IT eszköz segítségével végrehajtott támadások, ahol rendszerint az elkövető nem is lép közvetlenül kapcsolatba az áldozatával és ebből fakadóan kisebb a lebukás veszélye. A támadók felkészültek és járatosak a szoftverek és az IT eszközök használatában. Ezeknek a támadásoknak a kivédése már bizonyos fokú felhasználói tudást igényel, hiszen itt már az online lét világában történnek a különböző incidensek.

Phishing – Adathalászat: Ezt az elnevezést gyűjtőfogalomként használjuk. A személyes adatok visszaélés céljából történő gyűjtésének egyik leggyakoribb módja.

Az ilyen támadásokat tapasztalt bűnözők vezetik, gyakran egész bűnözői csoportokkal vagy akár egész államokkal szövetkezve. A legegyszerűbb támadási módszer az e-mail, melynek során a támadók különféle ürügyeket alkalmaznak a szenzitív adatok megszerzése érdekében. Például: Egy értesítés a banktól, hogy a Tisztelt Ügyfél számlája hamarosan lejár, és elkéri a bank a személyazonosításra alkalmas adatokat (hitelkártyaszám vagy online banki hozzáférési kód) a szerződés meghosszabbításához. Ezek az adathalász jellegű e-mailek gyakran olyan emberektől származnak, akiket a kiszemelt célpont ismer és akikben megbízik, és/vagy a munkahelyi felettesük e-mail-céméről érkeznek. Az ilyen jellegű leveleket egyszerre több e-mail címre is elküldik, abban a reményben, hogy csak lesz majd valaki, aki gondolkodás nélkül válaszol ezekre a sürgető jellegű kérésekre és felfedi személyes adatait, úgymint például a hitelkártya adatokat, a személyi igazolvány adatait, lakcímet vagy egyéb személyazonosításra alkalmas adatát. Az adathalászat célja érzékeny személyes adatok megszerzése, bejelentkezési adatok beszerzése az áldozat információs rendszeréhez, valamint rosszindulatú alkalmazások telepítése a személyi számítógépre, laptopra, tabletre vagy mobiltelefonra. Ha ez sikeresen megtörténik, akkor ezek után már szinte bármit meg tud tenni a támadó a felhasználó eszközein és különböző platformjain akár az áldozat tudta nélkül is. Például törölheti vagy titkosíthatja az áldozata fájljait, hozzáférhet banki tevékenységéhez, vírusokat terjeszthet a nevében vagy minden adatát zárolhatja. Tipikus jellemzője az ilyen email-eknek, hogy helyesírási és ragozási hibákkal vannak tele,

sürgető jellegű adatok vagy linkre való kattintásra szólít fel és általános, nem személyre szóló a megszólítása.

Whaling – bálnavadászat: Kifejezetten egy konkrét célszemély elleni támadás, mely leggyakrabban a cégvezetők („bálnák") ellen irányul. A célzott támadások az internetről származó fenyegetések, amelyek során a támadók az elektronikus információs rendszerek infrastruktúrájának egyes részeit veszik célba, hogy azon a részen felügyelet nélkül "garázdálkodhassanak". Ennek a viselkedésnek az a célja, hogy a támadó hozzáférjen a céleszköz feletti rendelkezés jogával. Ez a támadások egyik rendkívül kifinomult módszereket és magas szintű szakértelmet igénylő formája, amely ellen kifejezetten nehéz védekezni, ezért gyakran sikeres eredménnyel zárul. A whaling avagy úgymond bálnavadászat során az adathalász megkeresi a vállalat legfontosabb vezetőjének vagy valamely kiemelten fontos cégvezetőnek a nevét és e-mail címét (amely a legtöbb esetben egy-két kattintással könnyedén megtalálható az adott vállalat honlapján), és személyre szabott e-mailt küld a kiszemelt áldozat vezetői szerepéhez szorosan kapcsolódó tárgyban. Az e-mail tartalmaz egy linket, amelyre, ha a kiszemelt cégvezető rákattint, akkor kártékony programok töltődnek le az illető eszközére és a hackertámadás sikeressé válik. [9]

Spear phishing – szigonyozás: Van, ahol lándzsás adathalászatként hivatkoznak erre a módszerre. Ennél a taktikánál pont az ellenkezője történik, mint az a phising technikánál ismeretes, vagyis kevés címzetthez érkezik meg az adathalász jellegű email, ami jól megfogalmazott, szépen strukturált levél, amely úgy tűnik, hogy egy banktól, vagy jól ismert vállalattól érkezik és megbízható forrásból származik. Válaszban kérheti a gyanútlan felhasználótól a jelszavát, hozzáférési adatait, személyes adatait. Előfordulhat emellett az is, hogy linket tartalmaz, amely egy kártékony álweboldalra irányítja a célszemélyt, vagy egy káros mellékletet tartalmaz.

Baiting: Az adathalász egy hordozható adathordozót (például pendrive vagy külső winchester) ott „felejt" egy jól látható helyen, többnyire egy számítógép közelében és az emberi természet kíváncsiságát használja ki. Gyakran jól olvashatón ráírnak valamilyen extra figyelemfelkeltő szöveget is, hogy még nagyobb legyen a csábítás, úgymint például titkos, szexi, bizalmas satöbbi. Amikor a kíváncsi megtaláló csatlakoztatja a talált tárgyat a számítógéphez, akkor történik meg a fertőzés. Ez a módszer online módon is működik például egy ingyen letölthető játék vagy valamilyen egyéb szoftver alkalmazása során. Ezért is fontos hangsúlyozni, hogy csak biztonságos oldalakról szabad letölteni programokat.

Typosquatting más néven URL-eltérítés: Az eredeti weblappal első ránézésre teljesen megegyező, alternatív weboldalra irányítja a felhasználót. Az alternatív oldal grafikai dizájnja, nagyon hasonlít az eredeti weboldaléra és első ránézésre nem is lehet megkülönböztetni. Az álweboldal webcíme többnyire egyetlen karakterrel különbözik az eredetileg felkeresni kívánt weboldal címétől és a legtöbb esetben a felhasználó észre sem veszi, hogy nem megfelelő helyen jár. Gyanútlanul megadja a hitelesítő adatait, amit a támadó ezután könnyedén felhasználhat.

Kiváló magyar példa erre: legjobbank.hu vagy Iegjobbank.hu A különbség nehezen észrevehető. Az első karakter az egyiknél a kis „L" betű a másiknál a nagy „i".

A farmolás vagy angolul pharming: (átirányítás hamisított weblapra) A támadó a felhasználót egy hamis, de a megbízhatóhoz nagyon hasonlító weboldalra irányítja. Az át-

irányítás általában valamilyen szoftver segítségével történik, többnyire nem is látszik különbség az eredeti és az álweboldal URL címében. A hacker az általa létrehozott hamis weboldal segítségével szerzi meg a felhasználótól a bizalmas információkat.

SMiShing – adathalászat SMS segítségével: Az adathalász hacker egy rövid szöveges üzenetet küld az áldozatának (SMS: Short Message Service) aminek segítségével megpróbálja rábírni az áldozatát arra, hogy az valamilyen személyes adatát vagy a támadó szempontjából fontos információt osszon meg vele, esetleg az sms egy linket tartalmaz, amire, ha rákattint a felhasználó egy ártalmas weboldalra lesz irányítva. Ennek folyományaként kártékony program kerülhet telepítésre, vagy a támadó megszerezheti a felhasználó személyes akár banki adatait is. [10]

TOVÁBBI SOCIAL ENGINEERING ADATHALÁSZ FORMÁK ÉS ELNEVEZÉSÜK

Search engine phishing: Egy rendkívül nagy kedvezményt nyújtó vásárlási lehetőséget kínáló weboldal, mely azonnali vásárlásra buzdít és azonnali klikkelésre szólítja fel a gyanútlan felhasználót. Ezek között szerepelhet egy szerencsekerék megforgatása klikkeléssel, melynek segítségével 90%-os vásárlás kedvezményt nyer az illető, ha néhány percen belül felhasználja a nyeremény kupont. És amint klikkel a felhasználó, máris a támadó által létrehozott weboldalon landol.

Social data mining: A különböző social media felületeken, mint például a Facebook, Twitter, TikTok, Instagram, YouTube sok felhasználó posztol magáról és magával kapcsolatosan mindenféle privát információt, amit egy későbbi támadás során fel tud használni egy támadó. Gyakran a pontos helymeghatározást is nyilvános adattá teszik magukról és ezáltal könnyedén nyomon követhető válik, hogy mely helyeken fordul meg gyakrabban, mikor merre járt külföldön, vagy milyen ételeket, italokat fogyaszt szívesen az illető. Ezek az adatok nyilvánosan elérhetők és ez a tevékenység önmagában nem illegális, hiszen a felhasználók saját akaratuk szerint osztanak meg magukról információkat, viszont nagyon hasznos információkkal szolgálhat egy későbbi kibertámadáshoz.

Böngésző előzményeken alapuló adatgyűjtés és automatikus kitöltés funkció kihasználása: Ha az eszközünkhöz, melyet napi tevékenységeink során használunk, hozzáférhet más személy, akkor könnyedén rá tud keresni, mely oldalakon jártunk korábban. Akár hónapokra visszamenően is. Ezekből az előzményekből szintén megismerhetőek vagyunk, szokásaink, ízlésünk, gyakran látogatott weboldalaink alapján feltérképezhetővé válik, milyen módon lehet a legkönnyebb módon a közelünkbe férkőzni. Az inkognitó mód használatával (Chrome felületen: control + shift + n billentyűkombináció), el tudjuk kerülni, hogy az általunk látogatott oldalak megjelenjenek a böngészési előzményekben. [11]

ÖSSZEFOGLALÁS

A tanulmányban bemutatásra kerültek a social engineering különböző technikái és definiálásra kerültek a témához kapcsolódó alapfogalmak. A kiberbiztonság a 21. század egyik legkritikusabb jelensége, mely magánszemélyeket, kis és középvállalatokat, nagy cégeket, országokat és nemzeteket egyaránt érint. A tudatos digitális jelenlét és eszközhasználat kiemelkedően nagy hangsúlyt kap, elmulasztása egyaránt okozhat lényeges anyagi, mentális és presztízs veszteséget. Az online térben elkövetett illegális tevékenységek

ugyanúgy bűnözének minősülnek, mintha a boltban lopna vagy adót sikkasztana valaki. Sajnos a kiberbűnözést még mindig nem kezeljük megfelelő hozzáállással a társadalmunkban. A tetten érés nagyon nehéz a legtöbb esetben, ebből kifolyólag a kellő szankcionálás is. A legtöbb hétköznapi ember nem fordít elegendő odafigyelést az adatainak a védelmének érdekében. Ahogy az a tanulmányban bemutatásra került gyakran előfordul, hogy a legalapvetőbb biztonsági intézkedéseket sem tesszük meg, mint a kártyás fizetés során a pin kód eltakarása, vagy a bizalmas jellegű információk megbeszélése telefonálás során a megfelelő közegben, mások által nem hallható helyen. A legtöbben nincsenek a tudatában, hogy menynyire fontos a naprakész védelem minden eszközön és minden felületen. A legtöbb kibertámadás emberi mulasztás vagy gondatlanság miatt sikeres. Hiába találnak ki a szoftverfejlesztők nagyszerű programokat és alkalmazásokat, különböző tűzfalakat, vírusírtókat az adatok védelme érdekében, ha az átlagos emberek nincsenek tudatában az alapvető megelőzési technikákkal. A tudatos életvezetés minden aspektusban kiemelkedően fontos, így az online térben is. A programok rendszeres frissítése, a megfelelő erősségű jelszavak használata és gyakori cseréje, a nyílt és közös hálózatok használatának mellőzése, megfelelő vírusirtók és tűzfalak használata, kémprogram eltávolító alkalmazások, illetve a két lépcsős azonosítás használatával már sokat tehetünk önmagunk és adataink védelme érdekében. A figyelem felkeltése, a gyakori és ismétlődő tudatosítás kiemelkedően fontos szerepet kap a kiberbiztonság területén.

FELHASZNÁLT FORRÁSOK

[1] „Mitnick Security,” [Online]. Available: (https://www-mitnicksecurity-com.translate.goog/about-kevin-mitnick-mitnick-security?_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc. [Hozzáférés dátuma: 02. 05. 2024.].

[2] „444.hu,” 2023. [Online]. Available: https://444.hu/2023/07/21/meghalt-kevin-mitnick-a-korai-internet-legendas-hackere. [Hozzáférés dátuma: 02. 05. 2024.].

[3] K. D. Mitnick és S. L. William, A legendás hacker A megtévesztés művészete, Budapest: Perfact, 2003.

[4] K. D. Mitnick és S. L. William, A legendás hacker a behatolás művészete, Budapest: Perfact, 2006.

[5] „HVG.hu,” 2023. [Online]. Available: https://hvg.hu/tudomany/20230720_Kevin_Mitnick_meghalt_hekker_amerika. [Hozzáférés dátuma: 02. 05. 2024.].

[6] K. D. Mitnick és S. L. William, A legkeresettebb hacker, Budapest: HVG, 2012.

[7] G. Kaczur, Spear phishing, Budapest: NKE, 2018.

[8] I. Psenakova, „Ne hagyd magad becsapni!,” Lélektan és hadviselés - Interdiszciplináris folyóirat, II. évf., pp. 55-65, 2020/1.

[9] A. P. Bodó és N. Zámbó, A közreműködők kötelezettségei a célzott támadások elhárításában az IBTV. szerint, in: Célzott kibertámadások: NKE, 2018.

[10] C. Kollár és Á. Zakar , „A social engineering és a manipulációs technikák és módszerek,” Biztonságtudományi Szemle II. évf. 2. sz., pp. 23-38, 2020.

[11] L. Kovács és E. Terták , „A kiberbűnözés legjobb ellenszere a pénzügyi műveltség 11. évf. 1. sz.,” Gazdaság és Pénzügy, pp. 6-29, 2024.

DOI: https://doi.org/10.12700/btsz.2025.7.2.57

CRITICAL INFRASTRUCTURE FACILITY PROTECTION CHALLENGES IN THE CONTEXT OF SOCIAL ENGINEERING ATTACKS

KRITIKUS INFRASTRUKTÚRÁK OBJEKTUMVÉDELMÉNEK KIHÍVÁSAI A SOCIAL ENGINEERING TÁMADÁSOK KONTEXTUSÁBAN

MÁRTON Zoltán [1] – RAJNAI Zoltán[2] – BEREK Lajos[3]

Abstract

Critical infrastructure facilities face growing threats from social engineering attacks that exploit human behavior. This article explores how psychological manipulation endangers physical security in sectors such as energy, transport, and healthcare. A STEAM-based, interdisciplinary approach is proposed, combining scientific, technological, engineering, artistic, and mathematical elements to enhance resilience. The study highlights gamified and adaptive training methods as effective tools for strengthening security culture. Recent cases and literature (post-2020) demonstrate how phishing, impersonation, and the AI-powered „deepfakes" can be countered by integrating technology with improved human preparedness.

Keywords

social engineering; critical infrastructure; facility protection; STEAM; gamification

Absztrakt

A kritikus infrastruktúrák egyre nagyobb veszélynek vannak kitéve a social engineering támadások révén, amelyek az emberi viselkedést használják ki. A cikk bemutatja, miként veszélyezteti a pszichológiai manipuláció a fizikai biztonságot az energetikai, közlekedési és egészségügyi szektorban. STEAM-alapú, interdiszciplináris megközelítést javasolunk, amely ötvözi a tudományos, technológiai, mérnöki, művészeti és matematikai elemeket a reziliencia növelése érdekében. A kutatás kiemeli a játékosított és adaptív képzések szerepét a biztonsági kultúra erősítésében. Friss esetek és szakirodalmak igazolják, hogy a phishing, megszemélyesítés és az MI-alapú „deepfake" technikák hatékonyan kivédhetők a technológiai és humán védelem együttes alkalmazásával.

Kulcsszavak

social engineering; kritikus infrastruktúra; objektumvédelem; STEAM; játékosítás

[1] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X| PhD Student, Doctoral School on Safety and Security Sciences Óbuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

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

[3] berek.lajos@bgk.uni-obuda.hu| ORCID: 0000-0003-1705-1173| professor emiritus, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | professzor emiritus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A kritikus infrastruktúrák – ahogyan az energiatermelő létesítmények, közlekedési hálózatok irányító központjai vagy kórházak – védelme kiemelt fontosságú nemzetbiztonsági és társadalmi érdek. E létesítmények objektumvédelme hagyományosan a fizikai biztonsági rendszerekre (kerítések, beléptető rendszerek, videó megfigyelő rendszerek) és az informatikai védelemre egyaránt támaszkodik. Az utóbbi években azonban egyre nyilvánvalóbbá vált, hogy a legmodernebb technológiai védelem is sebezhető, amennyiben a támadók az emberi tényezőt veszik célba [1], [2]. A social engineering, vagyis a pszichológiai manipuláció eszköztárával a támadó nem a zárt ajtókat próbálja feltörni vagy a tűzfalakat megkerülni, hanem megkeresi a „gyenge láncszemet" jelentő alkalmazottat vagy biztonsági őrt, és manipulációval ráveszi a védelmi protokoll megsértésére. E módszer lényege, hogy **az emberi hibát és viselkedést kihasználva próbál hozzáférést szerezni védett információkhoz, rendszerekhez vagy létesítményekhez**, sokszor a megtévesztés kifinomult formáit alkalmazva [1].

A digitalizáció és a hálózatba kapcsoltság növekedésével a social engineering támadások száma és kifinomultsága is emelkedik világszerte [3]. A támadók gyakran összehangoltan alkalmazzák a kibertérben és a fizikai térben végrehajtott behatolási technikákat: egy jól megszerkesztett adathalász (phishing) e-maillel jutnak be egy erőmű vezérlőrendszerének hálózatába, vagy egy hamis karbantartónak adva ki magukat személyesen próbálnak belépni egy védett objektumba.

A kritikus infrastruktúrák ellen irányuló kibertámadások jelentős része indul valamilyen **social engineering módszerrel**, különösen adathalászattal vagy illetéktelen hozzáférési adatok megszerzésével [3]. Az Egyesült Államok kiberbiztonsági hatóságainak 2023-as kockázatértékelési jelentése (Risk and Vulnerability Assessment Analysis – RVAA) szerint a sikeres behatolások 40%-ában kompromittált, de legitim felhasználói fiókokat használtak ki (akár ellopott hitelesítési adatok révén), míg a második leggyakoribb módszer célzott adathalász link alkalmazása volt, az incidensek több mint 25%-ában [11]. A Cybersecurity Dive szakmai beszámolója szerint e jelentés megállapításai rámutatnak arra, hogy a humán kockázatok megfelelő kezelése nélkülözhetetlen a létfontosságú rendszerelemek védelmében [3].

A social engineering támadások nemcsak a kibertérben, hanem a fizikai világban is megjelennek. A hagyományos objektumvédelmi intézkedések – beleértve az épületőrzést, a beléptetést és a járőrszolgálatot – nem nyújtanak megfelelő védelmet, ha egy támadó pszichológiai manipulációval ráveszi a személyzetet a biztonsági eljárások kijátszására. Ilyen lehet, amikor egy támadó **idegenként bejut egy védett létesítménybe úgy, hogy** az ajtónál várakozva egyszerűen bemondja, hogy *„Hoztam a megrendelt eszközöket a szerverkarbantartáshoz"* – és a jóhiszemű biztonsági őr beengedi.

Számos beszámoló és esettanulmány igazolja, hogy még a szigorúan védett objektumokba is be lehet jutni megtévesztéssel. **Kowalski (2022) tanulmánya** kimutatta, hogy a tailgating – azaz egy jogosult személy nyomában történő illetéktelen belépés – a magas biztonságú környezetekben is komoly fenyegetést jelent [10]. E megállapítást gyakorlati tesztek is alátámasztják, többek között **az amerikai kormányzati RVAA jelentés** 2023-as kiadása, amely szerint számos fizikai behatolási kísérlet sikeres volt a humán tényező kihasználásával [11]. A támadók gyakran viselnek hivatalosnak tűnő egyenruhát vagy kitűzőt,

magabiztosan viselkednek, és kihasználják az emberi udvariasságot vagy az esetleges rutinokat a beléptetésnél. Az ilyen támadások sikeressége rávilágít arra, hogy a fizikai biztonság és a humán tényező szorosan összefügg: a **technikai biztonsági berendezések** (pl. beléptető kapuk, biometrikus azonosítók) csak addig hatékonyak, amíg az ember nem kapcsolja ki őket vagy nem hoz rossz döntést.

Mindezek fényében egyre hangsúlyosabbá vált az igény egy **holisztikus, interdiszciplináris megközelítésre** a kritikus infrastruktúrák védelmében. A STEAM[4] alapú szemlélet – amely a természettudományosés a műszaki tudást, a művészetek és a kreatív pedagógiai módszerekkel ötvözi – új perspektívát kínál a biztonságtudatosság növelésében. Jelen cikk célja, hogy a korábbiaktól eltérő koncepcionális keretben tárgyalja a kritikus infrastruktúrák objektumvédelmének és a social engineering fenyegetéseknek a metszéspontját. A fókusz az emberi tényező megerősítésén van: bemutatjuk, miként integrálható a STEAM szemlélet a biztonsági képzésbe, és hogyan tehetők ellenállóbbá a szervezetek a manipulációval szemben játékosított, adaptív képzési megoldások révén. A következőkben áttekintjük a legújabb social engineering módszereket és trendeket a kritikus szektorokban, majd ismertetjük az ezekkel szembeni lehetséges védekezési stratégiákat, különös tekintettel a humán kockázatok csökkentésére.

SOCIAL ENGINEERING FENYEGETÉSEK A KRITIKUS INFRASTRUKTÚRÁK ELLEN

A kritikus infrastruktúrák elleni social engineering támadások rendkívül sokfélék lehetnek, az egyszerű megtévesztéstől a komplex, több lépcsős, kifinomult módszerekig. Közös bennük, hogy a támadó a védelmi rendszerek **az emberi tényezőt, elsősorban az üzemeltetőket és felhasználókat veszi célba** és rajtuk keresztül próbál meg kárt okozni vagy hozzáférést szerezni. Az alábbiakban áttekintjük, hogyan jelennek meg a social engineering jellegű fenyegetések négy fő dimenzióban: az energetikai, közlekedési és egészségügyi ágazatokban; az új technológiai eszközök – mesterséges intelligencia (továbbiakban: MI) alkalmazásában; valamint a korábban ismert, klasszikus megtévesztési módszerek viszszatérésében.

Energetikai létesítmények

Az energiatermelő és -elosztó rendszerek (erőművek, elektromos hálózatok vezérlő központjai) kiemelt célpontjai a nemzetállami és bűnözői csoportoknak. Gyakori módszer a „**spear phishing"**[5] alkalmazása, amikor az erőmű dolgozóit célzott, hitelesnek tűnő e-mailekkel veszik célba. Ezek az üzenetek sokszor sürgős műszaki problémára hivatkoznak vagy valamilyen utasítást tartalmaznak, amelyre a dolgozó automatikusan reagálni akar.

2021-ben az energiaszektor a kibertámadások egyik leggyakoribb célpontja volt az Egyesült Királyságban, az összes támadás 24%-át ez a szektor szenvedte el, és számos esetben a támadók adathalász e-mailekkel jutottak be a hálózatba [4]. A „**spear phishing"** le-

[4] az angol Science, Technology, Engineering, Arts, and Mathematics (tudomány, technológia, mérnöki tudományok, művészetek és matematika) szavak kezdőbetűiből álló mozaikszó, amely az oktatásban ezeket a területeket integráltan kezeli a kreatív és problémamegoldó gondolkodás fejlesztése érdekében.

[5] célzott adathalászati módszer, amely során a támadó személyre szabott, hitelesnek tűnő üzenetekkel próbálja rávenni az áldozatot bizalmas információk kiadására vagy rosszindulatú fájl megnyitására.

hetővé teheti, hogy a behatoló megszerezze egy mérnök belépési adatait, majd azokkal távolról bejelentkezve átvegye az irányítást egyes rendszerek felett, vagy káros szoftvert (pl. zsarolóprogramot) juttasson a hálózatba.

Emellett fizikai social engineering is veszélyt jelent: ismert eset, hogy egy támadó **külső karbantartónak kiadva magát** próbált bejutni egy vízerőmű gépházába, hamis megbízólevelekkel és egyenruhában. Amennyiben a személyzet nincs kellően felkészítve az ilyen helyzetek felismerésére, az objektumvédelmi protokoll könnyen kijátszható.

Közlekedési rendszerek

A légiközlekedés, vasúti hálózatok, városi tömegközlekedés irányító rendszerei egyre inkább automatizáltak és hálózatba kötöttek, ugyanakkor emberek üzemeltetik és felügyelik őket. A támadók kihasználhatják, hogy ezen szervezeteknél is sok múlik a diszpécserek, forgalomirányítók, karbantartók éberségén.

Előfordulhat, hogy egy vasúti társaság informatikusának **telefonos átverésével („vishing" [6])** szereznek meg hozzáférést a belső hálózathoz: a támadó a telefonban a cég egyik beszállítójának IT-támogató mérnökének adja ki magát, és azt állítja, sürgősen szüksége van egy adminisztrátori jelszóra egy "rendszerhiba" elhárításához. Ha a megtévesztett alkalmazott kiadja a jelszót, a támadó azonnal beléphet a rendszerbe és megnyithatja az utat további támadásokhoz. A közlekedési ágazatban a **fizikai social engineering** is fenyeget: repülőtereken vagy vasúti csomópontokban gyakran dolgoznak külsős vállalkozók, beszállítók. Egy támadó egy hamis szállítói azonosító kártyával megpróbálhat behajtani a repülőtér védett területére arra hivatkozva, hogy árut hozott.

2019-ben a londoni Heathrow repülőtéren történt biztonsági incidens során kiderült, hogy a protokollok figyelmen kívül hagyása (egy USB eszköz engedély nélküli használata) és a dolgozók megtévesztése jelentős szerepet játszott a védelmi rendszer kijátszásában . Bár ez az eset korábbi, jól szemlélteti, hogy a közlekedési infrastruktúrákban is számolni kell az emberi tényezőből fakadó résekkel [2].

Egészségügyi szektor

A kórházak és egészségügyi létesítmények kritikus fontosságú adatokkal (betegek egészségügyi adatai) és berendezésekkel (életfenntartó rendszerek, gyógyszeradagolók) rendelkeznek, amelyek kiesése emberéleteket veszélyeztethet. Az egészségügy sajnos gyakran célpontja **zsarólóvírus (**azaz ransomware**)** támadásoknak is, melyek sokszor social engineeringgel kezdődnek. A támadó e-mailben küldhet egy fertőzött dokumentumot a kórházi pénzügynek, mely látszólag egy beszállítói számla – a dokumentum megnyitásával a kártevő települ és titkosítja a rendszereket. Ezen túl a „**vishing"** is megjelent ebben a szektorban: 2022 óta egy **Scattered Spider** néven ismert hackercsoport kifejezetten híressé vált arról, hogy **telefonon hívja fel az egészségügyi intézmények dolgozóit**, és az MI segítségével más személy (adott esetben egy vezető) hangján beszél, hogy érzékeny adatokat vagy hozzáférést szerezzen [5]. Az Amerikai Egészségügyi és Emberi Szolgáltatások Minisztériumának 2024-es figyelmeztetése szerint ez a csoport **MI-alapú hangklónozást** vetett be, hogy a célpont szervezeteknél az elsődleges hozzáférést megszerezze [5].

[6] (voice phishing) olyan megtévesztési technika, amely során a támadó telefonhíváson keresztül próbál bizalmas információkat kicsalni az áldozattól, például úgy, hogy hivatalos személynek (pl. rendszergazda, vezető) adja ki magát.

Egy ilyen támadás során a kórház informatikusa kaphat egy hívást a főigazgató "hangján", aki utasítja, hogy sürgősen adjon távoli hozzáférést egy külső szakértőnek – ha az informatikus nem elég óvatos, könnyen engedélyezhet egy támadónak hozzáférést a hálózathoz, nem is sejtve, hogy átverték.

Az egészségügyben a **fizikai social engineering** is jelen van: színlelt betegek, csalók próbálhatnak meg bejutni korlátozott területekre (gyógyszerraktár, szerverközpont) egy kórházban. Amennyiben a biztonsági protokollokat nem tartják be – ha egy támadó másolt belépőkártyával vagy csupán fehér köpenyt viselve követi az orvosokat egy védett területre –, az objektumvédelem működése meghiúsulhat.

Új technológiák a social engineering szolgálatában

A fenti szektorok mindegyikében megfigyelhető, hogy a támadók egyre gyakrabban alkalmaznak **új technológiákat** a megtévesztés hatékonyságának növelésére. Az MI térhódítása új dimenziót ad a social engineeringnek.

A generatív MI modellek, mint amilyen a ChatGPT, képesek olyan meggyőző adathalász üzeneteket írni, amelyek nyelvtanilag és stilisztikailag is kifogástalanok [1]. Míg korábban a gyanús e-maileken gyakran lehetett érezni, hogy nem anyanyelvi író tollából származnak (helyesírási hibák, furcsa megfogalmazások jelezték), addig ma már egy MI által generált szöveg professzionálisnak tűnhet.

Ez megnehezíti a felhasználók számára a támadói e-mailek felismerését. Továbbá a „**deepfake"** technológia – legyen szó **hamis hangokról vagy videókról** – kezd gyakorlati eszközzé válni a kiberbűnözésben. Ahogy arra hazai szakértők is rámutattak, a közösségi médiában hozzáférhető hang- és videóanyagok alapján bárkiről készíthető olyan hamis felvétel, amely első hallásra/látásra megtévesztő lehet [1].

Bár jelenleg a valós idejű, teljesen hihető „deepfake" videók előállítása még technológiai kihívás, a fejlődés gyors, és a jövőben az MI által támogatott social engineering támadások további emelkedésére számíthatunk [1]. A gyakorlatban ez azt jelentheti, hogy egy kritikus infrastruktúra üzemeltetője, egy videóhívás során azt hiheti, a jól ismert beszállítójával egyeztet, miközben valójában egy támadó generált avatárja kéri tőle a hozzáférési kódokat [8].

Hagyományos manipulációs technikák a fizikai térben

A pandémia alatt előtérbe került online támadások mellett újra felbukkannak a fizikai világban megvalósuló social engineering módszerek. A Nemzeti Kibervédelmi Intézet 2024-es jelentése szerint ismét gyakoribbá váltak az **"elhagyott" fertőzött USB pendrive-okkal végrehajtott támadások**, ahol a támadó a céges parkolóban elejt egy pendrive-ot abban bízva, hogy egy alkalmazott megtalálja és a kíváncsiságtól vezérelve a munkahelyi gépére csatlakoztatja azt [1]. Szintén említik a hamis QR-kódok terjesztését: plakátokra vagy épületen belül elhelyezve olyan QR matricákat ragasztanak ki, amelyek egy belső szabályzatra vagy ebédlői menüre hivatkoznak, de valójában egy adathalász weboldalra vezetnek [1]. Ezek a módszerek mind arra alapoznak, hogy a legfejlettebb technológiai védelmi rendszereket is meg lehet kerülni, ha az emberi kíváncsiságot, segítőkészséget vagy figyelmetlenséget kihasználják.

Összességében látható, hogy a social engineering támadások a kritikus infrastruktúrák mindhárom vizsgált területén komoly fenyegetést jelentenek. A támadási módszerek

folyamatosan bővülnek: a **klasszikus pszichológiai trükkök** (sürgetés, tekintélyre hivatkozás, bizalmi viszony kialakítása) mellé felsorakoztak a **korszerű technológiai eszközök** (MI, „deepfake") a megtévesztés hatékonyságának növelésére.

Mindez indokolja, hogy a kritikus infrastruktúrák védelmét ne csak technikai és procedurális oldalról közelítsük meg, hanem a humán tényezőre és annak fejlesztésére kiemelt figyelmet fordítsunk. A következő fejezetben azt tekintjük át, milyen stratégiák segíthetnek a social engineering jellegű fenyegetések mérséklésében, és hogyan integrálható egy interdiszciplináris (STEAM) szemlélet ezekbe a stratégiákba.

VÉDEKEZÉSI STRATÉGIÁK: TECHNOLÓGIA, EMBERI TÉNYEZŐ ÉS STEAM-ALAPÚ SZEMLÉLET

A kritikus infrastruktúrák védelmében a **hagyományos biztonsági megközelítések** a következő pillérekre támaszkodnak: (1) **technológiai védelmi megoldások** – ilyenek a tűzfalak, a behatolásészlelő rendszerek, a fizikai beléptető kapuk, a behatolásvédelmi rendszerk is.; (2) **szervezeti protokollok és eljárások** – biztonsági szabályzatok, hozzáférési jogosultságok szigorú kezelése, kétfaktoros hitelesítés előírása, látogatói kísérés és azonosítás; (3) **humán tényező** – a személyzet képzettsége, ébersége és biztonságtudatossága. Egy valóban hatékony védelmi rendszer e három elem összehangolt működésére épül.

Az utóbbi évek támadási trendjei azonban rámutattak, hogy a **humán faktor megerősítése** terén vannak a legnagyobb hiányosságok [3]. Hiába kiváló a technológiai pajzs, ha a kezelő „lyukat üt rajta" – tételezzük fel, hogy leírja a jelszavát egy cetlire, vagy gondolkodás nélkül rákattint egy ismeretlen linkre.

A védekezési stratégiák kulcsa **a technikai, szervezeti és humán biztonsági intézkedések összehangolt alkalmazása**. Ennek részeként kiemelt jelentősége van azoknak a technológiai megoldásoknak, amelyek képesek minimalizálni az emberi hibalehetőséget.

Erős azonosítás és jogosultságkezelés

Minden kritikus rendszerhez többlépcsős (két- vagy többfaktoros) hitelesítés szükséges, így ha egy alkalmazott véletlenül kiadná is a jelszavát egy támadónak, önmagában azzal ne lehessen bejutni. A jogosultságokat ráadásul a minimálisan szükséges szintre kell korlátozni (legkisebb jogosultság elve) [12] hogy egy esetleg kompromittált fiókkal se lehessen bármit elérni.

Rendellenesség alapú behatolás érzékelő rendszerek [13]

A hálózatban szokatlan viselkedést detektáló szoftverek (akár egy alkalmazott belép éjjel egy rendszerbe, amit amúgy sosem használ – ez lehet egy támadó) figyelmeztetést adhatnak, még mielőtt nagyobb baj történne. Emellett a fizikai biztonságban is vannak hasonló eszközök, hiszen az okoskamerák, amelyek MI-vel felismerhetik, ha valaki egy ajtó mögött átsurran a jogosult személy mellett.

Beépített biztonság („Secure by Design") elvek

Olyan rendszerek és folyamatok tervezése, amelyek alapból számolnak az emberi tényező gyengeségével. A vezérlőtermek ilyeneek, ahol a belépést úgy lehet kialakítani, hogy mindig két személy együttes jelenléte kelljen (négy szem elve) [14], így egy embert sokkal nehezebb manipulálni, ha a másik is ott van és figyel.

Ezek az intézkedések fontosak, de önmagukban nem elegendőek. A social engineering ellen a **szervezeti kultúra** fejlesztése és az emberek folyamatos képzése a leghatékonyabb fegyver [4], [9]. Itt lép be az **interdiszciplináris szemlélet** fontossága. A humán viselkedés megértése és befolyásolása ugyanis nem pusztán informatikai vagy biztonságtechnikai kérdés, hanem **pszichológiai, sőt pedagógiai feladat** is. A STEAM megközelítés integrálása lehetővé teszi, hogy a biztonsági képzési programokat és eljárásrendeket célszerű komplexebb, rugalmasabb formában kialakítani:

Tudományos (Science) alapok

A döntéshozatal és az emberi tényező kutatása – így a kognitív torzítások, a megtévesztés pszichológiája – tudományos megalapozást ad ahhoz, hogy felismerjük, miért dőlnek be az emberek a trükköknek. A biztonsági képzésekbe szükségszerű beépíteni ezen ismereteket, hogy a dolgozók megértsék a saját sebezhetőségüket (többek között, hogy miért hajlamosak engedelmeskedni egy látszólagos felettes utasításának, vagy miért kattintanak rá impulzívan egy sürgősnek tűnő e-mailre).

Technológiai és Mérnöki (Technology, Engineering) megoldások

A védelmi rendszerek tervezésekor a mérnöki gondolkodás és a technológiai innováció segíthet minimalizálni a social engineering kockázatát. A hozzáférési rendszerek terén a **"zero trust"** elv alkalmazása – azaz soha senkiben nem bízunk meg implicit módon, még a belső hálózatban sem – technológiai kontrollokat eredményez (állandó hitelesítés, hálózati szegmentáció), amelyek csökkentik egy sikeres social engineering támadás mozgásterét.

Ugyanakkor a mérnöki szemlélet abban is segít, hogy a humán védelmi elemeket (folyamatok, képzések) éppoly gondos tervezéssel kezeljük, mint a szoftvereket vagy gépeket.

Művészetek (Arts) és kreatív módszerek

A képzések és tudatosságnövelő programok hatékonyságát nagymértékben növelhetik a kreatív, élményalapú elemek. Ide tartozik a **gamifikáció** (játékosítás) – a következő fejezet e kérdéskört részletesen tárgyalja –, valamint a szemléltető gyakorlatok, szimulációk, történetmesélés. A művészetek bevonása alatt érthetjük a **színészek bevonását szituációs gyakorlatokba** (eljátszanak egy támadót és egy megtévesztett alkalmazottat, amit a dolgozók együtt elemeznek ki), vagy akár egy képzőművészeti kampányt a szervezeten belül (plakátverseny a legötletesebb „Ne engedd be az idegent!" üzenetre). Az ilyen kreatív megközelítés segít abban, hogy a biztonságtudatosság mélyebb élménnyé váljon, ne csak egy kötelező oktatás legyen.

Matematika és adatelemzés (Mathematics)

A modern szervezetek rengeteg adatot tudnak gyűjteni a biztonsági eseményekről és a dolgozók viselkedéséről – kiemelve egyet: hányan kattintottak egy próba-phishing e-mailre. Ezen adatok elemzése kvantitatív alapot ad a képzés fejlesztéséhez. A statisztikai kiértékelés megmutathatja, mely területeken vannak „**vakfoltok"** a szervezetben – ha a pénzügyi osztály sokkal gyakrabban esik áldozatul adathalász teszteknek, akkor ott célzottabb oktatás kell. A matematika tehát a **mérhetőség** és a folyamatos visszacsatolás miatt fontos: rendszeres riportokkal, metrikákkal lehet követni a biztonságtudatosság fejlődését vagy épp romlását, és ennek alapján finomhangolni a programokat.

Látható, hogy a STEAM megközelítés nem valami különálló, idegen elem a biztonságtudományban, hanem sokkal inkább egy **keretrendszer**, amely emlékeztet bennünket arra, hogy a komplex problémák – mint a kritikus infrastruktúrák védelme a social engineering ellen – komplex megoldásokat igényelnek. A mérnöki-technikai megoldások és az emberi viselkedésformálás nem egymást kizáró, hanem egymást kiegészítő tényezők. Egy atomerőmű védelmi vezetőjének éppúgy értenie kell a fizikai védelem technológiájához, mint ahhoz, hogyan lehet megtanítani az ott dolgozóknak, hogy soha ne engedjenek be kíséret nélkül senkit a vezérlőterembe. E szemlélet jegyében a következő alfejezetben részletesen foglalkozunk a **humán tényező fejlesztésének** egyik legígéretesebb modern eszközével: a játékosított, adaptív képzési programok révén, amelyek jelentősen növelhetik a dolgozók biztonságtudatosságát és rezilienciáját.

JÁTÉKOSÍTOTT ÉS ADAPTÍV KÉPZÉSMEGOLDÁSOK A HUMÁN ELLENÁLLÓKÉPESSÉG NÖVELÉSÉRE

A humán kockázatok csökkentésének leghatásosabb módja, ha a szervezet minden tagja – a biztonsági őrtől az informatikuson át a felső vezetésig – **tudatában van a social engineering veszélyeinek**, ismeri a támadók módszereit, és begyakorolta a helyes reakciókat. A hagyományos oktatások (évente egyszer egy biztonságtudatossági oktatás, hosszú előadásokkal vagy szöveges tananyagokkal) sajnos sokszor kevéssé hatékonyak: unalmasak, nem ragadják meg a figyelmet, és így a tanultak rövid idő alatt elhalványulnak.

Ezzel szemben a **játékosított (gamifikált) oktatás** az utóbbi években ígéretes alternatívaként jelentek meg a biztonsági képzések terén [4], [6]. A gamifikáció lényege, hogy a tanulási folyamatba **játékmechanizmusokat** építünk be – melynek központi elemei az pontgyűjtés, a verseny, a jutalmak, és a történetvezérelt küldetések– ezáltal növeljük a résztvevők motivációját és elköteleződését.

Egy **játékosított kiberbiztonsági oktatás** során a dolgozók nem pusztán passzív befogadói az információnak, hanem aktív résztvevők, akik döntéseket hoznak, problémákat oldanak meg és azonnali visszajelzést kapnak a tetteik következményéről.

Kialakítható egy „Cybersecurity Challenge" játék a szervezeten belül: a résztvevők különböző szinteken mennek keresztül, ahol fiktív szcenáriókban kell felismerniük a támadási próbálkozásokat. Az egyik pályán az e-mailek között kell kiszűrni a phishing kísérletet, a másikon egy látogatót kell helyesen protokoll szerint kezelni (udvariasan, de határozottan azonosítani és kísérni). Minden jó döntésért pont jár, a hibákért pontlevonás. A végén ranglista készül, a legjobbak elismerést kapnak. Az ilyen barátságos versengés növeli a részvételi kedvet – hiszen a játékban való jó szereplés belső motivációt jelent – és közben észrevétlenül tanít [4].

Kutatások igazolják, hogy a gamifikált megközelítés javítja a tanulási eredményeket: egy 2024-ben publikált tanulmányban [15] az energiagazdálkodási szektor okoshálózati (smart grid) üzemeltetői számára fejlesztett játékos oktatóprogram 29–40%-kal növelte a résztvevők kvízpontszámait három nehézségi szinten, jelezve a tudatosság és ismeretek jelentős bővülését [4].

A gamifikáció mellett egyre nagyobb hangsúlyt kap az **adaptív (személyre szabott) tanulás** a biztonsági oktatásban. Ez azt jelenti, hogy a képzési rendszer figyeli a résztvevők teljesítményét és reakcióit, és ennek alapján alakítja a további tartalmat az egyén igényeihez.

Példa: A dolgozó sorozatosan hibázik a phishing e-mailek felismerésében, akkor számára több olyan gyakorló feladatot ad a rendszer, ami ezen a területen segíti a fejlődést. Ugyanakkor, aki már jártas benne, annak nem pazarolja az idejét ismétlődő alapfeladatokkal, hanem tovább lép egy haladóbb szintre.

Az adaptivitást gyakran **MI algoritmusok** támogatják, amelyek elemzik a felhasználók interakcióit. A modern digitális oktatási platformok lehetővé teszik azt is, hogy **részletes metrikákat** gyűjtsenek a tanulókról: mennyi idő alatt válaszolnak, hányszor tévesztenek, mely kérdést hányszor néznek vissza. Egy magyar fejlesztésű, játékosított kiberbiztonsági oktatási rendszer (Cyber Drill Studio) tapasztalatai szerint a résztvevők tanulási folyamatáról gyűjtött adatok elemzése révén pontosan beazonosíthatók a problémás területek, és ennek alapján a képzési tartalom módosítható az adott szervezet és az egyének igényeihez illeszkedően [7]. Ily módon az oktatás folyamatosan fejlődik a visszajelzések alapján, és az egyének is testre szabott támogatást kapnak, akárcsak egy magántanártól – csak épp digitális formában.

A játékosítás és az adaptivitás ötvözése különösen hatékony: a résztvevők élvezettel tanulnak és versengenek, miközben a rendszer **automatikusan igazodik** a tudásszintjükhöz és tanulási tempójukhoz. Ez a megközelítés áthidalja az unalmas kötelező oktatás és a valós kihívások közti szakadékot. A dolgozók „biztonsági szimulátorban" gyakorolhatnak, akár ismétlődően is, kockázatmentesen hibázhatnak és tanulhatnak a hibákból. Egy jól kidolgozott képzési program **élménnyé teszi a tanulást** – a résztvevők szinte észre sem veszik, hogy épp egy biztonsági protokollt sajátítanak el, mert leköti őket a játék vagy a történet. Ráadásul a játékban szerzett pozitív élmények révén a biztonsági előírások betartása nem kényszernek fog tűnni számukra, hanem belső igénnyé válhat, hiszen saját sikerük kapcsolódik hozzá.

Számos gyakorlati példa létezik már az ilyen képzésekre. Több nagy nemzetközi vállalat alkalmaz **„cybersecurity escape room"** gyakorlatokat, ahol a csapatoknak különféle biztonsági rejtvényeket kell megoldaniuk egy szimulált kiber-incidens során, hogy „kiszabaduljanak" – ez egyszerre épít csapatmunkára és tanít meg konkrét eljárásokat. Magyarországon is volt példa kreatív megoldásokra: egy bank belső biztonsági kampánya keretében interaktív videósorozat készült, melyben a dolgozók maguk választhatták meg, hogyan reagál a főhős egy social engineering helyzetben, és a történet a döntéseik szerint alakult tovább. Az ilyen **interaktív oktatóanyagok** bevonják a nézőt és személyes élménnyé teszik a tanulságokat.

Természetesen a játékosított képzések is megfelelően illeszkedniük kell a szervezet kultúrájába. Fontos, hogy ne hozzanak létre nem kívánt versengést vagy szégyenérzetet a gyengébben teljesítőkben – ezért célszerű a hangsúlyt az egyéni fejlődésre és csapaton belüli együttműködésre helyezni, nem feltétlenül a nyilvános rangsorolásra. Továbbá biztosítani kell, hogy a vezetőség is aktívan támogassa és részvételével legitimálja ezeket a programokat, különben a dolgozók játék helyett gyerekes időpocsékolásnak is gondolhatnák. A tapasztalatok azonban azt mutatják, hogy ahol jól implementálták, ott a gamifikált képzések **gyorsabb bevonódást és jobb tanulási hatékonyságot** eredményeztek a hagyományos oktatáshoz képest [7].

Példa: a fent említett Cyber Drill Studio esetében egy átlagos osztálytermi foglalkozásban 2-3 óra kellett a résztvevők "feloldódásához", míg a játékos platformon mindez alig néhány perc alatt megtörtént, és a végén a kötelező vizsgák átlageredménye jelentősen

javult a korábbi évekhez képest [7]. Ez azt jelenti, hogy a résztvevők gyorsabban kezdtek el aktívan tanulni és jobban rögzültek bennük az ismeretek.

A gamifikált, adaptív képzések mellett is fontos a folyamatos éberség fenntartása. Jó gyakorlat, ha időnként **váratlan teszteket** iktatnak be – például a cég biztonsági csapata időről-időre szándékosan phishing e-mailt küld szét a dolgozóknak, vagy megpróbál bejutni fizikai védelem alá tartozó területre social engineering módszerrel (kvázi belső „red team" gyakorlatként). Az így kapott eredményeket (hányan dőltek be, hol kell javítani) fel lehet használni az adaptív képzés finomhangolására. Lényeges továbbá a **pozitív visszacsatolás**: ha egy dolgozó helyesen jár el egy kísérleti vagy valós incidens során (például jelent egy gyanús telefonhívást vagy megakadályozza egy illetéktelen bejutását), ismerjük el nyilvánosan, ezzel is ösztönözve a többieket a hasonló viselkedésre.

Összefoglalva, a modern, játékosított és adaptív képzésmegoldások integrálása a kritikus infrastruktúrák biztonsági protokolljaiba nagymértékben növelheti a humán védelmi vonal hatékonyságát. Az emberi tényező így nem a „leggyengébb láncszem" lesz, hanem épp ellenkezőleg, a védelmi rendszer tudatos és erős pillére. Az ilyen oktatás révén **kialakítható egy erős biztonságtudatossági kultúra**, ahol minden dolgozó tisztában van a rá leselkedő manipulációs próbálkozásokkal és magabiztosan, begyakorolt módon reagál azokra. Ezzel a kritikus infrastruktúrák védelme egy magasabb szintre emelhető, ahol a technológiai és emberi védelem valódi szinergiában működik.

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

A kutatás rámutatott, hogy a pszichológiai manipuláció az objektumvédelemben az egyik legnagyobb kihívás: a támadók az emberi tényező sebezhetőségét kihasználva képesek kijátszani a legfejlettebb biztonsági rendszereket is. A hatékony védekezés érdekében elengedhetetlen a biztonsági személyzet rendszeres képzése a social engineering támadások felismerésére és kivédésére, az MI-alapú, vagy a rendellenesség alapú behatolás technológiák alkalmazása, valamint a szervezeti protokollok – különösen a beléptetési és incidenskezelési eljárások – szigorítása. Empirikus kutatásaink és esettanulmányaink igazolták, hogy e lépések együttes alkalmazása jelentősen csökkenti a manipulációs kísérletek sikerességét. Összességében a tanulmány megállapította, hogy a technológiai és humán védelmi tényezők párhuzamos erősítése nyújtja a leghatékonyabb védelmet a social engineering támadásokkal szemben. Ugyanakkor a jövőben várhatóan megjelennek olyan új fenyegetések is, mint az MI által támogatott manipulációk és a „deepfake" technikák; ezért a védelmi stratégiákat folyamatosan fejleszteni és adaptálni kell a változó támadási módszerekhez.

ÖSSZEGZÉS ÉS JÖVŐBELI KUTATÁSI IRÁNYOK

A tanulmány átfogóan bemutatta, hogy a humán tényezőt célzó social engineering támadások komoly veszélyt jelentenek a kritikus infrastruktúrák védelmére, és rávilágított a folyamatos képzés, a technológiai támogatás és a szigorú biztonsági protokollok együttes alkalmazásának jelentőségére. **Főbb eredményeink és tanulságaink** szerint a biztonságtudatosság növelése és a pszichológiai manipuláció elleni védelmi intézkedések integrálása

alapvetően fontos az objektumvédelemben. Ugyanakkor a social engineering jellegű fenyegetések dinamikusan fejlődnek, így **további kutatásokra és fejlesztésekre** van szükség a védelmi képességek fenntartása érdekében. Az alábbiakban összefoglaljuk a legfontosabb jövőbeli kutatási és fejlesztési irányokat:

Játékosított, adaptív képzésprogramok fejlesztése

Eredményeink tükrében indokolt olyan *gamifikáció* alapú, interaktív oktatási programok továbbfejlesztése, amelyek képesek alkalmazkodni a résztvevők egyéni tudásszintjéhez és reakcióihoz. Az ilyen adaptív képzések –szituációs gyakorlatok, szimulációk vagy kiberbiztonsági játékok – élményszerű tanulást biztosítanak, növelve a biztonsági személyzet bevonódását és hosszú távú tudásmegtartását. A jövőben érdemes vizsgálni, miként tehetők ezek a programok még hatékonyabbá a kritikus infrastruktúrák védelmében dolgozók számára, különös tekintettel az újonnan felbukkanó támadási formákra.

STEAM-alapú szemlélet kiterjesztése más biztonsági területekre

A tanulmányban alkalmazott megközelítés és a megszerzett tapasztalatok alapján javasolt a **STEAM**-alapú (a műszaki-természettudományos és matematikai oktatást a művészetekkel kreatív módon kiegészítő) szemlélet továbbvitele más, hasonlóan kritikus területekre is. Ilyen lehet a közösségi média manipulációja és a dezinformáció elleni küzdelem, ahol a technológiai ismeretek mellett a pszichológiai, médiaszempontú és kreatív gondolkodásmód integrálása kulcsfontosságú. Egy interdiszciplináris, STEAM-alapú megközelítés segíthet új oktatási modulok és tudatosságnövelő programok kidolgozásában, amelyek szélesebb körben – az iskolai oktatástól a szakmai továbbképzésekig – fejleszthetik a fenyegetések felismerésének és kezelésének képességét.

Nemzetközi együttműködés és sztenderdizáció

Mivel a kritikus infrastruktúrák elleni social engineering támadások globális problémát jelentenek, a védekezés terén elengedhetetlen a nemzetközi szintű együttműködés erősítése. Ajánlott a tapasztalatok és bevált gyakorlatok megosztása nemzetközi fórumokon, valamint közös képzési szabványok és minősítések kialakítása. Európai uniós szinten és más nemzetközi szervezetek keretében érdemes kidolgozni egységes irányelveket a biztonságtudatossági képzésekre és a social engineering incidensek kezelésére. A sztenderdizáció – legyen szó oktatási tananyagokról, minőségbiztosítási keretrendszerekről vagy akár *benchmarking* jellegű támadásszimulációkról – hozzájárulhat ahhoz, hogy a szervezetek világszerte összehangoltan és magas színvonalon készüljenek fel a manipulációs módszerek ellen.

Összefoglalva, a fenti javaslatok mentén haladva tovább növelhető a kritikus infrastruktúrák ellenálló képessége a kifinomult social engineering támadásokkal szemben. A folyamatos innováció, az interdiszciplináris megközelítés és az együttműködés erősítése együttesen biztosíthatja, hogy a védelmi gyakorlatok lépést tartsanak a fenyegetések evolúciójával, és hosszú távon is magas szintű védelmet nyújtsanak az emberi tényezőt kihasználó támadások ellen.

FELHASZNÁLT IRODALOM

[1] National Cyber Security Center (NKI), „Éves kiberbiztonsági jelentés 2023," Budapest, 2024. [Online]. Available: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf

[2] M. Z. Rajnai, B. László, „Az objektumvédelem biztonságtudatos szemlélete a social engineering támadások tükrében," *Biztonságtudományi Szemle*, vol. 12, no. 1, pp. 1–24, 2024.

[3] M. Kapko, „Valid accounts remain top access point for critical infrastructure attacks, officials say," *Cybersecurity Dive*, Dec. 2023. [Online]. Available: https://www.cybersecuritydive.com/news/cisa-critical-infrastructure-attacks/727225

[4] Y. Ahmed, A. Mahfouz, A. Baroudi, and D. Khalil, „Enhancing Security Awareness Through Gamified Approaches," *arXiv preprint*, arXiv:2404.09052v1, Apr. 2024. [Online]. Available: https://arxiv.org/html/2404.09052v1

[5] Industrial Cyber, „HC3 warns of Scattered Spider hackers leveraging AI, social engineering to infiltrate healthcare," *Industrial Cyber*, Jan. 2024. [Online]. Available: https://industrialcyber.co/medical/hc3-warns-of-scattered-spider-hackers-leveraging-ai-social-engineering-to-infiltrate-healthcare-other-sectors

[6] P. A. Bartel and R. L. Smith, „Gamification of Cybersecurity for Workforce Development in Critical Infrastructure," *ResearchGate*, Oct. 2022. [Online]. Available: https://www.researchgate.net/publication/365104009_Gamification_of_Cybersecurity_for_Workforce_Development_in_Critical_Infrastructure

[7] Digital Hungary, „A magyar Games for Business-szel a kiberbiztonság is fogyasztható," *DigitalHungary.hu*, Oct. 2021. [Online]. Available: https://www.digitalhungary.hu/e-kereskedelem/A-magyar-Games-for-Businessel-a-kiberbiztonsag-is-fogyaszthato/8764

[8] C. Owen-Jackson, „Social engineering in the era of generative AI: Predictions for 2024," *IBM Think*, Jan. 2024. [Online]. Available: https://www.ibm.com/think/insights/social-engineering-generative-ai-2024-predictions

[9] M. J. Guitton, „Social Engineering in Critical Infrastructure: An Analysis of Human-Centric Cybersecurity Threats," *Computers & Security*, vol. 105, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102252

[10] J. M. Kowalski, „A Study on Tailgating Attacks in High-Security Environments," *Journal of Physical Security*, vol. 15, no. 3, pp. 42–55, 2022.

[11] Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Coast Guard (USCG), „Fiscal Year 2023 Risk and Vulnerability Assessment Analysis," U.S. Department of Homeland Security, 2023. [Online]. Available: https://www.cisa.gov/resources-tools/resources/fiscal-year-2023-risk-and-vulnerability-assessment-analysis

[12] V. Békefi, „Gamifikáció az oktatásban és a szervezetfejlesztésben," EOQ MNB Szakbizottsági Konferencia, Budapest, 2018. [Online]. Available: https://eoq.hu/szakb/11/ea180924.pdf

[13] T. Rudas, „Gamifikáció az oktatásban – lehetőségek és kihívások," Miskolci Egyetem, Automatizálási és Infokommunikációs Intézet, 2020. [Online]. Available: https://gepesz.uni-miskolc.hu/intezetek/HATVANY/news_files/26_0.pdf

[14] M. Hegedüsné Baranyai, „A gamifikáció hatása a pénzügyi tudatosság fejlesztésére," Magyar Nemzeti Bank, 2019. [Online]. Available: https://www.mnb.hu/letoltes/0328j000.pdf

[15] I. K. Holik, T. Kersánszki, I. D. Sanda, and Z. Márton, „Improving Security and Environmental Awareness through Game-Based Learning with Minecraft," International Journal of Engineering Pedagogy (iJEP), vol. 14, no. 4, pp. 1–18, 2024. [Online]. Available: https://doi.org/10.3991/ijep.v14i4.48127

DOI: https://doi.org/10.12700/btsz.2025.7.2.71

METHODS OF FUNCTION BASED ENGINEERING OF AUTOMOTIVE SAFETY CRITICAL SEALING SYSTEMS

AUTÓIPARI BIZTONSÁGKRITIKUS TÖMÍTŐRENDSZER FUNKCIÓALAPÚ TERVEZÉSÉNEK MÉRNÖKI MÓDSZERTANAI

SÁRI-BARNÁCZ Viktor[1] – FAZEKAS Bálint[2] – GODA Tibor János[3]

Abstract

The growing use of battery electric vehicles brings new challenges to safety-critical sealing systems, as their reliability becomes increasingly important due to higher functional demands. This article presents engineering methods used to define, analyze, and validate sealing functions and related safety aspects. Tools such as FMEA, FAM, DRBFM, DfR and 8D are introduced through a case study of an ASIL D-classified sealing system. Special focus is placed on function-based design and model-based engineering.

Keywords

DRBFM, sealing system, rubber friction, percolation, safety critical, engineering methods

Absztrakt

A tisztán elektromos hajtású járművek elterjedésével új kihívások jelennek meg a biztonságkritikus tömítőrendszerek tervezésében, mivel megnövekedett funkcionális terhelésük miatt megbízhatóságuk egyre fontosabbá válik. A cikk olyan mérnöki módszertanokat mutat be, amelyek a tömítések funkcionális és biztonsági megfelelőségének meghatározására, elemzésére és igazolására szolgálnak. Az alkalmazott eljárások - mint például az FMEA, a FAM, a DRBFM, a DfR vagy a 8D - egy ASIL D besorolású tömítőrendszer esettanulmányán keresztül kerülnek bemutatásra. Kiemelt figyelmet kap a funkcióalapú tervezés és a modellalapú mérnöki megközelítés.

Kulcsszavak

DRBFM, tömítésrendszer, gumisúrlódás, szivárgás, biztonságkritikus, mérnöki módszertanok

[1] viktor.sari@hu.bosch.com | ORCID: 0009-0001-4513-9108 | lead expert, Robert Bosch Kft. | vezető szakértő, Robert Bosch Kft.
[2] balint.fazekas@hu.bosch.com | ORCID: 0000-0001-5716-8531| expert, Robert Bosch Kft. | szakértő, Robert Bosch Kft.
[3] goda.tibor@bgk.uni-obuda.hu | ORCID: 0009-0004-5666-3142| professor, Bánki Donát Faculty of Mechanical and Safety Engineering, Obuda University | egyetemi tanár, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem

INTRODUCTION

Nowadays, the demand for battery electric vehicles (*BEV*) is increasing since they are proven to be more environmentally friendly [1], but the pressure is also there due to regulations targeting emission reduction [2]. Despite the many technical and environmental advantages that the *BEV* have over vehicles with internal combustion engines (*ICE*), there are also technical drawbacks. With the better efficiency of the *BEV* drive system, less heat is generated and thus less energy lost to evaporate environmental condensates in the engine compartment providing more favorable conditions for corrosion, therefore, demanding better, more reliable, and more efficient sealing systems for automotive safety critical applications (*steering, braking, etc.*).

Engineering of safety (*functional safety*) of automotive products has been standardized according to ISO 26262 [3]. This standard provides a framework for automotive safety engineering and defines metrics (see **Figure 1**) to determine how *safety-critical* a component is, based on the *severity* of the potential failure it may cause and how easily it can be prevented. The standard also recommends processes to ensure safety and has the following structure, covering a wide range of safety aspects:

- ISO 26262-1: Vocabulary: Defines common terminology by specifying terms such as *fault, error, failure, etc.*
- ISO 26262-2: Management of functional safety: Describes management practices for functional safety at both organizational and project levels throughout the vehicle lifecycle.

Decreased Controllability

Increased Severity

ASIL (Automotive Safety Integrity Level)		Controllability (C)			
Severity (S)	Expopsure (E)	C0 Controllable in General	C1 Simply Controllable	C2 Normally Controllable	C3 Difficult to Control or Uncontrollable
S0 No Injuries	–	QM			
S1 Light and Moderate Injuries	E0 – Unusual	QM			
	E1 – Very Low Probability	QM			
	E2 – Low Probability	QM			
	E3 – Medium Probability	QM			ASIL A
	E0 – High Probability	QM		ASIL A	ASIL B
S2 Severe Injuries, Possibly Life Threatening	E0 – Unusual	QM			
	E1 – Very Low Probability	QM			
	E2 – Low Probability	QM			ASIL A
	E3 – Medium Probability	QM		ASIL A	ASIL B
	E0 – High Probability	QM	ASIL A	ASIL B	ASIL C
S3 Life Threatening or Fatal Injuries	E0 – Unusual	QM			
	E1 – Very Low Probability	QM			ASIL A
	E2 – Low Probability	QM		ASIL A	ASIL B
	E3 – Medium Probability	QM	ASIL A	ASIL B	ASIL C
	E0 – High Probability	QM	ASIL B	ASIL C	ASIL D

1. Figure: Classification of automotive safety levels according to ISO 26262 (QM – Quality Management, ASIL – Automotive Safety Integrity Level)[4]

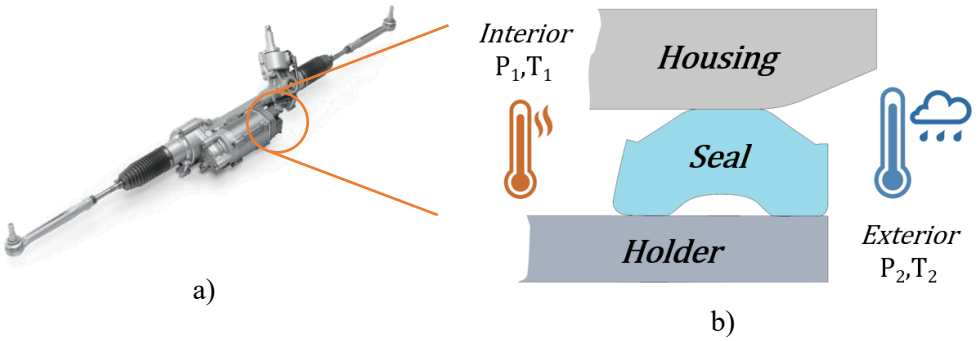
- ISO 26262-3: Concept phase: Covers the concept phase of development, including the identification of hazards and risks (*Hazard Analysis and Risk Assessment – HARA*) and the formulation of the *functional safety concept* with corresponding *safety goals*.
- ISO 26262-4,-5,-6: Product development at the system/hardware/software level: Focuses on the design and development of system/hardware/software by creating the *technical safety concept* (i.e. deriving safety goals into system requirements), also incorporates the safety validation plan.
- ISO 26262-7: Production, Operation, Service, and Decommissioning: Describes functional safety of a product throughout its entire lifecycle.
- ISO 26262-8: Supporting processes: Describes auxiliary processes such as change management, documentation, verification guidelines, and reuse of "*proven-in-use*" system components.
- ISO 26262-9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analysis*:* Provides guidelines for hazard classification. Recommends assignment of *ASIL*s (*A, B, C, D*) to represent different risk levels, with *ASIL D* being the most critical. A classification of *QM* (*quality management*) indicates that standard quality control is sufficient to ensure the safety of the product (**Figure 1**).
- ISO 26262-10,-11,-12: Guidelines on ISO 26262: An in formative guidance supporting application of the standard with examples and detailed explanations for other application domains, such as motorcycles and semiconductors.

Although ISO 26262 covers a wide range of safety aspects, it addresses safety only at a *higher, abstract* level. Many engineering methods have been developed over the years to identify, control, and assess technical risks at the *design detail level*. Some focus on the early identification of potential *failure modes* from a *functional* perspective (such as *FMEA – Failure Modes and Effects Analysis*)[10], [11] and some mapping the domains where the engineering know-how is limited (*FAM – Focus Area Matrix*) [12].

Other methods focusing on *in-depth* analysis of the physical behavior of *design elements* (such as *DfR – Design for Reliability*) [13] and *synthesis* application of *DRBFM* (*Design Review Based on Failure Mode*)[14] to achieve *safe* and *robust* design.

However, due to the high technical complexity, the large number of design parameters, and the production volumes (introducing statistical variability) associated with an automotive product, the *failure* of some design elements is inevitable. Therefore, engineering methods have been developed to manage and mitigate the *risks* once they occur (*PS – Problem solving*) [15] by swiftly handling complexity and identifying the *technical root cause* as early as possible (*analysis* application of DRBFM).

The main part of this article will introduce the most commonly used of these engineering methods, using an *automotive sealing system* as an example.



2. Figure: Automotive sealing system[5]:
a) Steering gear, the main product b) Sealing system of a steering control unit

The subject *sealing system* is a sub-component of a *steering gear*'s servomotor. The servomotor provides the assist to control the steering torque, i.e. the resistance felt by the driver to turn the steering wheel, see **Figure 2 (a)**. The sealing system of the servomotor includes a *form seal* mounted on a plastic component (referred as the *holder* in **Figure 2. (b)**) which provides the sealing effect between the *holder* and the *housing* as well as seals the interior from the humid, wet external environment.

Due to atmospheric effects, a pressure difference may develop between the interior and the exterior, which can lead to water intrusion in the event of *functional failure* of the seal. A temperature difference may also occur, as the internal parts can be heated by operational losses, while exposed to harsh environmental conditions externally.

This *sealing system* is classified as *ASIL D*, as its potential failure - *specifically, water ingress into the encapsulated electronics causing short circuits* - can lead to a sudden loss of (steering) assist. This may easily result in a traffic accident, as the driver may not have time to respond to the abrupt increase in steering resistance, especially during dynamic maneuvers. To assess the functional performance of such a sealing system in line with the *state-of-the-art*, modern theoretical approaches should be considered, such as *percolation theory* [6], [7].

ENGINEERING METHODS OF AUTOMOTIVE SAFETY AND QUALITY

In this section, the most commonly used methods are introduced using the previously presented sealing system as an example, to better illustrate how these methods are applied in practice.

FMEA - Failure modes and effects analysis

This method was originally developed by the *US Military* [16], later adopted by *NASA* and then by *Ford*, who spread the method in the automotive industry. Today, FMEA is considered as a legal document and is mandatory for all automotive suppliers where the *state-of-the-art* of the relevant engineering domain must be considered during thepreparation.

Function	**Failure mode**	**Potential Impact**	**#SEV**	**Potential Casues**	**#OCC**	**Detection Mode**	**#DET**	**#RPN**
For what the customer pays for?	What has gone wrong	What is the impact on the key out-put?	How severe is the effect? (1-10)	What causes to go wrong?	How frequently is this likely to occur? (1-10)	What are the existing controls to prevent the failure from occurring or detect it?	How easy is it to detect? (1-10)	Risk priority number (1-1000)
Seal of steering motor	*Water inside the electronics*	*No steering possible*	*9 (loss of assist)*	*Sealing damaged during assembly*	*2 (rarely happens)*	*Monitoring of assembly forces*	*1 (easy to detect)*	*18 (SxOxD)*

1. Table: Basic template of an FMEA with practical example of functional failure of a sealing system (own construction based on [17])

By principle, FMEA maps potential *functional failure modes* at an early stage of development in order to define measures to mitigate the *risk of the failure* as follows (see **Table 1** with example related to sealing functionality):

0.) FMEA is usually *generated* by following the mechanical structure of the product.
1.) Identification of the **function** of the component: *What's the purpose of the component? What is it supposed to do?*
2.) Identification of the **failure mode**: This is usually defined with involvement of *technical experts* of the subject area, as a single function can have *multiple* failure modes: *What could adversely affect the function*?
3.) Estimation of the **impact of the failure**: *What will the customer experience in event of failure?*
4.) **Severity** rating:
    - **1-3**: Insignificant - almost no impact on function.
    - **4-6**: Minor - partial malfunction, limited impact on functionality.
    - **7-8**: Major - high degree of negative impact on function and *customer satisfaction*.
    - **9-10**: Critical - serious impact that may lead to a *safety hazard* and violation of legal regulations.
5.) **Potential causes**: *What could cause the failur*e?
6.) **Occurrence** rating:
    - **1-3**: Rare - almost no chance of occurrence.
    - **4-6**: Low - low probability of occurrence.
    - **7-8**: Likely – failure is likely to occur.
    - **9-10**: Frequent – failure is almost certain to occur.
7.) **Detection** of the occurrence: *What methods can be used to detect the failure?*
8.) **Detection** rating:
    - **1-3**: High – failure can be confidently detected.
    - **4-6**: Moderate - high chance of detection.

- **7-8**: Low – low chance of detection.
- **9-10**: None – failure cannot be detected.

9.) Determination of **Risk Priority Number (RPN):** The *RPN* is calculated by multiplying the ratings of **severity** (4.), **occurrence** (6.), and **detection** (9.).

Based on the risk rating, further measures can be defined, some focusing on improving the detection, while others aim to eliminate the risk by modifying the design.FAM – **Focus area matrix**

A less formal and less commonly used method than FMEA. Also referred to as *Focus Analysis*. Usually prepared with rougher details of the design of the product, on a *high level* (low complexity). Used to *evaluate* the maturity of the *engineering know-how* in a specific domain, or aspect of the product, considering the known and the new engineering *requirements*. See **Table 2.** for an example where sealing system solutions originally applied in vehicles with *internal combustion engine (ICE)* are evaluated for use in *battery electric vehicles (BEV)*.

Requirements		**Form seal** *Low contact length with high contact pressure*	**Liquid seal** *High contact length with low contact pressure*	**Labyrinth seal** *High contact length with no contact pressure*
BEV(new)	*ICE(old)*			
Thermal load *Low*	Thermal load *High*	*Known and quantified ageing behavior*	*Known and quantified ageing behavior*	*Not affected*
Humidity *High*	Humidity *Moderate*	*Moderate performance expected*	*Unknown performance*	*Very poor performance expected*

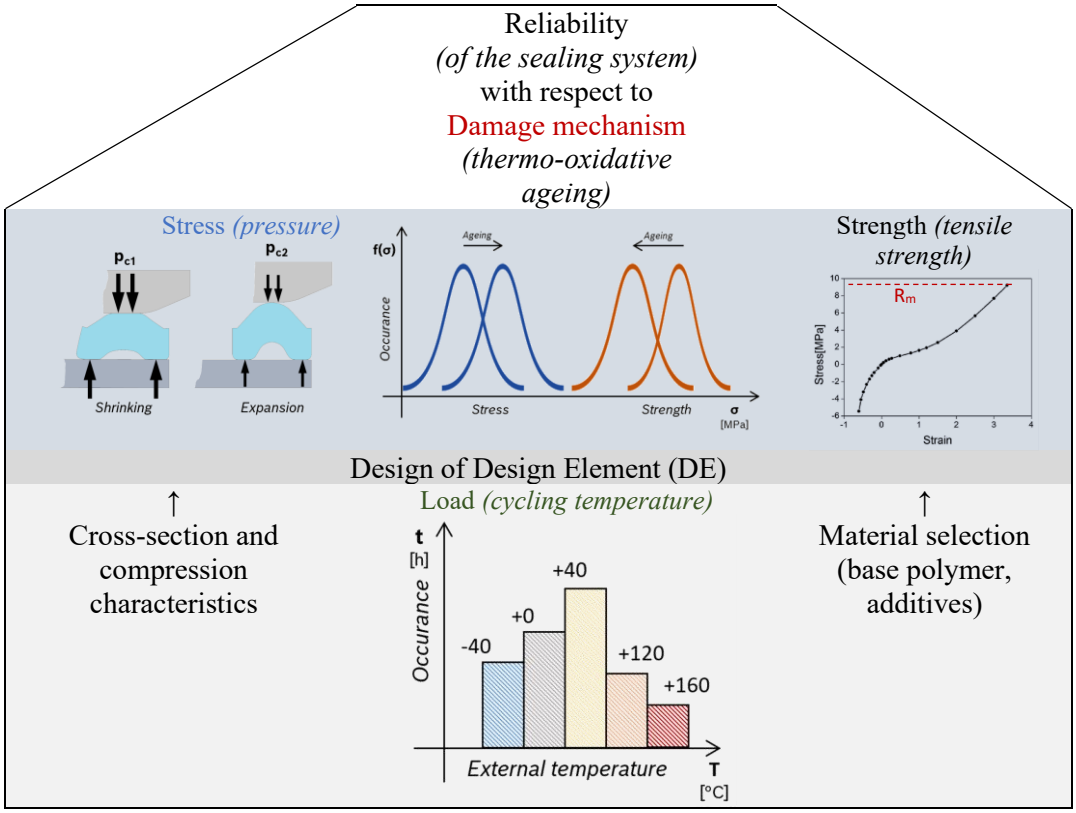
2. Table: Representation of FAM with a practical example of sealing solutions

Based on results of **Table 2,** further engineering tasks can be defined to *quantify* the performance of *liquid seal* (silicone) solution by analyzing percolation [6] of the seal, as well as to asses occurrence of *corrosion*.

DFR – Design for reliability

An engineering method focusing on the details of the design of a specific set of components (*design elements*) using the approach of the *House of Reliability* [18] and the *Five Finger Rule*. It incorporates statistics and a holistic system approach by partitioning the (overall) reliability of that system. The *House of Reliability* (see **Table 3.**) represent the *failure model* (concept) as follows:

- **Load**: sum of external loads acting on the design element *(mechanical, thermal, chemical, etc.). In case of a sealing system, the external temperature variation may induce thermo-oxidative degradation* [19], [20] *and may also generate mechanical loads.*



3. Table: House of reliability – representation of reliability aspects of sealing design element subjected to temperature-driven thermal shrinkage/expansion

- **Stress**: the effect of loads on the design element in relation to the damage mechanism. *In the sealing system example, temperature fluctuations alter the gap into which the seal is assembled (i.e., the available space for the seal), increasing compression forces (stress) within the material. This internal stress is also influenced by the elastic modulus, which itself is affected by thermal degradation.*
- **Strength**: the limiting value of a stress that the *design element* may withstand against the damage mechanism. *Rubber materials typically exhibit a higher degree of variability in material properties. In this case, the tensile strength in their virgin (unaged) state is also affected by aging, as the material becomes brittle over time.*
- **Damage mechanism:** the physical process depending on the duration and intensity of the stress and leads to the degradation of functional characteristic of the design element. *In the case of a sealing system, chemical changes in the material structure - driven by temperature (aging) - cause the material to stiffen. As stiffness increases, so does percolation (i.e., leakage, which is a functional characteristic). Furthermore, for the same level of compression, higher internal stresses develop, increasing the risk of catastrophic failure of the material structure.*

The goal of reliability design is to ensure that the *parameters* of the *design elements* are selected such that the applied stress remains consistently lower than the strength

throughout the product's service life, while also fulfilling other *requirements*, such as legal obligations.

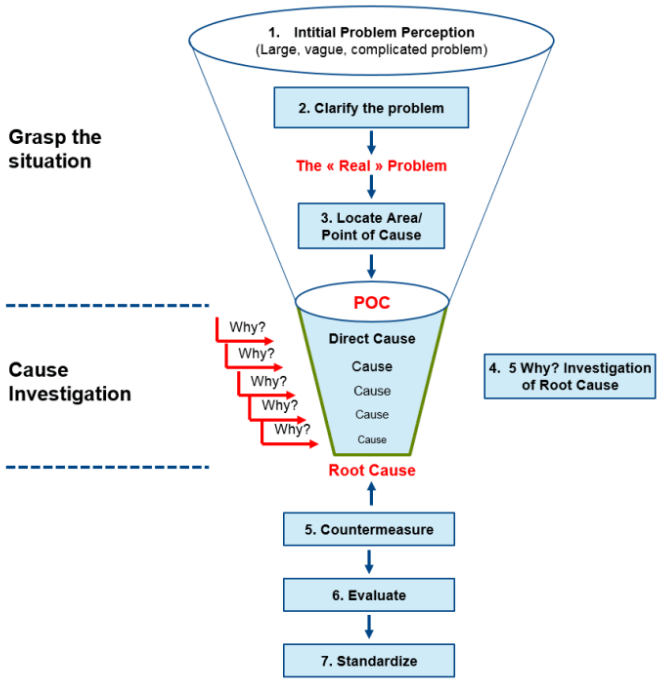
The *Five Finger Rule* is used to define the reliability requirements for the system and *design elements* by considering the following:

- **Functions** as defined in the *FMEA*.
- **Loads**, derived from environmental data and product *specification*.
- **Service time**, as specified by the customer.
- **Reliability targets** of the design elements, as derived through *reliability* partitioning.
- **Failure criteria** defining the conditions that constitute a *functional failure*.

PS – Problem solving

A collection of various engineering methods (*Shainin ,Six Sigma, 8D,etc.*) utilizes a wide range of techniques (*5-Why, Ishikawa, Funnel, etc.*), focusing on handling product failures that occur during development, production, or service [21]. One of the most widely used and well-known methods of automotive sector is the 8D (*Eight Disciplines*), a structured approach, where the problem is defined as a deviation from a defined target caused by an unknown *root cause*. The disciplines are (see **Figure 3.**):

- **D1 - Establish problem solving team**:
  Define a clear list of participants and their responsibilities, including a dedicated team leader and a management sponsor.
- **D2 - Problem definition:**
  Provide a detailed and exact description of the observed deviation, supported by relevant facts and data.
  Example: *During a test production run, a randomized sample was selected from the first batch of seals. In the leakage test, 50% of seals (5 out of 10) showed excessive leakage (Q>30ml/min) when subjected to the pressure of p=5bar at room temperature (23°C) using pure nitrogen (N_2) as test medium.*
- **D3 - Containment action:**
  Define and apply immediate measures to contain the impact of the observed problem and prevent further outflow of defective parts.
  Example: A 100% inspection of seals is performed during production, and any components failing the leakage test are scrapped.
- **D4 - Cause and effect analysis:**
  Identifies the root cause of the problem. There are recommended engineering methods to find the *root cause*, such as *5-Why*, *Ishikawa fishbone diagram.* For complex problems, advanced methods may be required (such as DRBFM).
  Example: Recent percolation theories indicate that the root cause of leakage can be related either to the leakage setup (right setting – pressure difference, right media – viscosity) or to design factors (surface roughness and rubber hardness influencing the percolation channel or contact pressure through geometry and rubber hardness). In this specific case, the supplier had changed certain process parameters of the rubber compound processing, resulting in increased hardness (stiffness) of the seals, which led to excessive leakage.



3. Figure: Lean Problem Solving "The Toyota Way" [21]

- **D5 - Corrective action:**
  Corrective actions must be defined to address both the *Technical Root Cause* (*TRC*) and the *Managerial Root Cause* (*MRC*).
  Example: *In this specific case, the TRC was the change(extension) of curing time of the compound leading to excessive-cross linking of the polymer chains and increased stiffness of the material. The corrective action was to revert the curing time to its original setting. The MRC was that the change can be implemented without detailed analysis of its impact and no hardness measurement were performed on the sealing before shipping.*
- **D6 - Implementation:**
  Implementation and validation of the effectiveness of the corrective actions. *Containment actions* may be withdrawn after successful verification.
  Example: The verification must be done with leakage measurements on the line.
- **D7 - Preventive actions:**
  Define measures to prevent future occurrence of similar problems.
  Example: Implementing in-process hardness measurements can provide early warning that the sealing rubber material may no longer be suitable, helping to prevent leakage-related failures.
- **D8 - Final meeting:**
  Assessment of the problem solving with the participation of all stakeholders.

Nowadays, in many areas of automotive engineering, *Problem Solving* (8D) is a standard practice and typically mandatory in the event of a customer claim. Another often

used method in production is *Shainin (Red-X)* [22], which aims to quickly narrow down *the root cause* of the problem.

DRBFM - Design review based on failure mode

DRBFM is one of the many engineering methods of *Toyota Motor Company* [23]. It was developed to analyze and predict the impact of changes (*risk analysis*) in a product (such as *design, material, tolerances, etc.)* through *function* and *model*-based methodology aimed at preventing future failures (*risk management*). As a modern engineering method, it focuses not only on technical details but also on meta-aspects of engineering, such as communication, in order to improve the efficiency of engineering analysis and to consciously managing of complexity.

The method is based on the following principles [24]:

- **GD^3**: *good design* (well understood and robust), *good discussion* (fact-based and goal-oriented), *good design review* (open, well-structured).

4. Figure: A design review meeting as depicted by Toyota Motor Company [23]

- **Transparent engineering**: engineering decisions and assumptions must be clearly stated and made transparent.
  Example: in the case of a sealing assembly analysis using finite-element simulation, many physical parameters must be assumed, such as the coefficient of friction. If an assumed value is treated as a fact, it can become a source of error.
- **Review culture**: every engineer can - *and should* - contribute to the engineering analysis if participation is enabled, regardless of experience or company status. This is made possible through an open, well-structured, clearly visualized, and goal-oriented review process.
- **Mindset**: show openly the gaps of knowledge with the aim to building understanding on the right complexity level using the most suitable approach (*calculation, simulation, measurement*) as required by the project.
- **Quantification**: both the *requirements of a function* and the *functional performance* of the product can - and should - be quantified in order to accurately manage *risks*, using engineering *models* with the right and *transparent* assumptions.

DRBFM-Techniques

The following techniques are often incorporated in a DRBFM analysis:

- "**Zoom-in**": the proper introduction of an engineering analysis, on the right level of *abstraction* and *resolution* (complexity of details) tailoring the relevant information and adapting the content based on the technical background of review participants (*technical experts, project members, management, etc.*).
- **Work package management**: division of the investigation into sub-tasks taking *priority* and *dependency* into account, enabling the *technical* project management of the sub-tasks of the analysis (e.g., the DRBFM) with clear *scope* and *deliverables*.
- **System view**: conscious handling of the scope of analysis considering *cross-effects* and *hierarchical dependencies* within the product.
- **Function-based engineering:** clear separation of the *problem space* (task of the product) and the *solution space* (design of the product or implementation). This principle is one of the cornerstones of the DRBFM methodology.
- **Physics-design connection** (model-based engineering): principle focusing on understanding the meta-connection between the content of engineering *drawing* and *functional performance* of the product. Another fundamental pillar of the DRBFM methodology.
- **Calculation-simulation-measurement** "triangle": a principle focused on selecting the appropriate engineering tool – *calculation, simulation, or measurement* - based on a clear understanding of its capabilities, limitations, and validity, see **Table 4**.

	Calculation *(Analytical model)*	**Simulation** *(Numerical model)*	**Measurement** *(Experiment)*
Engineering effort	Low-Mid	Mid-High	High-Very high
Cost	Low	High	Very high
Temporal effort	Low	High	Very high
Complexity (that could be handled by..)	Low	High	Very high
Validity	General	Specific	Specific
Confidence (in results)	Low-Mid	Mid-High	High

4. *Table: Aspects of engineering toolsets in DRBFM*

- **Cause-effect chain**: the failure mode is understood as a sequence of events leading to deviation in the *implementation* of the *working principle*.
- **Root cause analysis**: quantified analysis of the *failure mode,* using the *working principle* to enable the selection of the most *effective* and/or economically *feasible* measures to ensure *robustness* against the *functional failure*.
- **Complexity handling**: structuring an engineering analysis both *visually* and *meta-visually - in drawn, spoken and written form* - with the appropriate level of details

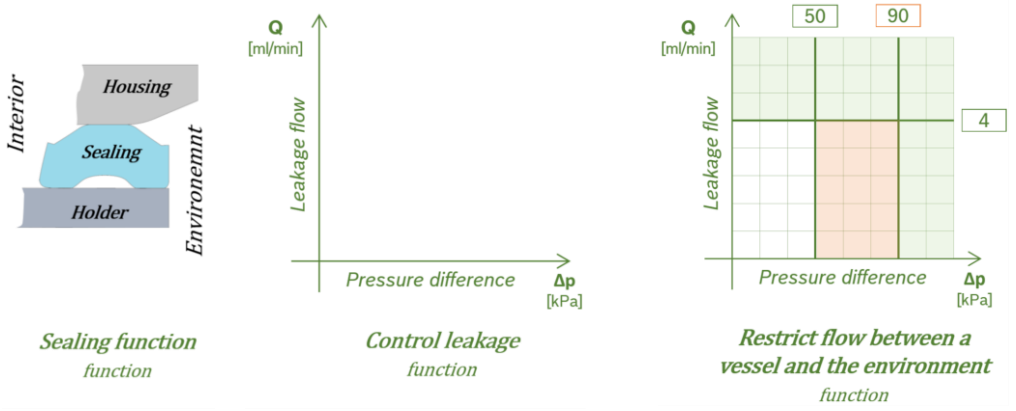
and simplification, adjusted based on the background of review participants (e.g., *experts, managers, etc.*)

Methodical cornerstone of DRBFM : functional definition of a seal

Function-based engineering is one of the most important techniques in the DRBFM methodology, therefore, a more detailed explanation with an example is provided in this section. *Functional* design approach used in automotive engineering aims to clearly separate the *problem space* (*i.e., What problems need to be solved?)* from the *solution space* (*i.e. How are those problems solved?).* This approach enables the *independent* selection of the *working principle (refer to model-based engineering)*, which serves to further distinguish the *solution space* from the *implementation* (*i.e. How it works versus How it is made*).

A definition of a function can be *qualitatively* characterized by how *abstract* and how *complete* its definition is. The appropriate level of abstraction and completeness depends on the engineering intent:

- **Abstract** and **Incomplete:**
  Used when an *impact* or a *risk* requires broad analysis of a poorly known and/or poorly understood system, or when *immediate* engineering (*risk*) assessment is required, see **Figure 5. (a)**,
- **Approximate** and **Partial:**
  Applied during functional system *synthesis* (i.e., *generative* design) to select the *working principle* with the greatest *robustness* (i.e., the least sensitivity to geometrical tolerances and environmental effects), see **Figure 5. (b)**,
- **Exact** and **Complete:**
  Used in functional system *analysis* to *evaluate functional performance* of an existing design, see **Figure 5. (c)**.



a) Abstract and incomplete *b) Approximate and partial* *c) Exact and complete*

5. Figure: Examples (visual representation) for the functional aspects of automotive sealing

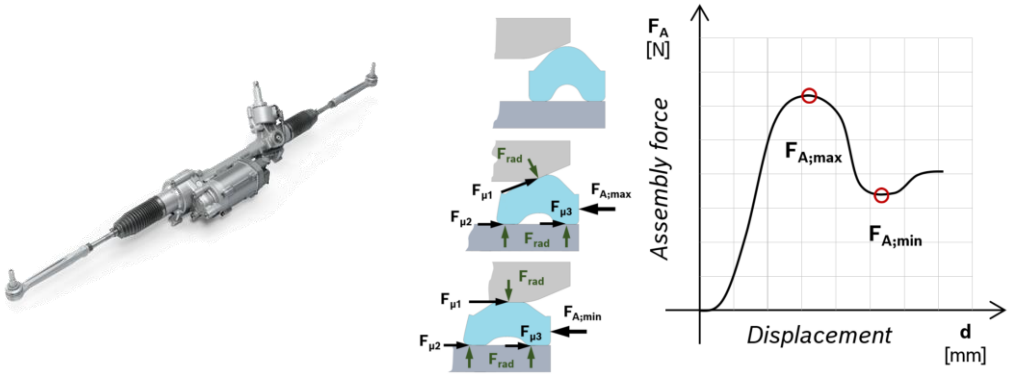
Methodical cornerstone of DRBFM : model-based engineering of a seal

Another cornerstone of the methodology is the model-based engineering, therefore detailed example is also provided – *just as in the case of functions* - to support the better

understanding and to provide insight into how it is used in combination with the other cornerstone.

The sealing effect is created by *compressing* a *soft elastomeric* material with an *assumed* smooth surface against a *hard, rough* (often metallic) surface according to [9]. This compressed state can be achieved through various assembly methods, such as *radial type – press-fit* or *axial type – heat shrinking.*

In the following section, a *model-based engineering* approach of *axial* sealing assembly will be presented. For *this* specific example, results from a seal-assembly study previously published by the authors of this article are used, see **Figure 6.** [5].



a) Steering system *b) Assembly process*

6. Figure: Assembly process of an automotive seal [5]

The *geometry* and the *material* of the seal must be selected according to the following conditions of the assembly:

- Due to the parallel assembly process, the sealing must *withstand* a temperature range of $T = 180°C \dots 250°C$. Given the selected material - *ethylene-acrylic elastomer* – which has a known limit to thermal exposure (time of $t = 5s$) the minimum assembly speed can be defined. To reach the target position of $d = 15mm$ within the allowed time, the speed must be $v = \frac{d}{t} = 5\,{}^{mm}/_{s}$
- According to *percolation theory* [7], the fulfillment of the sealing *function* (see **Figure 6.**) requires that the seal exert a minimum of *contact pressure* $p = 1MPa$ with minimal *contact length* $l = 0.6mm$ under all potential operating conditions, defined by the *environmental temperature* range$T = -30°C \dots 100°C$. Due to product design constrains – such as *thermal expansion* and *geometrical tolerances* – the seal must accommodate *variable* gap in the range of $g = 1 \dots 3mm$. These variations directly influence the *radial stiffness* of the sealing. By designing the seal with *nonlinear spring characteristics*, it is possible to minimize the *stresses* while still maintaining the sealing performance in *large gaps*.
- Based on geometry defined in (2), further aspects of the assembly can be engineered. Since the seal is deformed from *stress-free* to a *compressed* state with *axial* assembly method (*press-fit*), a chamfer must be applied with standard angle of $\alpha = 20°$, which restricts the *apparent coefficient of friction* $\mu = atan(\alpha) = 0.367$ to avoid self-locking - a *functional failure*.

- An additional requirement arises from the need to detect proper assembly. As established in step (2), it is known that this sealing geometry generates a *normal force* $F_N = 3500 \dots 800N$. During detection, *the axial force* is measured which must be at least $F_A = 100N$ to confirm the right position of the seal. This imposes a constrain to the minimum *apparent coefficient of friction* to satisfy $\mu = {F_A}/{F_N} = 0.125$.

From step (2) to (4) it becomes clear that the forces during assembly can be controlled by *controlling the friction* – which itself emerges as a *new function*. It is well known that rubber friction (*friction phenomenon* of the seal assembly) is strongly influenced by multiple factors, including *temperature* [25], sliding *speed* [26], *viscoelastic* behavior of the rubber [27], as well as the structure of the *surface* [28]–[30] demanding accurate description of the *friction phenomena* occurring during the assembly, highlighting the need for more research in this engineering field.

SUMMARY AND CONCLUSIONS

This article gives a practical overview of engineering methods used to evaluate and improve the functional reliability of automotive sealing systems, with a focus on safety-relevant applications. It compares several methodologies and highlights their specific purpose and when they are best applied:

- **FMEA** – Used early in development to define functions and identify potential failure modes, useful for structured risk assessment in known systems.
- **FAM (Focus Area Matrix)** – Applied when the system is not yet fully understood, helps to identify knowledge gaps and critical areas.
- **DRBFM (Design Review Based on Failure Mode)** – Supports detailed design reviews, especially after changes; effective in tracking how modifications affect reliability.
- **DfR (Design for Reliability)** – Applied throughout design phases to ensure robustness.
- **8D** – Used mainly during production or field failures for structured problem solving; focuses on root cause elimination and corrective actions.

The presented methods support structured engineering thinking and help ensure functional safety in sealing applications with increasing performance demands. By selecting and applying the right methodology at the right stage - *whether it's early risk identification, design validation, or problem solving* - reliability can be improved in a focused and traceable way.

REFERENCES

[1] "Electric vehicles from life cycle and circular economy perspectives - TERM 2018," Nov. 22, 2018. https://www.eea.europa.eu/en/analysis/publications/electric-vehicles-from-life-cycle (accessed Feb. 05, 2025).

[2] *Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law')*, vol. 243. 2021. Accessed: Jan. 03, 2024. [Online]. Available: http://data.europa.eu/eli/reg/2021/1119/oj/eng
[3] "ISO 26262-1:2018(en), Road vehicles — Functional safety — Part 1: Vocabulary."
[4] "What is ISO 26262? Automotive Electronics Safety," *Arrow.com*. https://www.arrow.com/en/research-and-events/articles/understanding-iso-26262 (accessed Feb. 05, 2025).
[5] Sári-Barnácz V. and Goda T. J., "Indirekt hiperelasztikus anyagmodell identifikáció autóipari gyártósor tömítésszerelési adatainak felhasználásával," *Gép*, vol. 75, no. 3–4, pp. 91–96, 2024, doi: 10.70750/GEP.2024.3-4.20.
[6] B. N. J. Persson, O. Albohr, U. Tartaglino, A. I. Volokitin, and E. Tosatti, "On the nature of surface roughness with application to contact mechanics, sealing, rubber friction and adhesion," *J. Phys. Condens. Matter*, vol. 17, no. 1, pp. R1–R62, Jan. 2005, doi: 10.1088/0953-8984/17/1/R01.
[7] B. N. J. Persson and C. Yang, "Theory of the leak-rate of seals," *J. Phys. Condens. Matter*, vol. 20, no. 31, p. 315011, Aug. 2008, doi: 10.1088/0953-8984/20/31/315011.
[8] B. Lorenz and B. N. J. Persson, "Leak-rate of seals: effective medium theory and comparison with experiment." arXiv, Nov. 16, 2009. doi: 10.48550/arXiv.0911.3019.
[9] B. Lorenz and B. N. J. Persson, "Leak rate of seals: Comparison of theory with experiment," *Europhys. Lett.*, vol. 86, no. 4, p. 44006, Jun. 2009, doi: 10.1209/0295-5075/86/44006.
[10] "The Basics of FMEA," *Routledge & CRC Press*. https://www.routledge.com/The-Basics-of-FMEA/Mikulak-McDermott-Beauregard/p/book/9781563273773 (accessed Jan. 07, 2025).
[11] A. Webmaster, "Details." https://www.aiag.org/store/publications/details?ProductCode=FMEAAV-1 (accessed Jan. 07, 2025).
[12] "The Design of Focus Area Maturity Models," *ResearchGate*. https://www.researchgate.net/publication/221581365_The_Design_of_Focus_Area_Maturity_Models (accessed Jan. 07, 2025).
[13] "Design for Reliability - 1st Edition - Jerry C. Whitaker - Dana Crowe." https://www.routledge.com/Design-for-Reliability/Crowe-Feinberg/p/book/9780849311116 (accessed Jan. 07, 2025).
[14] "Introduction to Design Review Based on Failure Modes (DRBFM) Web Course RePlay - SAE Training." https://www.sae.org/learn/content/pd331047on/ (accessed Jan. 07, 2025).
[15] "Download for free - 8D Problem Solving for Automotive Engineer e-book," *Automotive Quality Solutions*. https://www.automotivequal.com/free-quality-ebooks-8d-problem-solving-for-automotive-engineer/ (accessed Jan. 07, 2025).
[16] "MIL-STD-1629 A PROCEDURES PERFORMING A FAILURE MODE." http://everyspec.com/MIL-STD/MIL-STD-1600-1699/MIL_STD_1629A_1556/ (accessed Jan. 08, 2025).

[17] G. Forrest, "FMEA (Failure Mode and Effects Analysis): A Quick Guide to Minimizing Defects and Faults in Your Projects," *isixsigma.com*, Sep. 23, 2024. https://www.isixsigma.com/fmea/fmea-quick-guide/ (accessed Jan. 07, 2025).
[18] M. Braglia, G. Fantoni, and M. Frosolini, "The house of reliability," *Int. J. Qual. Reliab. Manag.*, vol. 24, no. 4, pp. 420–440, Jan. 2007, doi: 10.1108/02656710710740572.
[19] J. DUARTE and M. ACHENBACH, "On the modelling of rubber ageing and performance changes in rubbery components," *Model. Rubber Ageing Perform. Chang. Rubbery Compon.*, vol. 60, no. 4, pp. 172–175, 2007.
[20] A. Plota and A. Masek, "Lifetime Prediction Methods for Degradable Polymeric Materials—A Short Review," *Materials*, vol. 13, no. 20, Art. no. 20, Jan. 2020, doi: 10.3390/ma13204507.
[21] P. B.-M.-C. Manager @fabriq, "Lean problem solving tools and methods," *Fabriq*, Sep. 06, 2024. https://fabriq.tech/en/2024/09/06/lean-problem-solving-tools-and-methods/ (accessed Mar. 10, 2025).
[22] "Red X Problem Solving | Solve Complex Problems Fast," *Shainin LLC*. https://shainin.com/red-x/ (accessed Mar. 10, 2025).
[23] "TOYOTA MOTOR CORPORATION GLOBAL WEBSITE | 75 Years of TOYOTA | Research and Development Support | Improvements to the Engineering Planning and Development Process." https://www.toyota-global.com/company/history_of_toyota/75years/data/automotive_business/products_technology/research/engineering_planning/details.html (accessed Mar. 19, 2025).
[24] H. Shimizu, Y. Otsuka, and H. Noguchi, "Design review based on failure mode to visualise reliability problems in the development stage of mechanical products," *Int. J. Veh. Des.*, vol. 53, no. 3, p. 149, 2010, doi: 10.1504/IJVD.2010.033827.
[25] K. A. Grosch, "The Relation between the Friction and Visco-Elastic Properties of Rubber," *Proc. R. Soc. Lond. Ser. A*, vol. 274, pp. 21–39, Jun. 1963, doi: 10.1098/rspa.1963.0112.
[26] A. Schallamach, "A theory of dynamic rubber friction," *Wear*, vol. 6, no. 5, pp. 375–382, Sep. 1963, doi: 10.1016/0043-1648(63)90206-0.
[27] K. C. Ludema and D. Tabor, "The friction and visco-elastic properties of polymeric solids," *Wear*, vol. 9, no. 5, pp. 329–348, Sep. 1966, doi: 10.1016/0043-1648(66)90018-4.
[28] B. N. J. Persson, "Theory of rubber friction and contact mechanics," *J. Chem. Phys.*, vol. 115, no. 8, pp. 3840–3861, Aug. 2001.
[29] J. A. Greenwood and J. H. Tripp, "The Contact of Two Nominally Flat Rough Surfaces," *Proc. Inst. Mech. Eng.*, vol. 185, no. 1, pp. 625–633, Jun. 1970, doi: 10.1243/PIME_PROC_1970_185_069_02.
[30] M. Ciavarella, "A simplified version of Persson's multiscale theory for rubber friction due to viscoelastic losses." arXiv, Jan. 13, 2017. doi: 10.48550/arXiv.1701.03810.

AKNOWLEDGEMENTS

Project no. EKÖP-24-KDP-1 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the 2024-2.1.2 University Research Scholarship Program - Cooperative Doctoral Program funding scheme.

DOI: https://doi.org/10.12700/btsz.2025.7.2.89

A REVIEW OF THE MULTIFACETED NATURE OF CORROSION: THE IMPACT OF STEEL FORMABILITY AND SURFACE ROUGHNESS ON CORROSION RESISTANCE (PART 2)

A KORRÓZIÓS MEGHIBÁSODÁSOK ÁTTEKINTÉSE: AZ ACÉL ALAKÍTOTTSÁGÁNAK ÉS FELÜLETI ÉRDESSÉGÉNEK HATÁSA A KORRÓZIÓÁLLÓSÁGRA (2. RÉSZ)

HUSZÁK Csenge[1] – KOVÁCS Tünde Anna[2] – PINKE Péter[3]

Abstract

This two-part review article presents the diverse nature of corrosion, focusing on the effects of steel formability and surface roughness. In the first part of our article, we introduced corrosion and its main types, followed by a case study. In this article, we present additional case studies. The case studies partly confirm our general views and highlight the properties of individual corrosion-resistant steels. The results emphasise the need for comprehensive testing methods to use these factors, ensuring that the quality of the chemical composition and the manufacturing technology are also taken into account when selecting materials for safety-critical applications.

Keywords

Safety Critical Components, Corrosion, Surface Roughness, Corrosion Resistance, Structural Safety

Absztrakt

Ez a két részes áttekintő cikk a korrózió szerteágazó természetét mutatja be, fókuszban az acél alakítottságának és felületi érdességének hatására. Cikkünk első részében a korróziót, és annak főbb típusait mutattuk be, melyet követően bemutattunk egy esettanulmányt. E cikkben további esettanulmányokat mutatunk be. Az esettanulmányok részben igazolják az általános nézeteinket, illetve rámutatnak egy-egy korrózióálló acél tulajdonságára. Az eredmények hangsúlyozzák az átfogó tesztelési módszerek szükségességét, amelyek figyelembe veszik ezeket a tényezőket, biztosítva, hogy a biztonságkritikus alkalmazásokhoz használt anyagok kiválasztásakor a kémiai összetétel mellett a felületi minőséget és a gyártástechnológiát is figyelembe vegyék.

Kulcsszavak

Biztonságkritikus komponensek, Korrózió, Felületi érdesség, Korrózióállóság, Szerkezeti integritás

[1] huszak.csenge@bgk.uni-obuda.hu | ORCID: 0000-0001-8817-5435 | PhD Student, Óbuda University - Doctoral School on Safety and Security Sciences | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] kovacs.tunde@bgk.uni-obuda.hu | ORCID: 0000-0002-5867-5882 | University Professor, Óbuda University - Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[3] pinke.peter@bgk.uni-obuda.hu | ORCID: 0000-0003-2438-9957 | Associate Professor, Óbuda University - Bánki Donát Faculty of Mechanical and Safety Engineering | Egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

Corrosion is a significant problem in the industry, as the degradation of metals and other structural materials due to environmental influences can cause severe economic damage. It can significantly reduce the service life of industrial equipment, pipelines, tanks, and other structures, increasing maintenance and replacement costs. In addition, corrosion can pose safety risks, especially in industries such as the oil and gas, chemical, and energy sectors.

In the first part of our two-part review article, we described the main types of corrosion, reviewed the environmental influences that affect corrosion, and presented a case study in which the effects of temperature, pressure, the flow rate of the medium in contact with the material, and surface roughness on corrosion were examined. In this article, we present additional case studies.

REVIEW OF CASE STUDIES

Effect of Surface Roughness on Corrosion (Case Studies)

M. D. Giuseppe conducted corrosion tests [1] on AISI 430 (ferritic stainless steel), AISI 430F (martensitic stainless steel), AISI 303 (sulphur-enriched Cr-Ni austenitic stainless steel), AISI 304L (sulphur-free Cr-Ni austenitic stainless steel), and AISI 316L (Cr-Ni-Mo austenitic stainless steel) steels in his thesis. He performed the tests with both drawn and ground surface finishes.

In his work, Giuseppe conducted potentiodynamic polarisation, potentiostatic polarisation, ferric chloride solution, salt spray, and two different atmospheric corrosion tests on his samples. Among these tests, the potentiodynamic and potentiostatic tests are electrochemical corrosion tests accelerated by electricity, the chloride solution immersion and salt spray tests are chemically accelerated tests. In contrast, the atmospheric test is a real-time test. This review will describe the atmospheric salt spray and atmospheric tests.

When exposed to chloride-containing atmospheres, salt spray corrosion tests are used to determine the local corrosion resistance of stainless steel. The test aims to provide a qualitative comparison of different samples' resistance to pitting corrosion attacks in an accelerated real working environment simulation. The observed parameters are the time of corrosion appearance and the rate of spread.

Giuseppe tested three samples of each steel type and surface finish. He performed the tests daily, with weekly photographic reports on the macroscopic condition of the surface and the microscopic condition of the same samples to better observe and document the appearance of pitting corrosion. The following images (Figure 1 – 14) show the samples with a camera and a microscope after 0, 168, 336, and 816 hours.

Figure 1. AISI 430F (drawn surface finish) samples after 0, 168, 336, and 600 hours. [1]

Figure 2. AISI 430F (ground surface finish) samples after 0, 168, 336, and 600 hours. [1]

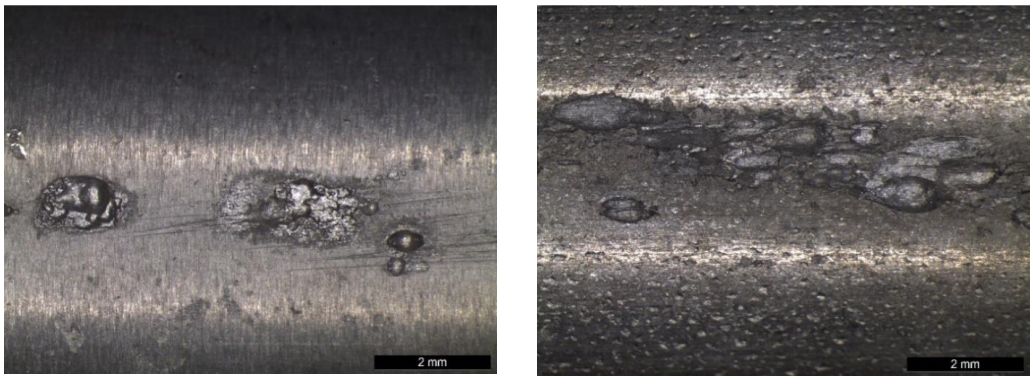


Figure 3. Microscopic image of AISI 430F drawn and ground surface samples. [1]

Figure 4. AISI 430 (drawn surface finish) samples after 0, 168, 336, and 816 hours. [1]

Figure 5. AISI 430 (ground surface finish) samples after 0, 168, 336, and 816 hours. [1]

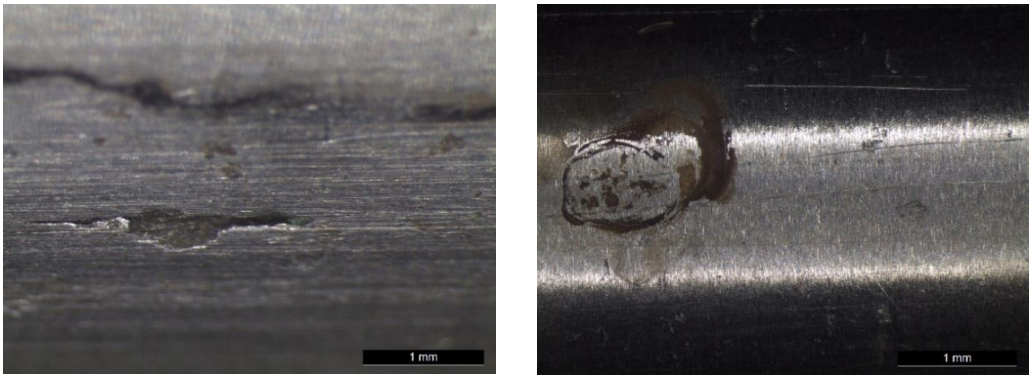


Figure 6. Microscopic image of AISI 430 drawn and ground surface samples [1]

Figure 7. AISI 303 (ground surface finish) samples after 0, 168, 336, and 816 hours. [1]

Figure 8. AISI 303 (ground surface finish) samples after 0, 168, 336, and 816 hours. [1]

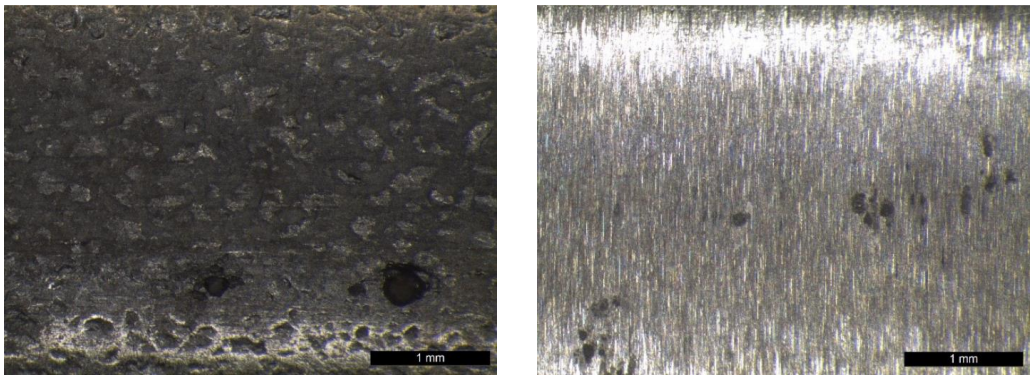


Figure 9. Microscopic image of AISI 303 drawn and ground surface samples. [1]

Figure 10. AISI 304L (drawn surface finish) samples after 0, 168, 336, and 816 hours. [1]

Figure 11. AISI 304L (ground surface finish) samples after 0, 168, 336, and 816 hours. [1]

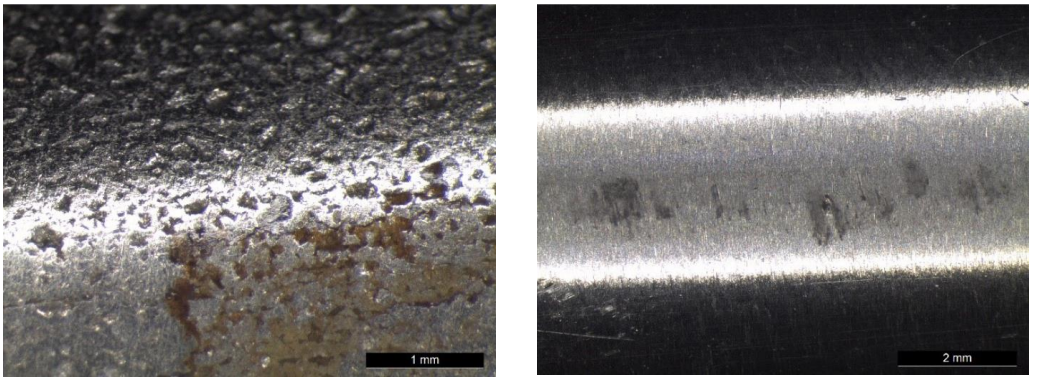


Figure 12. Microscopic image of AISI 304L drawn and ground surface samples. [1]

Figure 13. AISI 316L drawn and ground surface finish samples after 0 and 816 hours (first two images show the drawn sample before and after salt spray, the second two images show the ground sample before and after salt spray). [1]

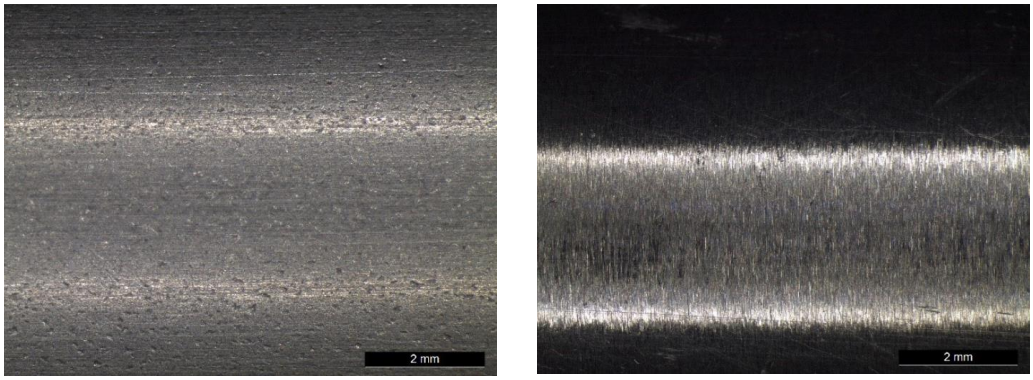


Figure 14. Microscopic image of AISI 316L drawn and ground surface samples. [1]

From his tests, Giuseppe concluded that the ground surface finish samples were more resistant to pitting corrosion than the drawn samples. The AISI 304L and 316L samples showed no signs of corrosion even after 816 hours of continuous exposure. The AISI 430F samples showed significant signs of corrosion early in the test and were removed from the chamber after 600 hours.

His atmospheric tests were interesting due to the choice of locations. These tests compare the results obtained at real, potential usage sites with later laboratory accelerated tests. These comparisons show how much damage occurs in a given time during accelerated tests compared to real conditions. These measurements compare the first appearance of corrosion during the salt spray test (or other lifespan tests) with the first appearance of corrosion in real conditions.

Giuseppe conducted atmospheric corrosion tests in Milan and Cefalù, Northern Sicily, 20 meters from the shore, for nearly 3/4 of a year. During this time, the highest temperature in Milan was 30°C; the lowest was -2°C and the average temperature was 15.6°C. The average humidity during the test period was 73%. The same values in Cefalù were 33°C, -4°C, and 33°C, with an average humidity of 52%. The following figures (Fig. 15-19) show

the results of the corrosion tests caused by the marine atmosphere, as the extent of corrosion in the urban environment was not observable.

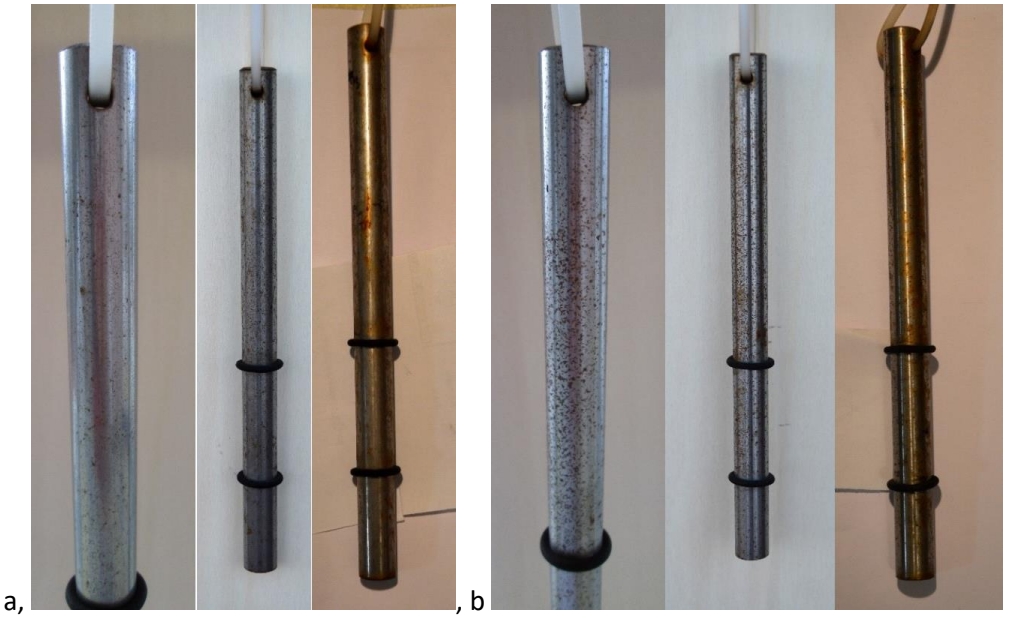


Figure 15. AISI 430F samples in the marine atmosphere after 80, 210, and 270 days a) with drawn surface finish; b) with ground surface finish [1]

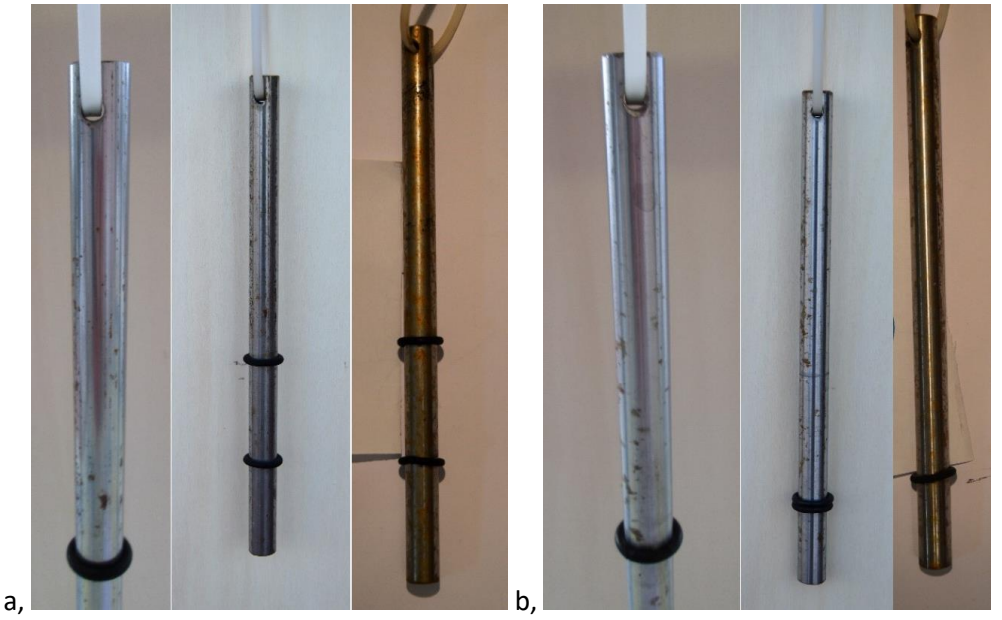


Figure 16. AISI 430 samples in the marine atmosphere after 80, 210, and 270 days a) with drawn surface finish; b) with ground surface finish. [1]

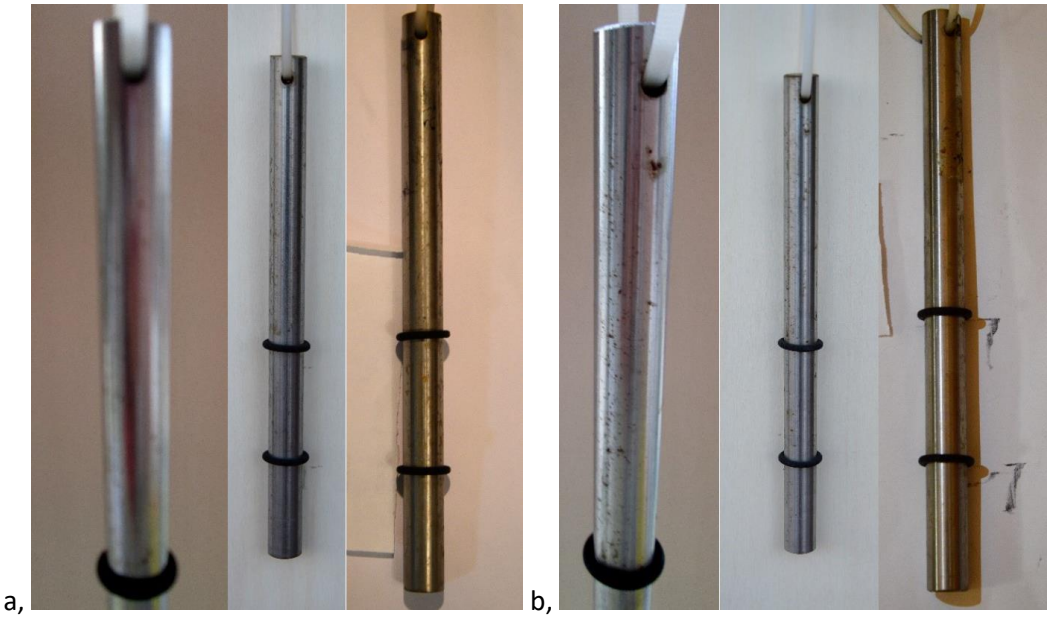


Figure 17. AISI 303 samples in the marine atmosphere after 80, 210, and 270 days a) with drawn surface finish; b) with ground surface finish [1]

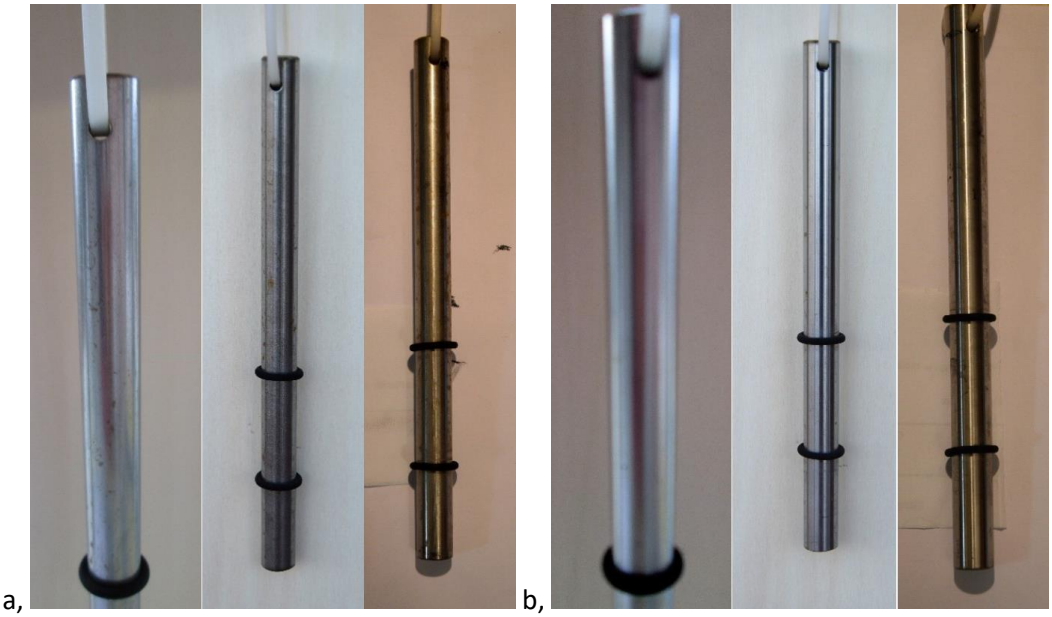


Figure 18. AISI 304L samples in the marine atmosphere after 80, 210, and 270 days a) with drawn surface finish; b) with ground surface finish. [1]

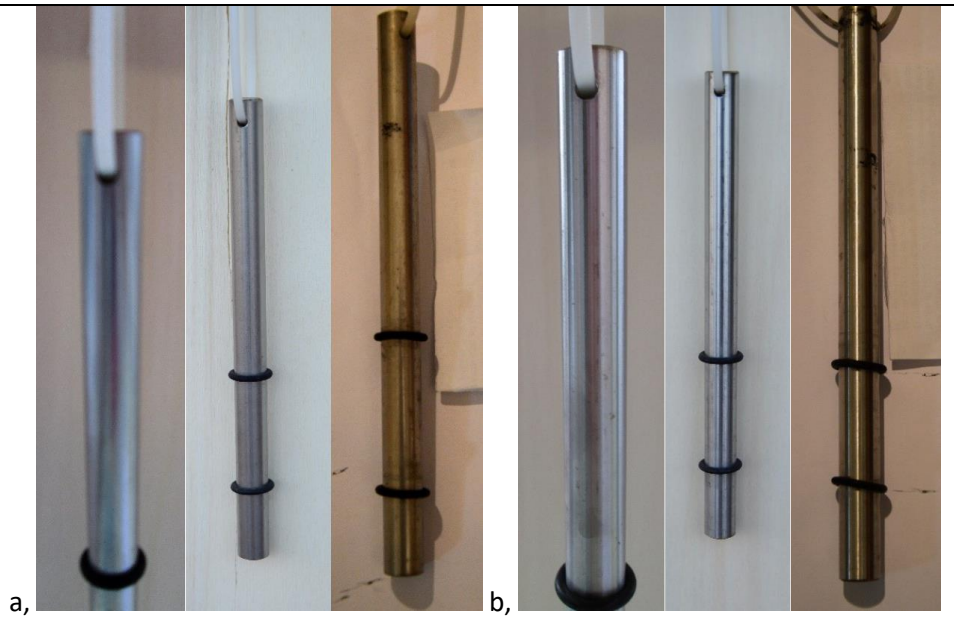


Figure 19. AISI 316 samples in the marine atmosphere after 80, 210, and 270 days a) with drawn surface finish; b) with ground surface finish [1]

Based on the results of these two tests, Giuseppe concluded that in the salt spray test, the ground samples were more resistant to pitting corrosion than the drawn samples. The AISI 304L and 316L samples showed no signs of corrosion even after 816 hours of continuous exposure. The AISI 430F samples showed significant corrosion early in the test.

In the case of the atmospheric exposure test, the samples resisted corrosion in the Milan atmosphere during the nine-month test period, but the marine environment was much more corrosive, as all samples showed discolouration, although none showed pitting corrosion. The AISI 316L samples did not suffer pitting corrosion, but both surface treatments became more opaque compared to the start of the test. The AISI 430 and 430F samples showed high-density dark discolourations on their surfaces, with the drawn samples discolouring more than the ground ones.

Giuseppe concluded from the tests presented here and further tests detailed in his thesis that despite different textures and chemical compositions, samples with ground surfaces showed better corrosion resistance in his tests than those with drawn surface finishes of the same material quality.

Haraszti et al. [2] [3] [4], and Tóth et al. [5] [6] conducted corrosion tests on welded stainless steels. They polished various samples with P120, P180, P320, and P400 grit sandpaper during their study. Some of the samples were heat-treated to simulate the heat-affected zone of the welding process, with the duration and temperature range of the heat treatment comparable to the welding process. The heat-treated and non-heat-treated samples were immersed in a 30°C ferric chloride solution for 96 hours.

In their research, the mass change of the heat-treated test specimens was measured. Based on this, they concluded that the heat-treated test specimens exhibited greater mass change, meaning a larger volume of material corroded during the test period, compared to the non-heat-treated specimens.

Effect of Steel Formability on Corrosion (Case Study)

Corrosion resulting from formability is associated with numerous factors linked to the manufacturing process. This review does not delve into the manufacturing technology and its parameters. This chapter presents a case study focusing on stress corrosion. The study's conclusion highlights that corrosion depends on many factors. The effects of some parameters (e.g., heat treatment) are well-defined, while the impact of other parameters (e.g., rolling) are not clearly defined due to various other phenomena [7] [8] [9] [10] [11].

Xu et al. [12] investigated 3D-printed 316L stainless steel. They prepared test specimens from 3D-printed 316L stainless steel and subjected them to mechanical and microscopic examinations [12]. The samples were made using Wire-Arc Additive Manufacturing (WAAM), a 3D printing method involving a wire electrode arc welding device that builds the desired object through deposition welding. The print head, i.e., the welding wire, was followed by a roller that compacted the object with a force of 8 kN. The schematic diagram and thermal image of this process are shown in the following figure (Fig. 20).

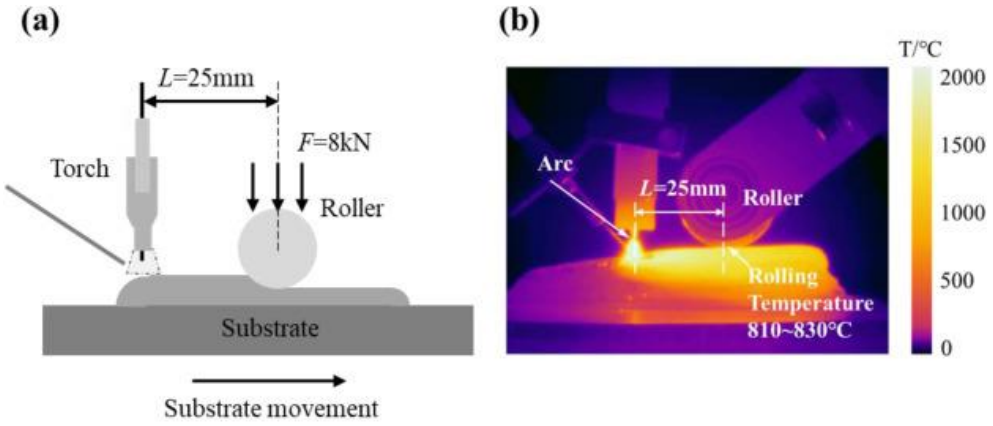


Figure 20. Schematic (a) and thermography photo (b) of the preparation of 3D-printed rolled samples. [12]

After preparing the samples, they were subjected to various heat treatments. The following two figures show the optical microscope images (Figure 21) and Back-Scattered Electron (BSE) scanning electron microscopy images (Figure 22) of the non-rolled and rolled test specimens at different temperatures.

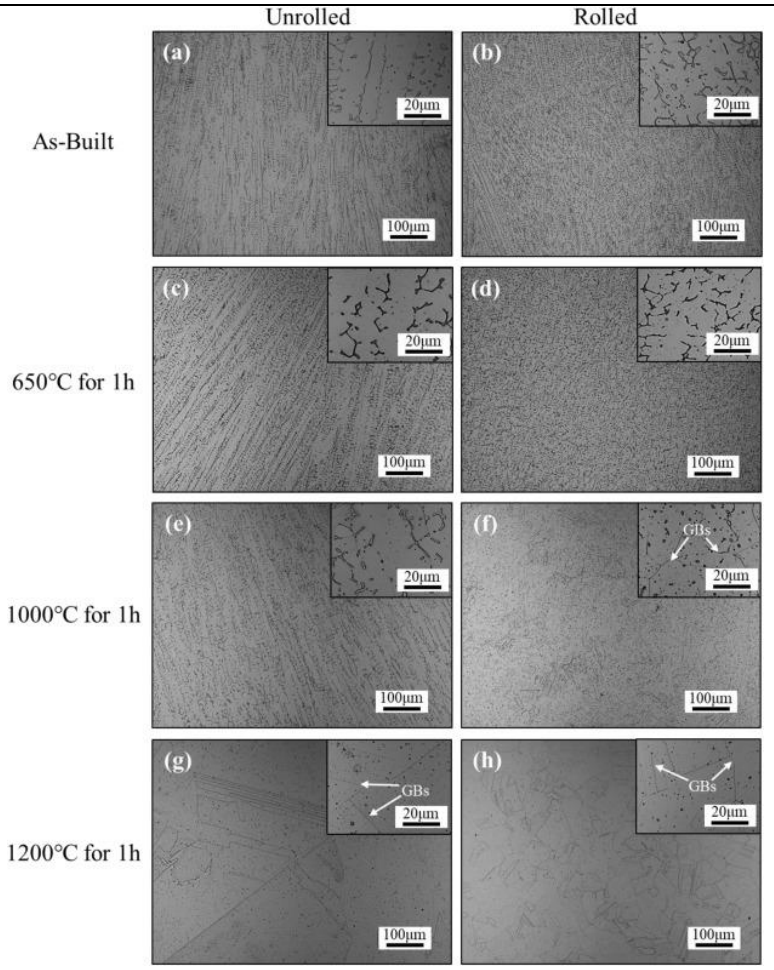


Figure 21. Optical microscope images of test specimens examined at different temperatures non-rolled and rolled test specimens without heat treatment (a, b), heat-treated at 650°C (c, d), heat-treated at 1000°C (e, f), and heat-treated at 1200°C (g, h). [12]

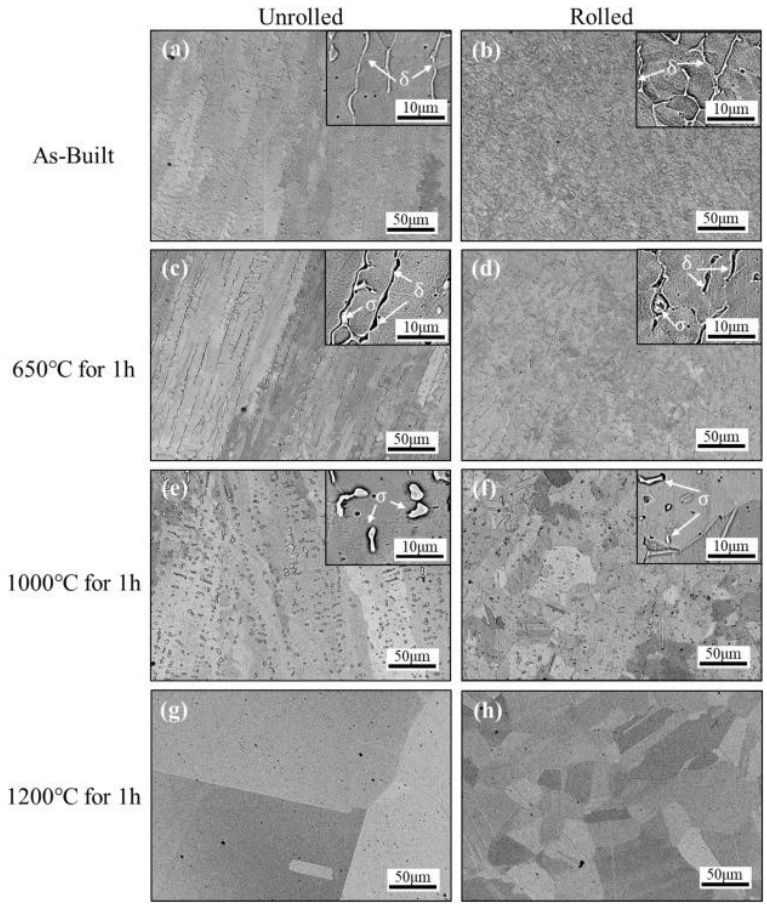


Figure 22. BSE microscope images of test specimens examined at different temperatures non-rolled and rolled test specimens without heat treatment (a, b), heat-treated at 650°C (c, d), heat-treated at 1000°C (e, f), and heat-treated at 1200°C (g, h). [12]

In the previous figures, Xu et al. observed the change in grain size, for which they prepared the schematic diagram shown in the following figure (Figure 23).

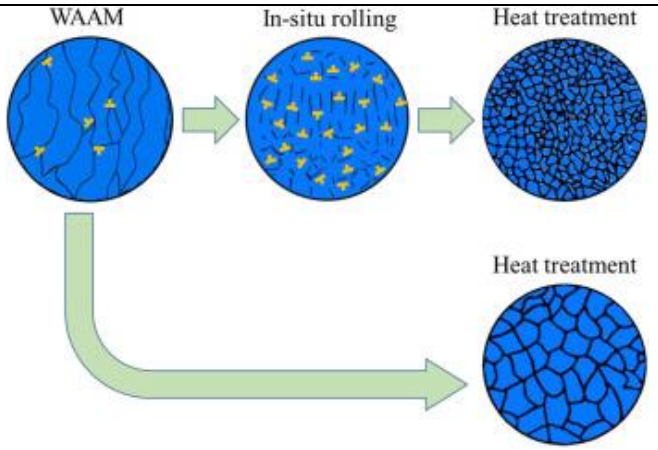


Figure 23. Schematic diagram of recrystallization and the change in dislocation density during rolling and heat treatment following WAAM 3D printing. [12]

Xu et al. found that heat treatment improved the mechanical properties of the 3D-printed samples made using the WAAM method when the samples were heat-treated and rolled. Xu et al. conducted potentiodynamic polarisation measurements in a 3.5% sodium chloride solution to measure the corrosion properties. Generally, lower corrosion current density indicates a slower corrosion rate, and a larger difference between pitting potential and corrosion potential indicates a wider passivation range, which signifies good corrosion resistance.

Xu et al. found that after heat treatment at 650°C, the corrosion current density decreased, and the passivation range also became smaller. This indicates that although the corrosion rate is slower, the stability of the passive film is not as good. After heat treatment at 1000°C, the corrosion current density increased, and the passivation range further narrowed, indicating worse corrosion resistance. This is explained by the precipitation of the σ phase and the formation of chromium-depleted zones. Heat treatment at 1200°C resulted in the best corrosion resistance, as the σ phase and δ ferrite completely dissolved, forming a fully austenitic microstructure [12] [13] [14] [15].

They also examined the effects of rolling in their article but could not draw a clear conclusion. Xu et al. found in their literature review that rolling causes residual stress and high dislocation density, which increases the diffusion path to the surface, thus forming a protective oxide layer, indicating that rolling improves corrosion resistance. If corrosion resistance is approached from the perspective of grain size, rolling results in many fine recrystallised grains, providing more grain boundaries. These grain boundaries are more chemically active and, thus, more susceptible to corrosion, reducing the stability of the passive film.

Xu et al. reached the following three conclusions related to corrosion:

σ phase precipitation: The precipitation of the σ phase significantly deteriorates corrosion resistance by creating chromium-depleted zones near the grain boundaries.

Residual stress: Residual stress and dislocations reduce the corrosion rate by increasing the stability of the oxide layer.

Grain boundaries: Fine grains provide more grain boundaries, which are more susceptible to corrosion, thus reducing the stability of the passive film.

SUMMARY

In this two-part review paper, we have presented the diverse nature of corrosion, particularly emphasising the effects of steel formability and surface roughness. Corrosion resistance is typically determined based on chemical composition alone, often neglecting steel's formability, surface roughness, and other manufacturing-related factors.

Our literature review included numerous environmental factors contributing to corrosion, such as material composition, electrochemical potential, surface roughness, stress and deformation, and temperature. The case studies we presented highlighted that rougher surfaces increase the risk of corrosion (Wang et al.) and that the formability of steel (Xu et al.) plays a key role in corrosion resistance.

The results of the case studies discussed in this review emphasise the importance of considering steel formability and surface roughness when evaluating corrosion resistance. Future research should develop more comprehensive testing methods that include these factors, ensuring that when selecting materials for safety-critical applications involving stainless components, not only the chemical composition but also the surface quality, manufacturing technology, and usage environment are considered.

REFERENCES

[1] M. D. Giuseppe, Localized corrosion of stainless steels: effect of surface finishing, Milano: Politecnico Milano, 2018.

[2] F. Haraszti, L. Trif, Z. May, K. T. és J. Telegdi, „Chemical background of contact corrosion between copper and galvanized steel screws," *International Journal of Corrosion and Scale Inhibition*, vol. 11, no. 4, pp. 1418-1434, 2022.

[3] F. Haraszti, „Hőkamera alkalmazása kontaktkorrózió vizsgálatára," *Műszaki Tudományos Közlemények*, vol. 11, no. 1, pp. 77-80, 2019.

[4] F. Haraszti és T. A. Kovács, „Galvanic Corrosion Occurs Heat Experiments by Thermographic Camera," *Journal of Physics Conference Series*, vol. 1045, no. 1, p. 012016, 2018.

[5] L. Tóth, F. Haraszti és T. Kovács, „Surface Roughness Effect in the Case of Welded Stainless Steel Corrosion Resistance," *Acta Materialia Transylvanica*, vol. 1, no. 1, pp. 53-56, 2018.

[6] L. Tóth, F. Haraszti és T. Kovács, „Heat Treatment Effect for Stainless Steel Corrosionresistance," *European Journal of Materials Science and Engineering*, vol. 3, no. 2, pp. 38-42, 2018.

[7] H. Alzyod, J. Takács és P. Ficzere, „Improving surface smoothness in FDM parts through ironing post-processing," *Journal of Reinforced Plastics and Composites*, vol. 43, no. 4, pp. 1-11, 2023.

[8] G. Kónya és P. Ficzere, „The Effect of Layer Thickness and Orientation of the Workpiece on the Micro- and Macrogeometric Properties and the Machining Time of the Part during 3D Printing," *Periodica Polytechnica Mechanical Engineering*, vol. 67, no. 2, pp. 143-150, 2023.

[9] T. A. Kovács, Z. Nyikes és V. Ghica, „The analysis of microstructural changes depending on the electro-acoustic effect under the ultrasonic welding process of

aluminum foils," *UPB Scientific Bulletin, Series B: Chemistry and Materials Science*, vol. 821, no. 4, pp. 213-222, 2021.

[10] C. Hetyei és R. Nagy, „Review of Wind Turbine Failures, Highlighting Fire Accidents," *Műszaki Katonai Közlöny*, vol. 30, no. 2, pp. 43-56, 2021.

[11] L. Tóth, E. Fábián, Z. Nyikes, I. Perianu és T. A. Kovács, „Effect of Surface Coatings on the Service Life of Unimax Casting Tool Steel," *Advance Engineering Forum*, vol. 53, no. 13, pp. 11-18, 2024.

[12] H. Xu, T. Tian, B. Hua, W. Zhan, L. Niu, B. Han és Q. Zhang, „Effect of in-situ rolling and heat treatment on microstructure, mechanical and corrosion properties of wire-arc additively manufactured 316L stainless steel," *Journal of Materials Research and Technology*, vol. 27, no. 6, pp. 3349-3361, 2026.

[13] E. Fábián, L. Tóth és C. Huszák, „Examination of Heat Treatment on the Microstructure and Wear of Tool Steels," *Acta Materialia Transylvanica*, vol. 2, no. 2, pp. 87-92, 2019.

[14] C. Hetyei és F. Szlivka, „Review of the Aerodynamical Load on a Dual-Rotor Wind Turbine's Blade," *Biztonságtudományi Szemle*, vol. 3, no. 1, pp. 91-108, 2021.

[15] R. Sánta, M. Bošnjaković és A. Čikić, „Experimental and Numerical Testing of Heat Pump Evaporator," *Applied Sciences*, vol. 12, no. 23, p. 11973, 2022.

[16] Hilti, Corrosion Handbook, 2015.

[17] P. A. Schweitzer, Fundamentals of Metallic Corrosion - Atmospheric and Media Corrosion of Metal, Boca Raton: CRC Press, 2007.

DOI: https://doi.org/10.12700/btsz.2025.7.2.105

PROCESSING INFORMATION SECURITY REQUIREMENTS FOR IT SYSTEMS USING RAG-SUPPORTED LLM

IT RENDSZEREKKEL KAPCSOLATOS INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK FELDOLGOZÁSA RAG TÁMOGATOTT LLM SEGÍTSÉGÉVEL

FEHÉR Dávid János[1]

Abstract

Managing information security requirements during IT system design poses significant challenges, as organizations must comply not only with international standards such as NIST 800-53 and ISO 27001:2022 but also with their internal regulations. Large Language Models (LLMs), particularly with support from Retrieval Augmented Generation (RAG), offer new possibilities for more efficient processing of these requirements. This publication highlights how LLMs provide real-time access to relevant information, reducing the time spent on manual research. While LLMs offer numerous benefits, their use also entails risks, such as potential misinterpretations. The research sheds light on key aspects of designing LLM-based systems and underscores the importance of human expertise in enhancing the efficiency and accuracy of managing information security compliance.

Keywords

Information security, LLM, RAG, Security compliance, Security control

Absztrakt

Az információbiztonsági követelmények kezelése az IT-rendszerek tervezése során komoly kihívást jelent, mivel a szervezeteknek nemcsak a nemzetközi szabványoknak, mint a NIST 800-53 és az ISO 27001:2022, hanem belső szabályzataiknak is meg kell felelniük. A nagy nyelvi modellek (Large Language Modell – LLM), különösen az adatlekérésre alapozott generálás (Retrieval Augmented Generation - RAG) támogatással, új lehetőségeket teremtenek a követelmények hatékonyabb feldolgozásában. A publikáció bemutatja, hogyan biztosítanak az LLM-ek valós idejű hozzáférést a releváns információkhoz, csökkentve a manuális kutatásra fordított időt. Az LLM-ek rengeteg pozitív lehetőséget rejtenek, de használatuk kockázatokat is rejt, például félreértelmezéseket. A kutatás rávilágít az LLM rendszerek tervezésének főbb pontjaira és az emberi szakértelem fontosságára, amely hatékonyabbá és pontosabbá teszi az információbiztonsági megfelelőség kezelését.

Kulcsszavak

Információbiztonság, Nagy nyelvi modell, Adatlekérésre alapozott generálás, Biztonsági megfelelőség, Biztonsági kontroll

[1] david.janos.feher@gmail.com| ORCID: 0000-0002-0742-8996 | PhD student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

IT vállalatok komplex környezetben komplex IT megoldásokat használnak. Ezen IT-megoldások tervezésében a rendszertervezők és mérnökök kulcsszerepet játszanak a megfelelőségi kontrollok technikai infrastruktúrákba történő beépítésében. Felelősségeik közé tartozik annak biztosítása, hogy az általuk választott, tervezett, kivitelezett, üzemeltetett és használt rendszerarchitektúrák, adatkezelési folyamatok, biztonsági protokollok és egyéb részletek összhangban legyenek a szervezet számára fontos szabványokkal, mint például a NIST 800-53 és az ISO 27001:2022 szabványokkal, de a kezelt adat és piaci terület függvényében területenként más és más követelménynek kell megfelelniük. A nemzetközi szabványokon kívül a szervezet saját működési módját, struktúráját és saját belső szabályzatait is figyelembe kell venni. Ezen követelmények nagy mértékben változhatnak a nemzetközi szabványok változása, szervezeti változások és rengeteg más egyéb esetben is, mind ezen információkkal naprakésznek lenni, minden dokumentumot elolvasni és észben tartani nagy terhet ró a szakemberekre. [1], [2], [3]

A mesterséges intelligencia azon belül is a nagy nyelvi modellek (Large Language Models - LLM) térnyerésével rengeteg területen próbálják ennek előnyeit használni, ide tartozik az információbiztonsági terület is. Az LLM jelentős potenciált rejt az információbiztonság területén lévő rengeteg követelményeket vagy ajánlásokat tartalmazó dokumentáció hatékonyabb feldolgozásához. Az LLM-ek még hatékonyabbak a Retrieval Augmented Generation (RAG) azaz visszakereséssel támogatott generálással kiegészítve, ez lehetővé teszi, hogy dokumentumokkal és egyéb fix információkkal még biztosabb válaszokat adjon a modell, sok esetben “grounding”-ként hivatkoznak erre. A mesterséges intelligencia területén a grounding azt jelenti, hogy egy modell vagy rendszer az általa használt információt külső valósnak vélt adatokhoz kapcsolja, így biztosítva, hogy a generált válaszok pontosak és relevánsak legyenek. Ezen cikkben az információbiztonsági követelményekhez való hatékonyabb LLM-mel támogatott hozzáférés lehetőségét mutatom be. A követelmények könnyen hozzáférhetővé tétele nemcsak a hatékonyságot növeli, hanem ezen felül csökkentheti az esetleges félreértéseket és a mulasztások valószínűségét is a fejlesztési folyamat során.[4], [5], [6], [7]

LLM KÖVETELMÉNYEKET TARTALMAZÓ TUDÁSBÁZISHOZ

A kisebb és nagyobb IT-megoldások, platformok, folyamatok tervezésében és kivitelezésében kiemelten fontos a megfelelőségi szabványok szemelőt tartása, figyelembevétele, és lehetőség szerint a betartása. Ahhoz, hogy a rendszerek körülötti folyamatokba bevont IT-rendszertervezők, mérnökök, szakemberek meg tudjanak felelni ezen követelményeknek pontos és naprakész általuk feldolgozott és megértett információra van szükség. [1]

A technikai csapatok gyakran szembesülnek összetett megfelelőségi követelménynyel kapcsolatos kérdésekkel a rendszerek tervezési fázisa során. Mint például, hogy milyen követelményeknek kell megfelelnie a rendszerekben használt jelszavaknak. Mit és hogyan kell titkosítani, hogyan tudják biztosítani a megfelelő naplózását a rendszernek. Az LLM-ek részletes, kontextus függő válaszokat nyújthatnak ezekre a kérdésekre, kiterjedt tréningadataikból merítve az adott szervezeti környezetre szabott útmutatást. A nagy nyelvimodel-

lek ebben lehetnek segítségünkre, hiszen segítségükkel gyorsan lehet megválaszolni a technikai kérdéseket, ezzel valós idejű hozzáférést biztosítva a kontrollkövetelményekhez, annak leírásaihoz. [1], [8]

Az LLM-ek és az RAG szerepe a kontrollkövetelmények hatékony lekérdezésében

A ChatGPT és a Gemini, mint az AI ökoszisztéma szerves híres részei a "GenAI" azaz generatív mesterséges intelligencia jól ismert példái, amelyek LLM-ek azaz nagy nyelvi modellek nyelvfeldolgozási képességeiket kihasználva képesek „megérteni" a kontextust és emberihez hasonló szövegeket generálni, valamint összetett feladatokban, például szövegírásban és akár kontrolkövetelmények feldolgozásában is segíteni. A legnagyobb LLM-ek, nagyon kiterjedt korpuszon vannak tanítva, amely tartalmaz rengeteg az interneten elérhető forrást ebbe beleértve a legismertebb szabványokat is mint például a NIST 800-53 és az ISO 27001. Elmondható, hogy a ChatGPT és a Gemini mind a kettő kifejezetten jó válaszokat ad komplex kérdésekre, beleértve az információbiztonsággal kapcsolatos kérdésekre. Ezen tényezők lehetővé teszik, hogy azonnali, az LLM számára elérhetővé tett kontextus függvényében válaszokat adjanak információbiztonsági megfelelőséggel kapcsolatos kérdésekre. Például, ha egy szakember a NIST 800-53 egy adott kontrolljának implementálásához keres útmutatást, akkor az LLM alapú generatív mesterséges intelligencia rendszerek képesek használható magyarázatot, megvalósítási lépéseket és egyéb információkat nyújtani. Az egyik fő problémája az LLM modelleknek az, hogy félrevezető vagy hibás választ is adhat, de ezen probléma megoldására való a „grounding", amely fogalomhoz tartozik az RAG architektúra. A rendszer rövid válaszideje óriási segítség abban, hogy a tervezési döntésekhez vagy egyéb döntésekhez szükséges információk vagy ajánlások sokkal elérhetőbbek legyenek. A közel azonnali információhoz való hozzáférés révén csökken a komplex dokumentációk és leírások keresésével, olvasásával, értelmezésével töltött idő. Ez nem csak azt jelenti, hogy kevesebb időt töltenek ezzel az emberek, hanem hogy a kényelmes lekérdezésnek hála hamarabb fognak utána járni a dolgoknak. [1], [3], [6], [9]

TERVEZÉS ÉS MEGVALÓSÍTÁS EGYSZERŰSÍTÉSE LLM-EKKEL

A különböző informatikai rendszerek és platformok tervezésének előkészítése, tervezése, kivitelezése minden szervezet esetén és minden rendszer esetén valamennyire eltér, nagyban függ a szervezettől, a személyzettől és a tervezendő rendszertől. A fejezetben egy általános megoldást kivitelezését mutatom be, amelynek fő elemei könnyen átemelhetőek az igények szerint. Az alábbi példák szemléltetik milyen típusú kérdésekre kereshetünk válaszokat a megoldással:

- Milyen titkosítás használható ügyféladatok kezelésére?
- Milyen titkosítás használható személyes adatok kezelésére?
- Milyen követelményeknek kell megfelelni a jelszavak adásánál? Hány karakter hosszúnak kell minimum lennie, hogy megfeleljek a szervezet követelményeinek?
- Hogyan kell kezelni a szerverek a helyi adminisztratív felhasználójának jelszavát? Milyen sűrűn cserélendők ezeken a jelszavak?
- Milyen naplófájlokat kell gyűjteni és továbbítani? Hogyan?

Főbb lépések az LLM-ek folyamatokba történő integrálásához.

Minden szervezet esetén más az egyes lépéseknek a prioritása és a részletei és nagy mértékben függ az integrálás magától a folyamattól is, hiszen nem mindegy, hogy egy kisebb belső használatra szánt informatikai megoldásról beszélünk, vagy pedig egy igazán összetett szervezeti részlegeken átívelő komplex megoldásokat. Fontos azt is szem előtt tartani, hogy mely esetekben érdemes a folyamatot automatizálással támogatni, hiszen vannak annyira egyedi egyszeri esetek, amelyeket nem érdemes automatizálni. Ezen részletektől eltekintve általánosan az alábbi főbb lépéseket érdemes elvégezni az integráláshoz:[9], [10], [11]

1. **Megfelelő csapatok és szakemberek bevonása:** Az egyik legfontosabb lépés a szervezeten belüli megfelelő szakemberek megtalálása, hiszen a folyamat során rengeteg a szervezet meglévő információbiztonsági követelményeivel kapcsolatos kérdés merül fel. Érdemes bevonni mindenkit, kiemelten azokat, akik korábban kiemelt szerepet töltöttek be a hasonló kérdések megválaszolásában.[12], [13]
2. **Megfelelőségi követelmények és célok meghatározása:** Először egyértelműen körvonalazzuk az elemzés célját, minek akarunk megfelelni, mint például NIST 800-53 vagy az ISO 27001:2022 szabvány megfelelés, belső információbiztonsági követelményeknek való megfelelés, azon belül is tisztázni, hogy a konkrét részleg, vagy szervezet különböző követelményei miként milyen átfedéssel és prioritással van szemelőt tartva. Itt külön érdemes dokumentálni, amennyiben nem egységes a megfelelési követelmény a teljes szervezetben, hanem eltér megoldásonként vagy csapatonként. [12], [13]
3. **Megfelelőségi követelményekkel kapcsolatos dokumentációk gyűjtése:** Fontos minél korábban elkezdeni összegyűjteni, a megfelelőséggel kapcsolatban elérhető írott információkat és dokumentációkat. Amennyiben van dokumentáció, amely nem naprakész vagy hiányos vagy nem létezik, akkor annak a frissítését kezdeményezni kell vagy az eltéréseket dokumentálni.
4. **Megfelelő LLM-eszközök kiválasztása:** Olyan LLM mesterséges intelligencia modell és platformot válasszunk, amellyel meg tudunk felelni az általunk használni tervezett adatok és anyagok kezelésével kapcsolatos szervezeti adatbiztonsági követelményeinknek. A legnagyobb felhő szolgáltató cégek platformjain valószínűleg megtaláljuk a szükséges szolgáltatásokat, a kutatásban leírtak tesztelése és validálása során a Google Cloud Platform (GCP) Vertex AI nevű AI platform volt használva. AWS és Azure Cloud esetén is rendelkezésre állnak jelenleg a szükséges komponensek. [7], [14], [15]
5. **Megfelelőségi követelményekkel kapcsolatos írott anyagok biztosítása:** A rendszer csak a leírt adatokat tudja feldolgozni és figyelembe venni, abban az esetben, ha valamire nincs írott dokumentációnk, de szükségünk van az információ figyelembevételére, akkor gondoskodni kell ennek az információnak a leírásáról. Amennyiben van rá lehetőség akkor ezen dokumentumokat érdemes rendszerezni és átnézni, hogy csak a valóban naprakész szabályzatok és részletek benne. Átfedés esetén priorizálni kell a dokumentumokat, például amennyiben van egy részlegszerinti követelmény, amely szigorúbb, mint a szervezet követelménye. A modern LLM modellek nagy token száma, ami azt jelenti, hogy nagy mennyiségű szöveg

feldolgozására alkalmas, így ezeket kategóriákként össze lehet vetni, és ajánlásokat létrehozni a feltöltött dokumentumok kapcsán. [12], [13]

6. **RAG elő-feldolgozás:** Az összegyűjtött dokumentumok validálása után egy "embedding model" azaz beágyazási modell segítségével átalakítjuk. A beágyazási modellt esetünkben arra használjuk, hogy szövegeink feldarabolása után abból numerikus reprezentációkat hozzunk létre, így a szövegünk hatékonyan feldolgozhatók és összehasonlíthatók machine learning (gépi tanulási) modellekben. Ezen átalakítás után létrejött adatunkat egy vektor adatbázisban tároljuk. [7], [14], [15]
7. **LLM alapú információfeldolgozás:** Lehetőségünk van az LLM megoldások segítségével is feldolgozni az adatainkat bizonyos szempontból, ezzel plusz mélységet adva a feldolgozott vektor adatainknak, akár metaadatként, akár egyéb kiegészítő információként.
8. **Egyéb információ források integrálása:** Lehetőségünk van más egyéb információ forrásokat, egyéb forrásokat is tartalmazó adatbázisokat és API alapú információ forrásokat integrálni.[16]
9. **Állandó promptok kidolgozása:** Az állandó promptok továbbra is fontosok, hiszen ezen rendszerek rengetett állandó változóként megadott promptot tartalmaz. Ezen fix promptok szerves részét képezik az adatfeldolgozásnak és a különböző integrációknak. Amennyiben egy felhasználó interakciót kezdeményez az LLM alapú megoldásunk felé az jelen esetünkben egy promptal indul, amely még kiegészítésre kerül a vektor adatbázisban tárolt releváns információval és más egyéb integrált információforrástól származó információval. Fontos, hogy nincs tökéletes prompt, és nincs tökéletes képlet hozzájuk, mivel ez nagyban függ a feldolgozott adattól és az egyéb tényezőktől. Érdemes az aktuális ajánlásokat átnézni és sokat tesztelni, kísérletezni a promptokkal, hogy megtaláljuk a mi igényeinknek és környezetünknek a leginkább megfelelőt.[17]
10. **RAG támogatott LLM alapú Chatbot publikálása:** Az RAG támogatott LLM alapú chatbot-ot a megfelelő tesztelés és felhasználói oktatás után megnyitásra kerül a felhasználók részére. A tesztelés során vagy akár már a publikálás után érkező felhasználói visszajelzések alapján finomhangolást iteratív jelleggel rendszeresen el kell végezni. [18]
11. **RAG támogatott LLM alapú Chatbot integrálása a munkafolyamatokba:** Amennyiben elfogadható válaszokat ad a chatbot, akkor átfogóan át kell tekinteni, hogy mely területeken érdemes először aktívan integrálni. Itt érdemes figyelembe venni azt, hogy mely csapatoknál használható leginkább a megoldás és hogy mely csapatoktól érkezhetnek hasznos visszajelzések, ideértve azokat, akik valamilyen módon találkoztak már információbiztonsági követelményekkel, vagy kellett volna már találkozniuk. Az információbiztonsági szakemberek különösen nagy segítség tudnak lenni, hiszen ők a tapasztalatukból adódóan releváns visszajelzést tudnak adni. A felmérés és a bevezetés során fontos a vezetői támogatás és érdemes lehet projekt menedzserek segítségével végezni ezen bevezetést. Fontos felkészíteni a felhasználókat a rendszer esetleges hibáira és informálni őket a problémák bejelentésére és visszajelzésére szolgáló kommunikációs csatornákról és annak használatáról. [12], [13], [18]

12. **Folyamatos naprakészen tartás, folyamatos fejlesztés:** Mivel a szervezettel vagy részleggel szemben érvényes követelmények szignifikánsan változhatnak, ezeknek dokumentáció oldalról is változásként kell megjelenniük, amelynek pedig a vektor adatbázisban történő változásnak kell lekövetnie. A rendszerből adódóan folyamatosan változni fog a mögötte lévő dokumentum rendszer, így folyamatos finomhangolásra és fejlesztésre van szükség a rendszer esetén. Ezen változások kezelésére megfelelő folyamatokat kell létrehozni. [12], [13], [18]

AZ RAG TÁMOGATOTT LLM-ALAPÚ MEGFELELŐSÉG ELŐNYEI ÉS KOCKÁZATAI

Ezen RAG támogatott LLM megoldás működéséből adódóan rengeteg szervezeti információval dolgozik, a publikációban ennek kockázatait nem tárom fel, hiszen nagyon eltérő módon állnak a szervezetek a nagyon eltérő szinten bíznak meg a LLM modellekben és a mögöttük álló cégekben adatbiztonsági szempontból. A bemutatott megoldás kivitelezhető a szervezet által üzemeltetett AI modellek segítségével is, de ennek komplexitása miatt ennek részleteit nem taglalja a publikáció. [12], [13], [18]

Lehetséges előnyök

Az RAG támogatott LLM a különböző IT rendszereket érintő folyamatokba történő integrálása számos előnyt kínál, :

- **Gyorsabb információbiztonsági folyamatok:** Az LLM-ek azonnali hozzáférést biztosítanak az információbiztonsági követelményeket érintő információkhoz, csökkentve a manuális kutatásra vagy más a követelményeket ismerő emberekre várással töltött időt, ezzel felgyorsítva és leegyszerűsítve a követelmények tisztázását.[7], [9], [19]
- **Konzisztens naprakész információ forrás:** Az egységes és felügyelt információs háttér miatt RAG támogatott LLM-ek közel valós időben tudnak reagálni a dokumentált követelményekben történő változásokra és tudják biztosítani az információbiztonsági követelmények és kontrollok konzisztens, egységes alkalmazhatóságát különböző projektekben, minimalizálva az információ terjedéséből adódó késések okozta eltéréseket. [7], [9], [19]
- **Csökkenő emberi erőforrás igény**: Az automatizálás miatt csökken az információbiztonsági szakemberek által manuálisan elvégzett munka, csökken a hozzájuk érkező információbiztonsági szabályzattal kapcsolatos kérdések száma vagy komplexiása.
- **Könnyű hozzáférhetőség:** Az RAG támogatott LLM-ek könnyen hozzáférhetőek, időzóna vagy munkaidő korlátok nélkül. Lehetővé téve a 24/7 történő kérdések feltételét, így a felhasználók számára is sokkal kézenfekvőbb és kényelmesebb lesz ezt használni, ezzel csökkenthető az információbiztonsági szakemberek felé történő kitettség. [7], [9], [19]

Lehetséges kockázatok

Az előnyök ellenére az RAG támogatott LLM-ekre való túlzott támaszkodás kockázatokkal járhat, amely szervezetenként más súllyal jelentkezik, és szervezetenként eltérő módon lehet ezekre reagálni:[20]

- **Lehetséges félreértelmezések:** Az RAG támogatott LLM-ek megfelelő ellenőrzési visszacsatolási mechanizmusok nélkül vagy nem megfelelően széleskörűen dokumentált környezet esetén félreértelmezhetik az összetett megfelelőségi kontextusokat vagy a felhasználó által használt szakkifejezéseket. [21]
- **Pontatlanságok bonyolult helyzetekben:** Bonyolult információbiztonsági követelményekkel kapcsolatos szituációkban az LLM-ek visszacsatolási mechanizmusok nélkül egyszerűsített vagy hibás tanácsokat adhatnak, ami szakértői beavatkozást igényelhet.[6], [21]
- **A kontextuális árnyalatok hiánya:** Az LLM-ek nem mindig képesek teljes mértékben megérteni a szervezeti sajátosságokat, amennyiben nem megfelelően vannak azok dokumentálva, így előfordulhat, hogy az ajánlásaik nem teljesen illeszkednek az adott vállalat valóságához. [6], [21]

Javaslatok a kockázatok csökkentésére

Az RAG támogatott LLM-ek pontosságával és részletességével kapcsolatban szervezetenként eltérő az igény. Egy alap RAG támogatott LLM chatbot összeállítása publikus felhőben elérhető menedzselt komponensekből igényel nagy emberi erőforrást, viszont a rendszer finomhangolása és a különböző ellenőrző folyamat megtervezése és egyéb kiegészítő információforrás integrálása már több erőforrást igényel. Fontos megtalálni a szervezet méretének és igényeinek megfelelő optimális állapotot. Az RAG támogatott LLM-ek használatának optimalizálása és a kapcsolódó kockázatok mérséklése érdekében az alábbi ajánlásokat érdemes követni: [6], [21]

- **Felhasználók oktatása, felhasználói tananyag:** Az oktatás segítségével elősegíthető, hogy a végfelhasználók optimálisabban tudják használni a rendszert és annak előnyeit. Kiemelten fontos, hogy a végfelhasználók megfelelő kritikával állnak a rendszer válaszaival szemben. Ezen felül fontos, hogy a felhasználók megfelelő promptokat használjanak, így arra érdemes külön kitérni az oktatások során. Megfelelő használati utasítás létrehozása és közzététele szintén nagy segítség az átlag felhasználónak.[19], [21]
- **LLM alapú ellenőrzési visszacsatolás:** Különböző pontjain a rendszernek visszacsatolási pontokat hozhatunk létre, amely a bemenetet, az integrált forrásokat és a kimenetet is validálhatja.
- **Automatizált válasz minőség ellenőrzés:** LLM megoldások és egyéb adattudományi megoldások segítségével lehet elemezni a válaszokat és azoknak minőségét a kérdés függvényében.
- **Folyamatos visszacsatolási folyamat:** Folyamat létrehozása, amely hatékonyan kezeli végfelhasználók és szakértők visszajelzésének feljegyzését és azok alapján hatékonyan kezelhető és menedzselhető finomhangolások létrehozását. [22]
- **Szakértői felülvizsgálat:** Az információbiztonsági szakértők ellenőrizhetik véletlenszerűen proaktív módon vagy reaktív módon a felhasználói visszajelzésekre vagy az automatizált minőségellenőrző folyamatok kimenetelei alapján.[22]

Metrikák a hatékonyság értékelésére

Szervezetenként és integrációs típusonként eltérő, hogy mely metrika milyen fontossággal jelenik meg a szervezet számára, főbb metrikák a teljesség igénye nélkül:

- **Válaszidő:** Az általános felhasználói elégedettség miatt is kiemelten fontos a válaszidő, hiszen amennyiben túl lassú a rendszer, akkor az felhasználói frusztrációt és ellenállást okozhat. Ezen felül amennyiben más rendszerekkel van integrálva a rendszer hibákat és egyéb problémákat okozhat a túl nagy válaszidő.[23], [24]
- **Relevancia:** Az LLM kimeneteinek a kérdéssel szemben való relevancia értékelése. Ez az ellenőrzés történhet automatizált módon egy másik LLM segítségével és ezen felül a felhasználó által. [21], [23], [24]
- **Hibaarányok:** Az LLM által generált tartalomban előfordulhatnak hibák, itt figyelhetjük a hibák gyakoriságát és típusait. Ez lehet túl rövid válasz, vagy hibaüzenet is, például egy szolgáltatás kiesés miatt vagy egyes komponensek hibája miatt. [21], [23], [24]
- **Követelménnyel szemben való illeszkedés:** LLM kimenetének vizsgálata, hogy mennyire felel meg a releváns megfelelőségi szabványoknak és előírásoknak. Ez az ellenőrzés történhet automatizált módon egy másik LLM segítségével és ezen felül a felhasználó által. [21], [23], [24]

Finomhangolási lehetőségek

Az RAG támogatott LLM-ek rengeteg mozgó paraméterrel és elemmel rendelkeznek, amiknek finomhangolása szükséges a megfelelő működés elérése érdekében, ez közé tartoznak az alábbi pontok:

- **Dokumentumok optimalizálása:** Amennyiben nem megfelelő szervezeti dokumentáció alapján dolgozunk, az problémát okozhat, így fontos a megfelelő lefedettsége a szervezet valóságának. Amennyiben átfednek a dokumentumainkban lefedett információk, de ezek szükségesek, akkor ezen dokumentumok között prioritási sorrendet érdemes megadni. [21], [23], [24]
- **Egyéb integrációk optimalizálása**: Meglévő integrációk felülvizsgálata és esetleges egyéb integrációs források felderítése, amennyiben még több kontextusra van szükségünk.[18]
- **Fix prompt finomhangolás:** A rendszernek szerves része a különböző fix promptok, így ezek finomhangolása és módosítása több iterációt igényelhet, ez nagy mértékben változhat amennyiben más paraméterek változnak. [25], [26]
- **Paraméter beállítás:** A rendszer több pontján is különböző paraméterek használ, az LLM kimeneteinek megfelelő befolyásolása érdekében. Ezen paraméterek lehetnek például hosszúságot, összetettséget, kreativitást, formátumot és hangnemet meghatározó elemek, hogy biztosítsuk a következetességet és az illeszkedést az elvárásainkkal szemben.[23], [25]

KÖVETKEZTETÉS

Az RAG támogatott nagy nyelvi modellek (LLM-ek) bevezetése és alkalmazása az információbiztonsági követelmények feldolgozásában jelentős előrelépést jelenthet az IT-rendszerek tervezési és kivitelezési folyamataiban. Az LLM-ek képességei lehetővé teszik a gyors és konzisztens információhozzáférést, amely kulcsfontosságú a komplex megfelelőségi követelmények betartásához. Ezek az eszközök nemcsak a tervezési ciklusok gyor-

sításában játszanak szerepet, hanem az egységes információforrás biztosításával a követelmények pontosabb értelmezését és alkalmazását is elősegítik. Az azonnali válaszok révén az LLM-ek hozzájárulnak a tervezési és fejlesztési folyamat hatékonyságának növeléséhez, ugyanakkor csökkentik a mulasztásokból eredő hibák valószínűségét.

Mindezek ellenére az RAG támogatott LLM-ek használata nem mentes a kockázatoktól. Az összetett információbiztonsági kontextusok félreértelmezésének lehetősége, a pontatlan válaszok kockázata és a szervezeti sajátosságok nem megfelelő figyelembevétele mind olyan tényezők, amelyek komoly kihívást jelenthetnek a rendszer sikeres alkalmazásában. Az ilyen típusú rendszerek akkor működnek hatékonyan, ha megfelelő visszacsatolási mechanizmusokkal, szakértői felügyelettel és folyamatos finomhangolással egészítik ki azokat.

A dokumentumok rendszerezett kezelése és naprakészen tartása, az LLM-ek paramétereinek folyamatos optimalizálása, valamint a felhasználók megfelelő oktatása elengedhetetlen elemei a sikeres implementációnak. Az LLM-ek alapvető képességei a releváns tartalom generálására és az információbiztonsági követelmények értelmezésére számos gyakorlati előnnyel járnak, azonban az emberi kontroll és kritikus gondolkodás továbbra is nélkülözhetetlen marad.

A kutatás során bemutatott megközelítés világosan rávilágít arra, hogy az LLM-ek alkalmazása nem csupán a megfelelőségi követelmények feldolgozását, hanem azok szervezeti környezethez való igazítását is jelentősen megkönnyítheti. Az olyan technológiák, mint az RAG támogatott LLM-ek, lehetőséget teremtenek az információs struktúrák hatékonyabb kezelésére, miközben csökkentik a manuális erőforrásigényt és a hibák valószínűségét. Az RAG támogatott LLM-ek szerepe az információbiztonsági megfelelőségkezelésben folyamatosan bővülni fog, ahogyan ezek az eszközök tovább fejlődnek és még elérhetőbbek lesznek. Az automatizált megoldások és az emberi szakértelem együttes alkalmazásával a szervezetek képesek lesznek hatékonyabb biztonsági szintet fenntartani, miközben hatékonyabbá teszik az informatikai rendszerek tervezését, üzemeltetését érintő folyamataikat. A technológia adta lehetőségek kiaknázása ugyanakkor csak akkor lesz sikeres, ha azt átgondolt és alaposan megtervezett folyamatokkal támogatják, amelyek figyelembe veszik a szervezet specifikus igényeit és kihívásait.

FELHASZNÁLT IRODALOM

[1] B. Kenyon, ‘Nine steps to success: an ISO 27001: 2022 implementation overview’, 2024.
[2] P. Nurmi, ‘Enhancing ISO 27001: 2022 Implementation Through Project Management’, 2024.
[3] Y. Kurii and I. Opirskyy, ‘Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013’, *NIST Spec Publ*, vol. 800, no. 53, p. 10, 2022.
[4] R. Islam and I. Ahmed, ‘Gemini-the most powerful LLM: Myth or Truth’, presented at the 2024 5th Information Communication Technologies Conference (ICTC), IEEE, 2024, pp. 303–308.
[5] B. Chand and B. Patel, ‘RAG-based Chat Application using LLMs: A Case Study of Vikram Sarabhai Library IIM Ahmedabad’, 2024.

[6] ‘What is Retrieval-Augmented Generation (RAG)?’, Google Cloud. Accessed: Nov. 06, 2024. [Online]. Available: https://cloud.google.com/use-cases/retrieval-augmented-generation
[7] ‘RAG Engine overview | Generative AI on Vertex AI’, Google Cloud. Accessed: Nov. 06, 2024. [Online]. Available: https://cloud.google.com/vertex-ai/generative-ai/docs/rag-overview
[8] ‘Vertex AI with Gemini 1.5 Pro and Gemini 1.5 Flash’, Google Cloud. Accessed: Nov. 06, 2024. [Online]. Available: https://cloud.google.com/vertex-ai
[9] S. B. Islam, M. A. Rahman, K. Hossain, E. Hoque, S. Joty, and M. R. Parvez, ‘OPEN-RAG: Enhanced Retrieval-Augmented Reasoning with Open-Source Large Language Models’, *ArXiv Prepr. ArXiv241001782*, 2024.
[10] R. Sahu and M. Speretta, ‘Statistical Word Analysis to support the Semiautomatic Implementation of the NIST 800-53 Cybersecurity Framework’, 2024.
[11] ‘What is ISO 27001? – TechTarget Definition’. Accessed: May 20, 2023. [Online]. Available: https://www.techtarget.com/whatis/definition/ISO-27001
[12] D. Moskowitz and D. Nichols, *A Practitioner’s Guide to Adapting the NIST Cybersecurity Framework: Create, Protect, and Deliver Digital Business Value Series*. Tso, the Stationery Office, 2023. [Online]. Available: https://books.google.hu/books?id=wd2EzwEACAAJ
[13] C. Bartsch, *Information Security Based on ISO 27001 Strategies: A Leadership Introduction to Information Security*. Amazon Digital Services LLC - Kdp, 2023. [Online]. Available: https://books.google.hu/books?id=0shi0AEACAAJ
[14] ‘What is RAG? - Retrieval-Augmented Generation AI Explained - AWS’, Amazon Web Services, Inc. Accessed: Nov. 06, 2024. [Online]. Available: https://aws.amazon.com/what-is/retrieval-augmented-generation/
[15] HeidiSteen, ‘RAG and generative AI - Azure AI Search’. Accessed: Nov. 06, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/search/retrieval-augmented-generation-overview
[16] ‘RAG with databases on Google Cloud’, Google Cloud Blog. Accessed: Nov. 06, 2024. [Online]. Available: https://cloud.google.com/blog/products/ai-machine-learning/rag-with-databases-on-google-cloud
[17] G. Team *et al.*, ‘Gemini 1.5: Unlocking multimodal understanding across millions of tokens of context’, *ArXiv Prepr. ArXiv240305530*, 2024.
[18] ‘Build a RAG chatbot with GKE and Cloud Storage | Kubernetes Engine’, Google Cloud. Accessed: Nov. 06, 2024. [Online]. Available: https://cloud.google.com/kubernetes-engine/docs/tutorials/build-rag-chatbot
[19] M. Kulkarni, P. Tangarajan, K. Kim, and A. Trivedi, ‘Reinforcement Learning for Optimizing RAG for Domain Chatbots’, *ArXiv Prepr. ArXiv240106800*, 2024.
[20] B. Jonkhout, ‘Evaluating Large Language Models for Automated Cyber Security Analysis Processes’, 2024.
[21] Z. Ji, T. Yu, Y. Xu, N. Lee, E. Ishii, and P. Fung, ‘Towards mitigating LLM hallucination via self reflection’, presented at the Findings of the Association for Computational Linguistics: EMNLP 2023, 2023, pp. 1827–1843.

[22] J. Wei, Y. Yao, J.-F. Ton, H. Guo, A. Estornell, and Y. Liu, ‘Measuring and reducing llm hallucination without gold-standard answers via expertise-weighting’, *ArXiv Prepr. ArXiv240210412*, 2024.
[23] D. Banerjee, P. Singh, A. Avadhanam, and S. Srivastava, ‘Benchmarking LLM powered chatbots: methods and metrics’, *ArXiv Prepr. ArXiv230804624*, 2023.
[24] T. Hu and X.-H. Zhou, ‘Unveiling LLM Evaluation Focused on Metrics: Challenges and Solutions’, *ArXiv Prepr. ArXiv240409135*, 2024.
[25] L. Li, Y. Zhang, and L. Chen, ‘Prompt distillation for efficient llm-based recommendation’, presented at the Proceedings of the 32nd ACM International Conference on Information and Knowledge Management, 2023, pp. 1348–1357.
[26] J. Zamfirescu-Pereira, R. Y. Wong, B. Hartmann, and Q. Yang, ‘Why Johnny can’t prompt: how non-AI experts try (and fail) to design LLM prompts’, presented at the Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, 2023, pp. 1–21.

DOI: https://doi.org/10.12700/btsz.2025.7.2.117

WHITE-BOX MODELING AND ARTIFICIAL INTELLIGENCE-BASED OPTIMIZATION OF GROUND SOURCE HEAT PUMP SYSTEMS

TALAJSZONDÁS HŐSZIVATTYÚS RENDSZEREK FEHÉRDOBOZ MODELLEZÉSE ÉS MESTERSÉGES INTELLIGENCIA ALAPÚ OPTIMALIZÁLÁSA

ZÓNAI Viktor[1] – KOLLÁR Csaba[2] – SÁNTA Róbert[3]

Abstract

Artificial intelligence offers new opportunities to improve the efficiency of building services systems, particularly in optimizing the performance of heat pump systems. In our research, we present the theoretical and practical design of heat pump systems using a systems theory-based modeling approach. By applying machine learning, we refined the input–output models of heat pumps, thereby enhancing system control under varying load conditions. We describe the multiple degrees of freedom in heat pump systems that can be optimized using AI-based predictive models to increase the coefficient of performance (COP). Our study highlights the potential of AI-driven optimization in the design and operation of heat pump systems, contributing to more efficient decision-making and sustainable energy management.

Keywords

ground source heat pump, white-box modeling, artificial intelligence, input–output model, system optimization

Absztrakt

A mesterséges intelligencia új lehetőségeket kínál az épületgépészeti rendszerek hatékonyságának növelésére, különösen a hőszivattyús rendszerek teljesítményének optimalizálásában. Kutatásunkban bemutatjuk a hőszivattyús rendszerek elméleti és gyakorlati tervezését rendszerelméleti modellezés alkalmazásával. A gépi tanulás segítségével pontosítottuk a hőszivattyúk input-output modelljeit, ezáltal javítva a rendszer szabályozását változó terhelési körülmények között. Ismertetjük a hőszivattyús rendszer több szabadságfokát, amelyek mesterséges intelligencia alapú prediktív modellekkel optimalizálhatók a COP növelése érdekében. Tanulmányunk rávilágít az AI-alapú optimalizáció lehetőségére a hőszivattyús rendszerek tervezésében és üzemeltetésében, hozzájárulva a hatékonyabb döntéshozatalhoz és a fenntartható energiagazdálkodáshoz.

Kulcsszavak

talajszondás hőszivattyú, fehérdoboz modellezés, mesterséges intelligencia, input–output modell, rendszeroptimalizálás

[1] zonai.viktor@uni-obuda.hu | ORCID: 0009-0008-5415-8096 | PhD candidate, Doctoral School on Safety and Security Sciences, Óbuda University | PhD hallgató, Biztonságtudományi Doktori Iskola, Óbudai Egyetem

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

[3] santar@uniduna.hu | ORCID: 0000-0001-7559-2758 | associate professor, Department of Mechanical Engineering and Material Sciences, Institute of Engineering Sciences, University of Dunaújváros | egyetemi docens, Műszaki Intézet, Dunaújvárosi Egyetem

BEVEZETÉS

A megújuló energiaforrások közül a geotermikus energia kiemelkedő helyen áll a fűtési-hűtési szektor dekarbonizációjában, mert hozzájárul a fosszilis tüzelőanyagoktól való függés csökkentéséhez [1]. A talajszondás hőszivattyús rendszerek a geotermikus energia hasznosításának hatékony módját kínálják, mivel a földkéreg állandó hőmérsékletét hasznosítva ezek a rendszerek a leghatékonyabb fűtési-hűtési technológiák közé tartoznak [2]. Mivel a geotermikus hőszivattyúk a talajból nyerik a fűtési-hűtési energiát, működésük minimális közvetlen károsanyag-kibocsátással jár [3].

A geotermikus hőszivattyús rendszerek maximális kihasználásához nemcsak a megfelelő tervezés, hanem a hatékony üzemeltetés és szabályozás is fontos. A komplex rendszer optimális vezérlése azonban számos tényező együttes figyelembevételét igényli (pl. külső hőmérséklet, épület hőigénye, talajhőmérséklet dinamikája), ami hagyományos, statikus szabályozással nehezen valósítható meg teljeskörűen [4]. Ebben nyújtanak új lehetőségeket a mesterséges intelligencia (AI) alapú megoldások, különösen a gépi tanulás és a neurális hálózatok alkalmazása. Az AI-alapú vezérlő algoritmusok képesek megtanulni az optimális működést anélkül, hogy minden lehetséges szituációt előre explicit módon programozni kellene, mivel rengeteg paraméter összefüggéseit tudják felismerni és kezelésükre megtanított modellt alkotni [5]. Ennek köszönhetően a hőszivattyú vezérlése adaptívvá válik, azaz a rendszer valós időben alkalmazkodhat a változó környezeti feltételekhez és terhelési viszonyokhoz [6]. Ilyen intelligens vezérléssel növelhető a rendszer hatékonysága. Különböző kutatási eredmények szerint a neurális hálózatokra épülő, öntanuló szabályozás elkerüli a nem megfelelő beállításokat és folyamatosan optimalizálja a hőszivattyú működését, ami mérhető energiamegtakarítást és jobb hőkomfortot eredményez [7]. Az AI tehát új távlatokat nyit a hőszivattyús rendszerek irányításában – a hagyományos fix szabályozási görbék helyett intelligens, önfejlesztő algoritmusok veszik át az irányítást, amelyek a rendszer teljesítményét folyamatosan optimalizálják a változó igényekhez igazodva.

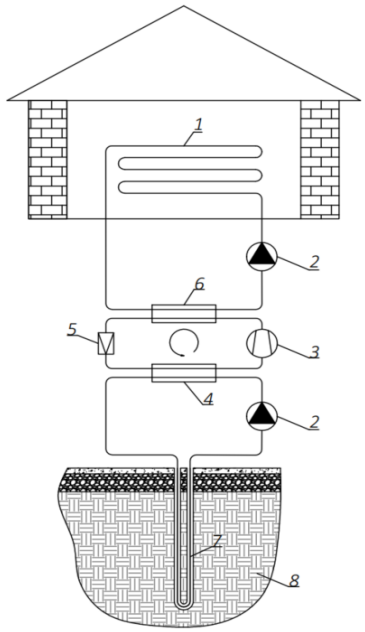
A meglévő rendszerek gyakran nem képesek hatékonyan reagálni a dinamikus környezeti és terhelési változásokra, mivel a hagyományos szabályozási megoldások csak korlátozottan adaptálhatók, és nem képesek előre jelezni a rendszer viselkedését. Az ilyen rendszerek érzékenyek lehetnek a nemlineáris hatásokra, valamint a külső és belső zavarokra, ez a működési hatékonyság csökkenéséhez vezethet és nőhet az energiafogyasztás. Mindezek alapján sürgető szükség mutatkozik olyan újfajta modellezési és vezérlési módszerekre, amelyek képesek a rendszer komplexitásának figyelembevételével dinamikusan alkalmazkodni a változó működési körülményekhez.

Jelen kutatás célja egy üzemelő talajszondás hőszivattyús rendszer input–output alapú fehér doboz modelljének felállítása, amely kiterjed a primer, hűtőközeg és szekunder oldalak termodinamikai jellemzésére. A modell célja, hogy pontosan leírja a rendszer energiaáramlási folyamatait és hatásfokát meghatározó összefüggéseket, valamint, hogy alapot biztosítson mesterséges intelligencia alapú optimalizáló algoritmusok integrálásához. A kutatás során a fizikai modellezést kiegészítve bemutatjuk, hogyan illeszthetők be AI-alapú szabályozási logikák a rendszer működésébe annak érdekében, hogy valós időben alkalmazkodni tudjon a változó környezeti feltételekhez és fogyasztói igényekhez.

HŐSZIVATTYÚS RENDSZEREK RENDSZERELMÉLETI MODELLEZÉSE

A hőszivattyúk működési elve

A kompresszoros hőszivattyúk a modern energiahatékony technológiák egyik kiemelkedő példáját jelentik. Ezen rendszerek képesek alacsony hőmérsékletű forrásokból, például a talajból, a külső levegőből, a felszíni és talajvízből, valamint geotermikus vizekből hőt kinyerni, majd azt magasabb hőmérsékleti szintre emelve hasznosítani. A működési elv alapja egy zárt körfolyamat, amely során egy speciális hűtőközeg közvetítésével zajlik a hőátadás [8]. Az elpárologtató és a kondenzátor meghatározó elemei a folyamatban, biztosítva a hőenergia felvételét és leadását. A talajszondás rendszerek esetében a hőcserélők a talajba telepített szondákon keresztül működnek, és attól függően, hogy a rendszer fűtési vagy hűtési üzemmódban működik, hőelvonást vagy hőleadást végeznek [2].



Jelmagyarázat:
1 – Fűtőkör
2 – Keringető szivattyú
3 - Kompresszor
4 - Elpárologtató
5 - Fojtószelep
6 – Kondenzátor
7 - Talajszonda
8 - Talaj

1. ábra: Talajszondás hőszivattyúk általános körfolyamata

A földkéreg belső hőmérséklete, amely a radioaktív bomlás révén folyamatos hőáramlást biztosít, az egyik legmegbízhatóbb energiaforrása ezeknek a rendszereknek [9]. A kezdeti rendszerek még kísérleti fázisban voltak, és hatékonyságuk korlátozott maradt. A technológia fejlődését jelentősen elősegítette a kompresszorok továbbfejlesztése, amely lehetővé tette a nagyobb hőmérséklet-különbségek áthidalását, ezáltal javítva a rendszer hatásfokát és szélesebb körű alkalmazhatóságát. Az energiaválság hatására az 1970-es és 1980-as években egyre nagyobb figyelem irányult a megújuló energiaforrásokra, így a geotermikus energiát hasznosító rendszerek fejlesztésére is [10]. Ebben az időszakban jelentős technológiai előrelépések történtek, többek között az energiaátadás hatékonyságának növelése és az energiafogyasztás csökkentése terén. A hőszivattyús rendszerek további fejlődése során a modern kompresszorok megjelenése új mérföldkövet jelentett, mivel ezek lehetővé tették a hőszivattyúk számára, hogy hatékonyabban használják ki a talaj stabil hőmérsékleti

adottságait [11]. Ezzel párhuzamosan az innovatív hőcserélő technológiák, a precíz szabályozási rendszerek és a fejlettebb hűtőközegek tovább növelték az energiahatékonyságot, így a talajszondás hőszivattyúk egyre szélesebb körben elterjedtek az épületenergetikai alkalmazásokban [12].

Magyarország földtani adottságai különösen kedvezőek a geotermikus energia hasznosítására, azonban a talajszondás hőszivattyúk elterjedése csak a 2000-es évek elején kezdett gyorsulni [13]. A technológia iránti növekvő érdeklődést az energiahatékonysági követelmények szigorodása, valamint az alternatív és megújuló energiaforrások iránti növekvő kereslet ösztönözte. A kormányzat által biztosított támogatások, az egyre szigorúbb energiatakarékossági előírások, valamint a fenntarthatóság melletti társadalmi elköteleződés szintén hozzájárultak a technológia térnyeréséhez [14]. A 2000-es évektől kezdve az energiaárak emelkedése és Magyarország Európai Unióhoz való csatlakozása, amely további ösztönzőt jelentett a hőszivattyús rendszerek elterjedésére. Az új épületek tervezésénél, illetve a meglévő épületek korszerűsítésénél egyre többen választják ezt a technológiát, mivel költséghatékony és környezetbarát alternatívát jelent a hagyományos fűtési és hűtési rendszerekkel szemben [15].

A talajszondás hőszivattyús rendszer input-output modellje

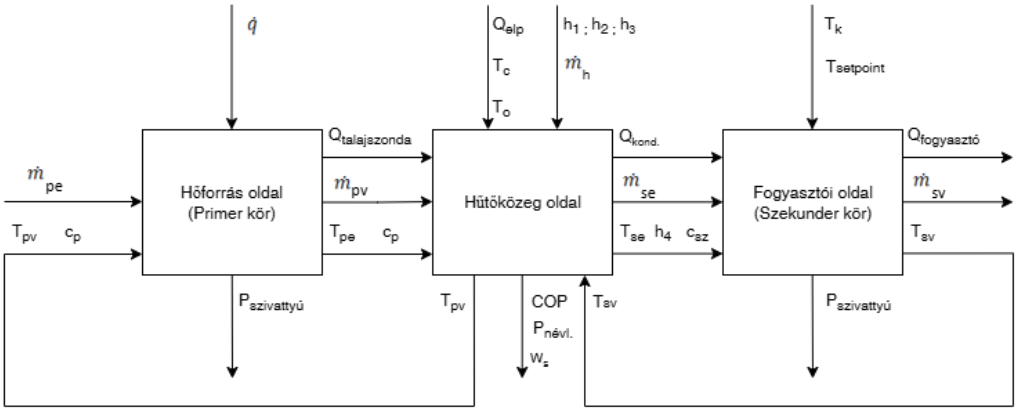
A hőszivattyús rendszerek működése egymással szoros kapcsolatban álló termodinamikai folyamatokon alapul. Ezek a folyamatok a hőforrásból történő hőkinyeréstől a hűtőközeg energiaátalakítási ciklusán át a fogyasztói oldalon megvalósuló hőleadásig terjednek. A hőszivattyús rendszerek három fő áramlási körből állnak, amelyek egyaránt meghatározzák az energiaáramlás folyamatát:

- Hőforrás oldal (Primer kör): Ez az áramlási kör biztosítja a hőenergiát hőszivattyú számára. A hőforrás lehet maga a talaj, víz, levegő, de akár bármilyen technológiai folyamatokból felszabadult hő.
- Hűtőközeg ciklus (Hőszivattyú kör): A hőszivattyús rendszer központi része, amelyet a kompresszor, az elpárologtató, a kondenzátor és a fojtószelep komponensek alkotnak. A zárt áramlási kör munkaközege a hűtőközeg, amely halmazállapotváltozások során felveszi a hőt a hőforrásból majd pedig leadja azt a fogyasztónak mechanikai energiafelhasználás mellett.
- Fogyasztói oldal (Szekunder kör): A rendszer által leadott hőenergia elosztása a fűtési vagy hűtési rendszerben, amely közvetlenül befolyásolja a felhasználói komfortot és az energiahatékonyságot. A fogyasztói oldal kialakítása lehet, padló-, falvagy mennyezet fűtés, de akár radiátor vagy fan-coil kialakítású is.

A hőszivattyús rendszerek matematikai modellezése és annak optimalizálása a rendszer fizikai modelljének a leképezése. A matematikai modellalkotásunk lényegében a rendszert leíró egyenletek (beleértve a kezdeti feltételeket, peremfeltételeket és adatrendszert) felállítása. Az általunk bemutatott modell koncentrált paraméterű, azaz a rendszer paramétereinek térbeli eloszlását állandónak tekintjük. Ez azt jelenti, hogy az egyes paraméterek csak egy adott, konkrét értékkel szerepelnek.

A matematikai modellek előállítására a white-box (fizikai alapú), black-box (adatvezérelt) és a grey-box (vegyes modell alkalmazása) módszerek alkalmazhatók. A matematikai modellünk előállítására a fizikai alapú elméleti megközelítési módszert alkalmaztuk. Az input-output modellezés rendszerszintű alapjait és a kapcsolódó terminológiát többek

között Zadeh és Polak [16] is tárgyalja. A white-box modellek a hőszivattyús rendszer fizikai törvényein alapulnak, és a hő- és tömegáramlási egyenletek és termodinamikai törvények segítségével írják le a rendszer működését, tehát az előzetes információkra támaszkodva, fizikai megfontolások alapján történik. Kutatásunkban a hőszivattyús rendszer anyag- és energiaáramainak összefüggéseit egy fehér doboz modell alkalmazásával elemezzük egy meglévő talajszondás hőszivattyús rendszer esetében. A modell nem terjed ki a tervezési szakaszra, mivel a vizsgálat középpontjában az üzemeltetés optimalizálása áll, amely során mesterséges intelligencia alapú szabályozási logikák is alkalmazásra kerülnek. Mindezen vizsgálatok alapjául a komponensenként meghatározott transzformációs egyenletek szolgálnak, amelyek a különböző bemeneti és kimeneti változók közötti kapcsolatokat írják le. A transzformációs egyenleteket meghatározzák a bemeneti és kimeneti változók közötti kapcsolatot a döntési változó függvényében. Ezek az összefüggések teszik lehetővé a rendszer viselkedésének elemzését és optimalizálását különböző paraméterek változásának függvényében. Meglévő rendszerek esetén a talajszonda jellemzői és a telepítés feltételei előre meghatározottak, míg új telepítés esetén a különböző telepítési paraméterek a talajszondás modell döntési változóiként kezelhetők. A 2.ábra bemutatja egy üzemelő talajszondás rendszer fehérdoboz modelljét a hőforrástól a fogyasztóig.



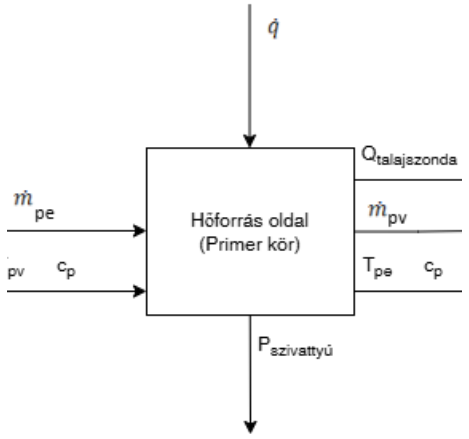
2. ábra: Üzemben lévő talajszondás hőszivattyú bemeneti-kimeneti modellje

A talajszondás hőszivattyús hőforrás oldali input-output modellje

A primer kör feladata a hőenergia szállítása egy hőhordozó közeg (például víz, glikol-víz keverék) segítségével, amelyet egy keringető szivattyú mozgat a rendszerben. A folyamat során a közeg a hőforrásból hőt vesz fel, majd azt a hőszivattyú elpárologtatójához továbbítja, ahol a hűtőközeg elpárolgása révén a rendszer számára hasznosíthatóvá válik.

A hőforrás oldal bemeneti-kimeneti modellje, amely a 3.ábrán látható, azt a folyamatot írja le, amely során a talajból nyert hőenergia a hőszivattyú primer körébe kerül átadásra. A hőforrás oldal maga a talajszonda, amelynek hőfelvétele csak a talajból származó q hőáramból eredhet. A modell bemeneti oldalán szereplő legfontosabb változók a primer kör tömegárama, a visszatérő hőhordozó közeg hőmérséklete, a hőáramsűrűség a talajszonda mentén, valamint a közeg fajhőkapacitása. Ezek az adatok a talajhő kinyerési folyamat alapját alkotják, és egy adott mélység (H) mentén történő hőcsere jellemzésére szolgálnak. A modell kimeneti oldalán megjelenő főbb paraméterek, a primer oldali előremenő

hőmérséklet, a teljes szondán keresztül átvett hőteljesítmény (a hőáramsűrűség integrálásával számítva), a keringető szivattyú villamos teljesítményigénye. Ezek a kimenetek lehetővé teszik a talajkör energetikai értékelését és a hőszivattyúval való illesztés optimalizálását. A transzformációs egyenletek közül az első a talajszonda menti hőáramsűrűség meghatározására szolgál, amely a szondán belüli és a környező talaj hőmérséklet-különbsége, valamint az adott mélységhez tartozó termikus ellenállás alapján számítható. A teljes hőteljesítmény az adott mélység menti hőáram sűrűség integrálásával nyerhető, vagy egy egyszerűsített formában a tömegáram, fajhő és hőmérséklet-különbség szorzataként is meghatározható. A keringető szivattyú teljesítményigénye a tömegáram és a nyomáskülönbség szorzatán alapul, figyelembe véve a hidraulikus és mechanikai hatásfokokat.



3. ábra: Talajszondás hőszivattyús rendszer hőforrás oldali input-output modellje üzemelési állapotban

A talajszondás hőforrás bemeneti és kimeneti paramétereit, illetve transzformációs egyenleteit az 1.táblázat foglal össze:

Bemeneti paraméterek	Kimeneti paraméterek	Transzformációs egyenletek
$\dot{m}_p$, T_{pv}, $\dot{q}$, c_p	c_p, $\dot{m}_p$, T_{pe}, $Q_{talajszonda}$, $P_{szivattyú}$	$\dot{q}(H) = \frac{T_{talaj}(H) - T_{pv}(H)}{R_{eredő}(H)}$ $Q_{talajszonda} = \int_0^H \dot{q}(H)dH$ $Q_{talajszonda} = \dot{m}_p c_p (T_{pe} - T_{pv})$ $P_{szivattyú} = \dot{m}_p W \frac{1}{\eta_i}\frac{1}{\eta_m}$

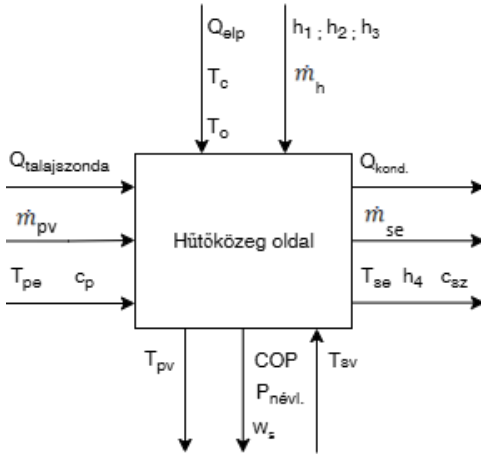
1. Táblázat: Hőforrás oldali input-output paraméterek

A talajszondás hőszivattyús hűtőközeg oldali input-output modellje

A hőforrás közvetlenül a hűtőközeg ciklushoz kapcsolódik és az elpárologtatónak adja át a talajból kinyert hőt. A hűtőközeg kör működése négy fő lépésből áll. Elsőként az

elpárologtatóban a hűtőközeg folyadék formában lép be és a primer oldalról felvett hőenergia hatására elpárolog, miközben belső energiája megnő. Ezután a kompresszorban a hűtőközeg gőz halmazállapotban lép be, és a sűrítési folyamat során megnövekedik a nyomása és hőmérséklete, miközben térfogata csökken. Ezt követően a magas hőmérsékletű és nyomású gőz a kondenzátorba kerül, ahol a szekunder kör számára leadja a hőenergiát, és közben ismét folyékony halmazállapotba kerül. A folyadék hűtőközeg végül áthalad az expanziós szelepen, ahol nyomása és hőmérséklete lecsökken, majd újra az elpárologtatóba jut, ahol a ciklus újrakezdődik.

A hűtőközeg oldal bemeneti–kimeneti modellje, amelyet a 4.ábrán mutatunk be a hőszivattyú azon részfolyamatait írja le, amelyek során a hő a primer körből a szekunder kör felé történő szállításához szükséges munkavégzés és hőcserélés zajlik le. A modell bemeneti oldalán a primer körhöz kapcsolódó fizikai jellemzők szerepelnek, mint a tömegáram, az előremenő hőmérséklet, valamint a hőhordozó közeg fajhője. Ezen túlmenően a modell figyelembe veszi a talajszondán keresztül felvett hőteljesítményt, valamint a szekunder oldal visszatérő hőmérsékletét, amely a hőleadás oldali állapotot reprezentálja. A rendszer kimeneti oldalán olyan jellemzők találhatók, amelyek a hűtőközeg körfolyamat eredményeként alakulnak ki, ideértve a primer oldal visszatérő hőmérsékletét, a szekunder kör tömegáramát, a kondenzátor hőteljesítményét, az előremenő hőmérsékletet, valamint a hűtőközeg entalpiaértékeinek (pl. h_4) számított értékeit. Ezek alapján számítható a kompresszor által végzett fajlagos munka, valamint a rendszer teljesítménytényezője (COP), amely a leadott hőteljesítmény és a bevitt elektromos teljesítmény hányadosaként értelmezhető. A hűtőközeg körfolyamat szerves része az elpárologtató és az egyes entalpiaváltozások, ezek részletesen nem jelennek meg a modellben, mivel ezek a belső termodinamikai cikluson belül zajlanak le, amelyet ebben az esetben feketedobozként kezelünk. A transzformációs egyenletek a hőmérleg- és energiamérleg összefüggéseken alapulnak. A kondenzációs hőteljesítmény a hűtőközeg tömegárama és entalpiakülönbsége alapján számítható, míg a teljesítménytényező a kondenzátor hőteljesítményének és a névleges villamos teljesítménynek a hányadosaként adódik. A névleges teljesítmény a kompresszor villamos munkája, amelyet a mechanikai és elektromos hatásfok figyelembevételével határozunk meg. A fajlagos munka a belépő és kilépő entalpiaértékek különbségéből származtatható.



4. ábra: Talajszondás hőszivattyús rendszer hűtőközeg oldali input-output modellje üzemelési állapotban

A hűtőközeg kör bemeneti és kimeneti paramétereit, illetve transzformációs egyenleteit a 2. táblázat foglalja magába:

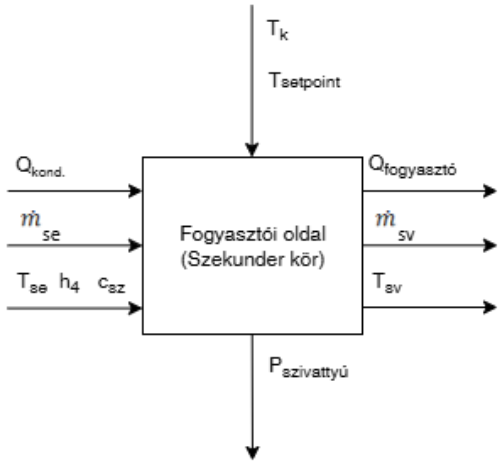
Bemeneti adatok	Kimeneti adatok	Transzformációs egyenletek
$\dot{m}_p, T_{pe}, c_p, Q_{talajszonda}, T_{sv}$	T_{pv}, $\dot{m}_s$, $Q_{kond.}$, T_{se}, c_s, h_4, $P_{névleges}, COP, W_s$	$Q_{kond} = \dot{m}_h(h_2 - h_3)$ $Q_{talajszonda} = \dot{m}_p c_p(T_{pe} - T_{pv})$ $COP = \frac{Q_{kond}}{P_{névl.}}$ $P_{névleges} = \dot{m}_h W \frac{1}{\eta_i}\frac{1}{\eta_m}$ $h_2 = f(T_c, T_o)$ $h_4 = h_2 - \frac{Q_{kond.}}{\dot{m}_h}$ $W_s = h_2 - h_1$

2. Táblázat: Hűtőközeg oldali input-output paraméterek

A talajszondás hőszivattyús fogyasztó oldali input-output modellje

A rendszer fogyasztói oldala (szekunder kör) az a rendszeregység, amelyen keresztül a hőszivattyú által előállított hőenergia eljut a végfelhasználóhoz. Ez a szakasz biztosítja a hőenergia elosztását az épület fűtési rendszerébe. A fogyasztói oldal tehát a hőszivattyús rendszer azon része, amely közvetlen kapcsolatban áll a komfortigények teljesítésével.

A fogyasztói oldal bemeneti-kimeneti modelljében, 5. ábra, a rendszer azon szakaszát vizsgáljuk, ahol a hőszivattyú által előállított hőenergia átadásra kerül a végfelhasználó felé. A modell bemeneti paraméterei közé tartozik a szekunder oldali tömegáram, a kondenzátor hőteljesítménye, az előremenő hőmérséklet, a hőhordozó közeg fajhője, valamint a hűtőközeg entalpiaértéke a kondenzátor után. További fontos bemeneti adat a külső hőmérséklet, valamint a kívánt előremenő hőmérséklet, azaz a beállított érték (T_setpoint), amely meghatározza a komfortigény szerinti hőellátást. A modell kimeneti oldalán a rendszer által ténylegesen leadott hőteljesítmény, a szekunder oldal visszatérő hőmérséklete, valamint a szekunder szivattyú villamos teljesítményigénye jelenik meg. Ezek az értékek jellemzik a fogyasztói oldal energiaátadási hatékonyságát és villamosenergia-felhasználását. A transzformációs egyenletek alapján a fogyasztói hőteljesítmény kiszámítása a szekunder tömegáram, a hőhordozó közeg fajhője és az előremenő-visszatérő hőmérséklet különbsége alapján történik. A szivattyú villamos teljesítményfelvételét a szekunder tömegáram, a kompresszor teljesítménye, valamint az elektromos és mechanikai hatásfok figyelembevételével számítjuk.



5. ábra: Talajszondás hőszivattyús rendszer fogyasztói oldali input-output modellje üzemelési állapotban

A fogyasztói oldal bemeneti és kimeneti paramétereit, valamint a kapcsolódó transzformációs egyenleteket a 3. táblázat tartalmazza:

Bemeneti adatok	Kimeneti adatok	Transzformációs egyenletek
$\dot{m}_s$, $Q_{kond.}$, T_{se}, c_s, h_4, T_k, $T_{setpoint}$	$\dot{m}_s$, $Q_{fogyasztó.}$, T_{sv}, $P_{szivattyú}$	$Q_{fogyaszó} = \dot{m}_p c_p (T_{se} - T_{sv})$ $P_{szivattyú} = \dot{m}_s W \frac{1}{\eta_i} \frac{1}{\eta_m}$

3. Táblázat: Fogyasztói oldali input-output paraméterek

A fehérdoboz modellen alapuló leírás részletes és pontos képet ad a rendszer termodinamikai viselkedéséről, az ilyen modellek korlátozottan képesek alkalmazkodni a valós működés során fellépő gyorsan változó körülményekhez, illetve a nemlineáris vagy nem jól modellezhető viselkedésekhez. Ennek kezelésére a következő fejezetben bemutatjuk, hogyan egészíthető ki a fizikai modell mesterséges intelligencia alapú optimalizáló és vezérlési réteggel, amely képes valós idejű döntéseket hozni a rendszer hatékonyabb működtetése érdekében.

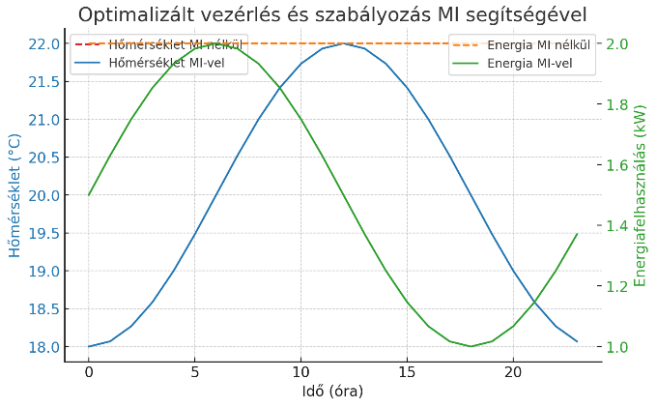
MESTERSÉGES INTELLIGENCIA ALAPÚ OPTIMALIZÁLÁS ALKALMAZÁSA

A mesterséges intelligencia alkalmazása jelentős mértékben javíthatja a hőszivattyús rendszerek hatékonyságát, élettartamát, valamint a felhasználói komfortot. Az alábbiakban összefoglaljuk az AI főbb alkalmazási területeit a hőszivattyúk működésében:

Optimalizált vezérlés és szabályozás:

- Az AI valós idejű adatok alapján folyamatosan elemzi a hőszivattyú működési paramétereit, valamint a külső és belső hőmérsékleti viszonyokat és aktuális energiaárakat, majd ezek alapján optimalizálja a rendszer működését. Ennek konkrét példái:

- Tanuló algoritmusok: Az AI-alapú rendszerek képesek tanulni az épület energiaigényeiből és a felhasználók szokásaiból, így intelligens és testreszabott vezérlést biztosítanak.
- Előrejelzés-alapú működtetés: Időjárási adatok és előrejelzések alapján az AI előzetesen szabályozza a fűtési vagy hűtési teljesítményt, ezzel csökkentve a szükségtelen energiafelhasználást.
- Intelligens leolvasztási folyamat: Fagyási viszonyok esetén az AI képes minimalizálni a leolvasztási ciklusok gyakoriságát és időtartamát, mérsékelve ezzel a rendszer energiapazarlását és optimalizálva annak teljesítményét.



6. ábra: Optimalizált vezérlés és szabályozás AI segítségével

A 6. ábra az AI-alapú optimalizált vezérlés és szabályozás hatását mutatja be. A kék folytonos vonal jelzi az AI-alapú dinamikus hőmérséklet-szabályozást, amely folyamatosan alkalmazkodik a környezeti feltételekhez, növelve a komfortérzetet és az energiahatékonyságot. Ezzel szemben a piros szaggatott vonal az AI nélküli, statikus hőmérséklet-beállítást reprezentálja, amely nem képes reagálni a változó külső körülményekre. A zöld vonal az AI-alapú rendszer energiafelhasználás-csökkentő hatását szemlélteti, amely a fűtési és hűtési igények függvényében optimalizálja az energiafogyasztást. A narancssárga szaggatott vonal az AI nélküli rendszer kevésbé hatékony, állandó energiafogyasztását jelzi. Az AI-alapú optimalizált szabályozás legfontosabb előnyei:

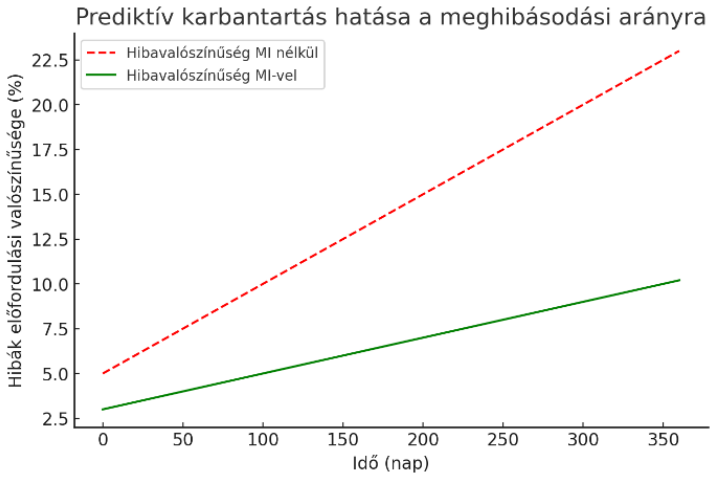
Energiahatékonyság növelés:

- Dinamikus teljesítményszabályozás: Az AI folyamatosan elemzi a terhelési viszonyokat és a hőforrás állapotát, optimalizálva a kompresszor és a szivattyúk működését.
- Hálózati integráció: A rendszer képes együttműködni az elektromos hálózat változó tarifáival és a megújuló energiaforrásokkal (pl. napelemek), ezáltal gazdaságosabb energiafelhasználást biztosítva.

Prediktív karbantartás:

- Hibák előrejelzése: Az AI rendszeresen monitorozza a főbb komponenseket (pl. kompresszor, szivattyúk, hőcserélők), így a potenciális meghibásodások előre jelezhetővé válnak, lehetővé téve az időben végrehajtott karbantartást.

- Anomália-detekció: Az AI képes a normálistól eltérő működési viszonyokat (pl. szivárgások, túlzott energiafogyasztás) felismerni, és szükség esetén automatikusan értesíteni a felhasználót vagy a karbantartó személyzetet.



7. ábra: Prediktív karbantartás hatása a meghibásodási arányra

A 7. ábra szemlélteti a prediktív karbantartás hatását a hőszivattyús rendszer meghibásodási valószínűségére. Az ábrán a piros szaggatott vonal az AI-alapú prediktív karbantartás nélküli állapotot mutatja, ahol a meghibásodás valószínűsége az idő előrehaladtával folyamatosan növekszik. Ezzel szemben a zöld folytonos vonal az AI-alapú prediktív karbantartással ellátott rendszert reprezentálja, amely esetében a meghibásodások bekövetkezésének valószínűsége lassabb ütemben emelkedik. Ennek oka, hogy az intelligens rendszer előre jelzi a potenciális meghibásodásokat, lehetővé teszi az időben történő beavatkozásokat.

Felhasználói komfort növelés:

- Az AI-alapú rendszer automatikusan alkalmazkodik a lakók jelenlétéhez és szokásaihoz, ezáltal optimális hőmérséklet-szabályozást biztosít.
- Az intelligens rendszerek integrálhatók hangvezérelt asszisztensekkel (például Alexa vagy Google Assistant), így egyszerűbbé és kényelmesebbé válik a hőszivattyú működésének szabályozása.

Az AI-integráció célja és rendszerszintű szerepe

A rendszer optimalizálásának egyik lehetséges megközelítése a hagyományos, fizikai törvényeken alapuló (white-box) modellezés kiegészítése mesterséges intelligencián (AI) alapuló döntéstámogatási és vezérlési módszerekkel. Az AI integrálása lehetővé teszi a hőszivattyús rendszer működésének valós idejű monitorozását és dinamikus optimalizálását, különösen a fogyasztói igényekhez való alkalmazkodásra, az energiahatékonyság növelésére, valamint az üzemeltetési biztonság fokozására. Az AI-alapú megközelítés lényege, hogy az egyes alrendszerekhez tartozó input–output paraméterek, valamint a mérhető és számított állapotjelzők elemzése révén olyan szabályozási változók kerülnek meghatározásra, amelyek a rendszer viselkedését energiahatékonysági vagy komfortkritériumok

mentén optimalizálják. A mesterséges intelligencia tehát nem önálló fizikai modellként jelenik meg, hanem egy, a mért adatokból tanuló, prediktív képességekkel rendelkező vezérlési struktúraként, amely képes a rendszer valós viselkedéséhez illeszkedő működési stratégiákat kialakítani. A 4. táblázat az AI-alapú rendszer bemeneti és kimeneti paramétereit, valamint az alkalmazott algoritmikus logikákat foglalja össze, összhangban az input–output alapú szemlélettel, amely a hőszivattyús rendszer szabályozási lehetőségeinek értelmezéséhez szükséges.

Bemeneti adatok	Kimeneti adatok	AI működési logikák
$\dot{m}_p$, $\dot{m}_s$, c_p, c_s, T_{pv}, T_{pe}, T_{sv}, T_{se}, $Q_{talajszonda}$, $Q_{kond.}$, $Q_{fogyasztó.}$, COP, W_s, $P_{szivattyú}$, h_1, h_2, h_3, h_4, T_k, $T_{setpoint}$	${\dot{m}_p}^{AI}$, ${\dot{m}_s}^{AI}$, ${T_{setpoint}}^{AI}$, ${W_s}^{AI}$, COP^{AI}, ${P_{szivattyú}}^{AI}$	$Min(P_{elektromos}), ha\ Q_{fogyasztó} \geq Q_{igény}$ $W_s + \sum P_{szivattyú} \rightarrow min!$ $COP = \frac{Q}{P} \rightarrow max!$ $COP = f(T_p, T_s, \dot{m}_p, Q_{kond.}, \dots.)$ $COP < 3$ és $T_{sv} > T_{setpoint} + 2 \rightarrow \dot{m}_s \downarrow$ $Y_{\{t+1\}} = f(X_t, X_{\{t-1\}}, \dots, X_{\{t-n\}})$

4. Táblázat: Mesterséges intelligencia alapú szabályozás input-output modellje

Az AI-alapú modell bemenetét a rendszer valós idejű és számított üzemi jellemzői képezik, ideértve többek között a tömegáramokat, a primer és szekunder kör hőmérsékleteit, a hőteljesítményeket, a COP értéket, valamint a szivattyúk és a kompresszor villamos teljesítményfelvételét. A modell kimenete olyan szabályozási javaslatokat fogalmaz meg, amelyek célja az energiahatékonyság növelése és a fogyasztói igények kiszolgálása minimális villamosenergia-felhasználás mellett. Ezek a predikciók a primer és szekunder kör optimalizált tömegáramaira, a setpoint hőmérséklet módosítására, valamint a kompresszor és szivattyúk célteljesítményére vonatkoznak. A mesterséges intelligencia működése különféle logikai struktúrákon alapul, amelyek közül kiemelkedik az energiafelhasználás minimalizálását célzó optimalizálás, a COP érték maximalizálása, valamint az előrejelző modellek alkalmazása. A rendszer például képes arra, hogy ha a COP értéke 3 alá csökken, miközben a visszatérő hőmérséklet meghaladja a kívánt értéket, akkor automatikusan csökkentse a szekunder oldali tömegáramot. A modell prediktív komponensei idősoros gépi tanulási technikákra épülnek, amelyek a korábbi időpillanatok jellemzőinek figyelembevételével becsülik meg a rendszer következő állapotát.

Szabályozási modellek összehasonlítása

A hagyományos épületgépészeti szabályozás jellemzően PID (proporcionális-integrális-derivált) vezérlést alkalmaz, amely egy adott referenciaérték elérésére törekszik. Ezzel szemben az AI-alapú szabályozás képes folyamatosan tanulni a rendszer működéséből, és optimalizálni a vezérlési paramétereket valós időben. Az 5.táblázat bemutatja a hagyományos PID és AI alapú szabályozások közötti előnyöket és hátrányokat.

Szabályozási típus	Működés	Előnyök	Hátrányok
PID szabályozás	Előre meghatározott referenciaérték alapján működik	Egyszerű, könnyen implementálható	Nem adaptív, nem képes tanulni
AI-alapú szabályozás	Valós idejű adatokat elemez és optimalizál	Folyamatos alkalmazkodás, magasabb hatékonyság	Nagy számítási kapacitást igényel

5. Táblázat: PID és AI alapú szabályozások összehasonlítása

A PID szabályozás három komponensből áll. A proporcionális rész a hiba nagyságával arányos jelet generál, az integrális komponens az időben felhalmozott hibát veszi figyelembe, míg a derivált tag a hiba változási sebességére reagál. Ez a szabályozásforma jól működik lineáris, kiszámítható rendszerek esetében, azonban nem képes adaptívan követni a változó körülményeket vagy előre jelezni a rendszer válaszait. A PID szabályozó beállítása tapasztalati úton történik, és nem minden esetben garantálja az optimális energiafelhasználást. Chai és társai [17], Luo és társai [18], Badescu és társai [19] kutatásaikban szintén PID szabályozással foglalkoznak. Kutatásaik rávilágítanak arra, hogy bár a PID szabályozás egyszerűsége miatt sok esetben előnyös, nem képes tanulni a rendszer viselkedéséből, és korlátozott az alkalmazkodóképessége.

Az AI-alapú szabályozás különböző intelligens algoritmusokat alkalmazhat, amelyeket a következő fejezetben részletesen tárgyalunk. Ezek a szabályozási módszerek képesek a rendszer működési mintáiból tanulni, előrejelzéseket készíteni, és optimalizálni a szabályozási paramétereket valós időben. Az utóbbi években egyre több kutatás foglalkozik a mesterséges intelligencián alapuló szabályozási módszerek alkalmazásával a hőszivattyús rendszerekben. Wang és társai [20] egy gépi tanuláson alapuló szabályozási modellt alkalmaztak egy hőszivattyús rendszer energiafelhasználásának csökkentésére. Eredményeik szerint az AI-alapú vezérlés akár 10–15%-os energiamegtakarítást is eredményezhetett a hagyományos PID-hez képest. Zhao és társai [21] egy mélytanulásra épülő előrejelző modellt alkalmaztak, amely a hőmérséklet-ingadozásokra reagálva szabályozta a rendszer teljesítményét. A kutatás szerint a modell nemcsak pontosabban tudta kiszolgálni a komfortigényt, hanem csökkentette a berendezés ki- és bekapcsolási ciklusainak számát is, ezzel növelve az élettartamot. Sun és társai [22] erősítéses tanulási módszert alkalmaztak, amely képes volt önállóan tanulni a rendszer működéséből anélkül, hogy előre definiált szabályokat kellett volna beállítani. A modell az idő előrehaladtával egyre jobb teljesítményt ért el, és folyamatosan adaptálta magát a környezeti változásokhoz.

Alkalmazott AI-módszerek

Az AI-technológiák különböző formái eltérő előnyökkel és korlátokkal rendelkeznek. Az alkalmazott mesterséges intelligencia módszerek alapvetően négy fő megközelítés szerint csoportosíthatók, amelyek közé tartozik a felügyelt tanulás, nem felügyelt tanulás, megerősítéses tanulás és szabályalapú rendszerek. A módszerek kiválasztása függ az elér-

hető adatok mennyiségétől, a rendszer komplexitásától, valamint a kívánt szabályozási céltól. Az alábbi 6.táblázatban bemutatjuk a leggyakrabban alkalmazott módszereket és azok szerepét a hőszivattyús rendszerekben.

Megnevezés	Előnyök	Hátrányok	Alkalmazási területek
Mélytanulási modellek (Deep Learning - DL)	Kiváló mintafelismerési képesség. Nagy mennyiségű adat esetén pontosabb eredmények. Alkalmazható komplex, nemlineáris rendszerekben.	Magas számítási igény (GPU szükséges lehet) Nagy mennyiségű tanulóadatot igényel.	Hőmérsékleti és terhelési előrejelzések készítése. Optimalizált vezérlés a felhasználói komfort növelése érdekében. Időbeli dinamikus rendszerek szabályozása (pl. RNN és LSTM modellek segítségével).
Gépi tanulás (Machine Learning - ML)	Jó általánosítási képesség. Kis adathalmazokon is működik.	Kevésbé hatékony komplex rendszerekben. Jellemzően kézi paraméterhangolást igényel.	Energiafogyasztás modellezése és előrejelzése. Komfortérzet-alapú szabályozás.
Fuzzy logika alapú szabályozás (Fuzzy Logic Control - FLC)	Nem igényel nagyméretű tanulóadatot. Könnyen értelmezhető szabályrendszer.	Nem alkalmas összetett rendszerek pontos modellezésére.	Adaptív fűtés-hűtési szabályozás.
Erősítéses tanulás (Reinforcement Learning - RL, DRL)	Automatikusan alkalmazkodik a változó körülményekhez.	Hosszú tanulási idő szükséges.	Öntanuló vezérlés a fogyasztási minták alapján.

6. Táblázat: Leggyakrabban alkalmazott AI módszerek a hőszivattyús rendszerekben

A táblázatban szereplő módszerek mindegyike más előnyöket kínál a hőszivattyús rendszerek szabályozásában. A mélytanulási modellek különösen hatékonyak idősoros előrejelzésekhez és komplex energetikai mintázatok felismeréséhez, ugyanakkor magas adatigényt és számítási teljesítményt követelnek. A gépi tanulási modellek gyorsabb implementációt tesznek lehetővé, de korlátozottabbak nemlineáris rendszerek esetén. A fuzzy logika jól alkalmazható ott, ahol a fizikai folyamatok nem írhatók le egzakt módon, míg az erősítéses tanulás hosszabb tanítási idő mellett rugalmasan tud alkalmazkodni a változó körülményekhez.

ÖSSZEGZÉS

A tanulmány során bemutatott modellalapú megközelítés igazolta, hogy egy hőszivattyús rendszer működése átfogóan értelmezhető komponensenként felépített, input–output struktúrájú fehér doboz modell segítségével. A hőszivattyús rendszer három fő áramlási körének bemeneti és kimeneti paraméterei, valamint azok transzformációs egyenletei alapján részletes energetikai és működési elemzés végezhető. Ez a fizikai alapokon támaszkodó megközelítés lehetőséget ad a rendszer teljesítményének értékelésére és a működési folyamatok mélyebb megértésére. Valós üzemeltetési környezetben, ahol a külső körülmények, terhelési viszonyok és felhasználói igények folyamatosan változnak, a hagyományos szabályozási módszerek, mint például a PID, csak korlátozott alkalmazkodóképességgel rendelkeznek. Ezzel szemben a mesterséges intelligencia alapú szabályozási megközelítések képesek valós időben reagálni a rendszer állapotára, tanulni a működésből, és prediktív módon optimalizálni a vezérlési paramétereket. A mesterséges intelligencia alkalmazása a hőszivattyúk teljesítményszabályozásában számos előnnyel járhat, beleértve az energiatakarékosságot, a hosszú távú működési hatékonyságot és a környezetbarát működést. Az AI által vezérelt rendszerek képesek a valós idejű adatok alapján dinamikusan optimalizálni a hőszivattyú működését, figyelembe véve az energiafogyasztást és a környezeti tényezőket. Mindez hozzájárulhat a fenntarthatóbb és gazdaságosabb energetikai megoldásokhoz. A kutatás során bemutatott AI-módszerek alkalmazása új lehetőségeket nyit a hőszivattyús rendszerek energiahatékonyságának javítására, a COP érték maximalizálására és a komfortigények pontosabb kiszolgálására.

FELHASZNÁLT IRODALOM[4]

[1] J. W. Lund, D. H. Freeston, and T. L. Boyd, “Direct utilization of geothermal energy 2010 worldwide review,” *Geothermics*, vol. 40, no. 3, pp. 159–180, Sep. 2011, doi: https://doi.org/10.1016/j.geothermics.2011.07.004.

[2] B. Sanner, C. Karytsas, D. Mendrinos, and L. Rybach, “Current status of ground source heat pumps and underground thermal energy storage in Europe,” *Geothermics*, vol. 32, no. 4–6, pp. 579–588, Aug.–Dec. 2003, doi: https://doi.org/10.1016/S0375-6505(03)00060-9.

[3] S. J. Self, B. V. Reddy, and M. A. Rosen, “Geothermal Heat Pump Systems: Status Review and Comparison with Other Heating Options,” *Applied Energy*, vol. 101, pp. 341–348, Jan. 2013, doi: https://doi.org/10.1016/j.apenergy.2012.01.048.

[4] H. Li and M. Zheng, "Optimal control strategy of ground source heat pump systems based on load forecasting," *Energy and Buildings*, vol. 41, no. 2, pp. 217–223, 2009. https://doi.org/10.1016/S0375-6505(03)00060-9.

[5] B. Sanner, C. Karytsas, D. Mendrinos, and L. Rybach, "Current status of ground source heat pumps and underground thermal energy storage in Europe," *Geothermics*, vol. 32, no. 4–6, pp. 579–588, 2003.

[6] Y. Yao and J. Chen, “Adaptive control of ground source heat pump systems with neural network-based model predictive control,” *Energy and Buildings*, vol. 55, pp. 243–252, Dec. 2012, doi: https://doi.org/10.1016/j.enbuild.2012.08.001.

[4] példák hivatkozásokra | REFERENCES examples of references

[7] R. Yang és L. Wang, „Development of multi-agent system for building energy and comfort management based on occupant behaviors," *Energy and Buildings*, vol. 56, pp. 1–7, Jan. 2013, doi: 10.1016/j.enbuild.2012.10.025.
[8] A. M. Omer, „Ground-source heat pumps systems and applications," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 2, pp. 344–371, Feb. 2008, doi: 10.1016/j.rser.2006.10.003.
[9] M. Kozák és L. Mikó, „Geotermikus potenciál hasznosításának lehetőségei Kelet-Magyarországon.
[10] W. Thomson, „On the economy of the heating or cooling of buildings by means of currents of air," *Proceedings of the Philosophical Society of Glasgow*, vol. III, pp. 269–272, 1853.
[11] K. J. Chua, S. K. Chou, és W. M. Yang, „Advances in heat pump systems: A review," *Applied Energy*, vol. 87, no. 12, pp. 3611–3624, Dec. 2010, doi: 10.1016/j.apenergy.2010.06.014.
[12] L. Pérez-Lombard, J. Ortiz, and C. Pout, "A review on buildings energy consumption information,"*Energy and Buildings*, vol. 40, no. 3, pp. 394–398, 2008, doi: 10.1016/j.enbuild.2007.03.007.
[13] M. Árpási, „Geothermal development in Hungary—country update report 2000–2002," *Geothermics*, vol. 32, no. 4–6, pp. 725–735, Aug.–Dec. 2003, doi: 10.1016/j.geothermics.2003.07.001.
[14] Hungarian Energy and Public Utility Regulatory Authority, „National Energy Strategy 2030 with an outlook to 2040," 2022. [Online]. Available: https://2010-2014.kormany.hu/download/7/d7/70000/Hungarian%20Energy%20Strategy%202030.pdf.
[15] Z. Kovács és J. Hancsók, „Biofuels: the renewable energy sources of the future," *Hungarian Journal of Industrial Chemistry*, vol. 37, no. 2, pp. 111–116, 2009.
[16] L. A. Zadeh és E. Polak, *Rendszerelmélet*, Budapest, Hungary: Műszaki Könyvkiadó, 1972.
[17] X. Chai, Y. Lin, X. Zhang, és J. Wang, „PID control strategies for residential heat pump systems: A performance evaluation," *Energy and Buildings*, vol. 174, pp. 305–314, Sep. 2018, doi: 10.1016/j.enbuild.2018.06.041.
[18] X. Luo, H. Li, és X. Zhou, „Comparison of PID and MPC control strategies in variable-load HVAC systems," *Applied Thermal Engineering*, vol. 170, p. 115020, Feb. 2020, doi: 10.1016/j.applthermaleng.2020.115020.
[19] V. Badescu és D. Fodor, „Performance of ground-source heat pump systems under PID control with intermittent operation," *Renewable Energy*, vol. 139, pp. 602–611, Aug. 2019, doi: 10.1016/j.renene.2019.02.113.
[20] Y. Wang, T. Zhang, és Z. Li, „Energy-efficient control of heat pump systems using machine learning methods," *Energy and Buildings*, vol. 210, p. 109748, Mar. 2020, doi: 10.1016/j.enbuild.2019.109748.
[21] H. Zhao, Y. Liu, és J. Zhang, „Deep learning-based predictive control of building heating systems," *Applied Energy*, vol. 285, p. 116402, Mar. 2021, doi: 10.1016/j.apenergy.2021.116402.
[22] Y. Sun, X. Wang, és H. Chen, „Reinforcement learning for optimal control of heat pump systems in dynamic environments," *Renewable Energy*, vol. 190, pp. 1234–1245, May 2022, doi: 10.1016/j.renene.2022.03.098.

DOI: https://doi.org/10.12700/btsz.2025.7.2.133

THE TRANSFORMATION OF WORKPLACE SAFETY IN THE AGE OF TELEWORKING

A MUNKAHELYI BIZTONSÁG ÁTALAKULÁSA A TÁVMUNKA KORÁBAN

GOMBKÖTŐ Judit[1]

Abstract

The rise of teleworking has fundamentally changed the challenges of occupational safety and privacy, especially in the areas of information security and cyber protection. The aim of this research is to map the risks of teleworking and the protection strategies used by companies with the help of a questionnaire survey. The results show that smaller companies are exposed to higher risks due to lower levels of IT security measures and education, while larger organizations reduce threats with more advanced protection protocols. The most significant security challenges are data leakage, identity theft, and network attacks. The research identifies four key areas of development: IT security education, network security measures, securing company devices and applying advanced authentication solutions. Sustainable security of teleworking requires integrated technological and awareness-raising strategies.

Keywords

teleworking, occupational safety, data security, cyber defense, information security

Absztrakt

A távmunka térnyerése alapjaiban változtatta meg a munkahelyi biztonság és adatvédelem kihívásait, különösen az információbiztonság és a kibervédelem területén. Jelen kutatás célja a távmunka kockázatainak és a vállalatok által alkalmazott védelmi stratégiáknak a feltérképezése egy kérdőíves felmérés segítségével. Az eredmények rámutatnak, hogy a kisebb vállalatok magasabb kockázatoknak vannak kitéve az alacsonyabb szintű IT biztonsági intézkedések és oktatás miatt, míg a nagyobb szervezetek fejlettebb védelmi protokollokkal csökkentik a fenyegetéseket. A legjelentősebb biztonsági kihívások az adatszivárgás, az azonosító adatok ellopása és a hálózati támadások. A kutatás négy kulcsfontosságú fejlesztési területet azonosít: IT biztonsági oktatás, hálózatbiztonsági intézkedések, biztonságos céges eszközök biztosítása és fejlett hitelesítési megoldások alkalmazása. A távmunka fenntartható biztonságának érdekében integrált technológiai és tudatosságnövelő stratégiák bevezetése szükséges.

Kulcsszavak

távmunka, munkahelyi biztonság, adatbiztonság, kibervédelem, információ biztonság

[1] judit.gombkoto@msg-plaut.hu | ORCID: 0009-0002-8438-7216 | Senior SAP Consultant, msg Plaut Hungary Kft., Vezető SAP tanácsadó, msg-Plaut Hungary Kft.

BEVEZETÉS

Az elmúlt években a távmunka széles körű elterjedése alapjaiban alakította át a munkahelyi biztonság és adatvédelem kérdését. Míg korábban a dolgozók többsége irodai környezetben, ellenőrzött informatikai rendszerek és biztonsági protokollok mellett végezte feladatait, addig napjainkban egyre többen végzik teendőiket otthonról vagy kevésbé kontrollált helyszínekről. Ez a változás új kihívásokat teremt mind a szervezetek, mind az alkalmazottak számára, különösen az információvédelem, a kiberbiztonság és a digitális fenyegetések kezelése szempontjából.

Jelen kutatás célja annak feltérképezése, hogyan módosult a munkahelyi biztonság a távmunka térnyerésével, milyen kockázatokkal szembesülnek az érintettek, valamint milyen védelmi stratégiákat alkalmaznak a vállalatok az új munkavégzési formákhoz igazodva. A vizsgálat kérdőíves felmérésen alapul, amely a távmunka gyakoriságát, a használt technológiai megoldásokat, a kibervédelmi intézkedéseket és a személyes biztonsági tapasztalatokat elemzi. Az eredmények rávilágítanak a távmunka adatbiztonsági vonatkozásaira, a legjelentősebb fenyegetésekre, valamint arra, mennyire felkészültek a munkáltatók és munkavállalók egy esetleges kibertámadás vagy biztonsági incidens esetén.

A tanulmány elősegíti a távmunka biztonsági aspektusainak alaposabb megértését, valamint javaslatokat fogalmazzon meg a védelmi protokollok és oktatási stratégiák továbbfejlesztésére.

SZAKIRODALMI ÁTTEKINTÉS

A munkahelyi biztonság kérdése az utóbbi évtizedben jelentős átalakuláson ment keresztül, különösen a távmunka és a hibrid munkavégzés elterjedésének következtében. A szakirodalom számos aspektusból vizsgálja ezt a változást, többek között az információbiztonság [1] [11] [12], a szervezeti bizalom [2] [4], a munkavállalói jóllét [3] [7], valamint a jogi és egészségvédelmi szempontok tükrében [5] [9].

A digitális munkahelyek és a távmunka térhódításával új kihívások jelentek meg az információbiztonság terén. A digitális munkakörnyezetek növelik a kibertámadások és adatszivárgások kockázatát, ezért a szervezeteknek új védelmi stratégiákat kell kidolgozniuk, például VPN-használatot, kétfaktoros hitelesítést és szigorúbb hozzáférés-kezelést [1] [11] [15]. A távmunka tömeges elterjedése miatt a hagyományos IT-biztonsági kockázatelemzések már nem feltétlenül érvényesek, ezért a vállalatoknak új biztonsági protokollokat kell alkalmazniuk [12] [19]. A COVID–19 járvány idején az információbiztonsági előírások és gyakorlatok jelentős átalakuláson mentek keresztül, a biztonságos távoli munkavégzés érdekében [5].

A távmunka egyik kritikus aspektusa a munkavállalók közötti bizalom és a szervezeti kommunikáció fenntartása. A távoli munkavégzés csökkentheti a személyes interakciókat és növelheti a bizalmi problémák kialakulásának esélyét [2]. A távmunka során a formális és informális belső kommunikáció sérülhet, ami a munkavállalók elszigeteltségét és a csapatkohézió csökkenését eredményezheti [4]. A hatékony kommunikáció és együttműködés fenntartása érdekében új digitális eszközök bevezetése szükséges [10].

A távmunka nemcsak az információbiztonságot, hanem a munkavállalók fizikai és mentális jóllétét is befolyásolja. A távmunka segítheti a munka-magánélet egyensúlyának megteremtését, ugyanakkor új kihívásokat is felvet a munkáltatók és a munkavállalók számára [3]. A járvány alatti távmunka hatásai között jelentős eltérések figyelhetők meg a hagyományos

irodai munkavégzéshez képest, különösen a szubjektív jóllét tekintetében [7]. A munkavállalói elégedettség és az adatbiztonsági tudatosság szoros összefüggésben állhat a távmunka körülményeivel [13].

A COVID–19 világjárvány katalizátorként működött a távmunka gyors elterjedésében, ugyanakkor számos új biztonsági és egészségvédelmi kérdést is felvetett. A felsőoktatásban dolgozók munkavégzése jelentős átalakuláson ment keresztül, ami hatással volt a termelékenységre és a munkavállalói jóllétre [6]. A vállalatoknak nemcsak technológiai szempontból kellett gyorsan alkalmazkodniuk, hanem jogi és adatvédelmi szempontból is, például a GDPR-nak megfelelő távmunkavégzési szabályzatok kidolgozásával [9] [14]. A hibrid munkavégzésre való áttérés során számos munkahelyi biztonsági és egészségvédelmi kérdés merült fel, amelyek kezelése elengedhetetlen a fenntartható működéshez [5].

Az információbiztonsági fenyegetések kezelése érdekében a szervezeteknek azonosítaniuk kell kritikus folyamataikat, mérniük kell azok távmunka-függőségét, és megfelelő kockázatkezelési stratégiákat kell kidolgozniuk ezek védelme érdekében [12]. A vállalatoknak megfelelő távmunka-biztonsági követelményeket kell kidolgozniuk, amelyek magukban foglalják a titkosítási protokollokat és a biztonságos hozzáférési rendszereket [15]. Az adatvédelmi kihívások sajátos szabályozási megközelítést igényelnek, különösen a munkavállalók online nyomon követése és a munkáltatók ellenőrzési lehetőségei kapcsán [14].

A jövőbeli kutatásoknak érdemes tovább vizsgálniuk a távmunka hosszú távú hatásait, valamint a szervezeti és jogszabályi keretek fejlesztésének lehetőségeit annak érdekében, hogy a munkavégzés ezen formája mind a munkavállalók, mind a munkáltatók számára biztonságos és fenntartható legyen.

ANYAG ÉS MÓDSZERTAN

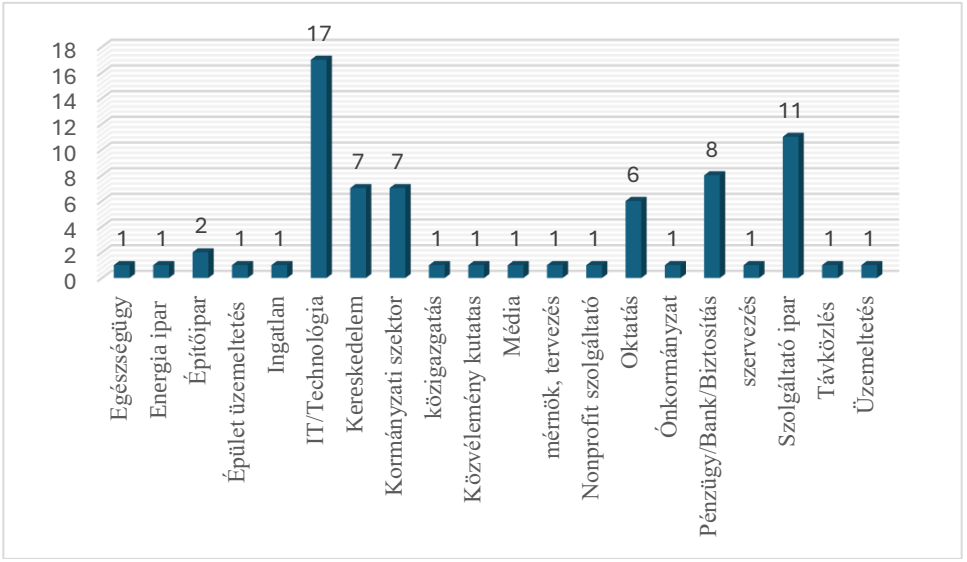
A kutatás célja a távmunka elterjedésével összefüggő munkahelyi biztonsági kihívások és munkavállalói tapasztalatok feltérképezése. Ennek érdekében kérdőíves felmérést végeztem, amely kvantitatív adatokon keresztül vizsgálta a válaszadók távoli munkavégzéssel kapcsolatos tapasztalatait, az alkalmazott biztonsági intézkedéseket és az észlelt kockázatokat.

Az adatgyűjtés egy online kérdőív segítségével történt, amelyet a Google Forms platformon keresztül tettem elérhetővé. A válaszadók különböző iparágakban dolgozó munkavállalók közül kerültek ki lásd, 1-es ábra, ami lehetőséget biztosított a szélesebb körű tapasztalatok elemzésére. Az online adatfelvétel anonim módon zajlott, ami növelte az őszinte válaszok arányát, ezáltal a kapott eredmények megbízhatóságát. A kutatás célja nem a reprezentativitás biztosítása volt, hanem az összefüggések feltárása, így az eredmények kvalitatív értelmezését részesítettem előnyben. Az adatgyűjtés 2025 januárjában zajlott.

A kérdőív 14 kérdésből állt, amelyek több tématerületet érintettek. Az első szakasz a demográfiai jellemzőkre koncentrált, beleértve az iparági hovatartozást, a vállalat méretét és a betöltött pozíciót. A második rész a munkahelyi biztonsági tényezőket vizsgálta, különös tekintettel a távmunka gyakoriságára, a használt eszközökre, a munkavégzés helyszíneire, valamint a munkáltató által biztosított kibervédelmi intézkedésekre. Emellett felmértem, hogy a válaszadók találkoztak-e adatbiztonsági incidensekkel, milyen fenyegetéseket tartanak kockázatosnak, és részt vettek-e informatikai biztonsági képzésen.

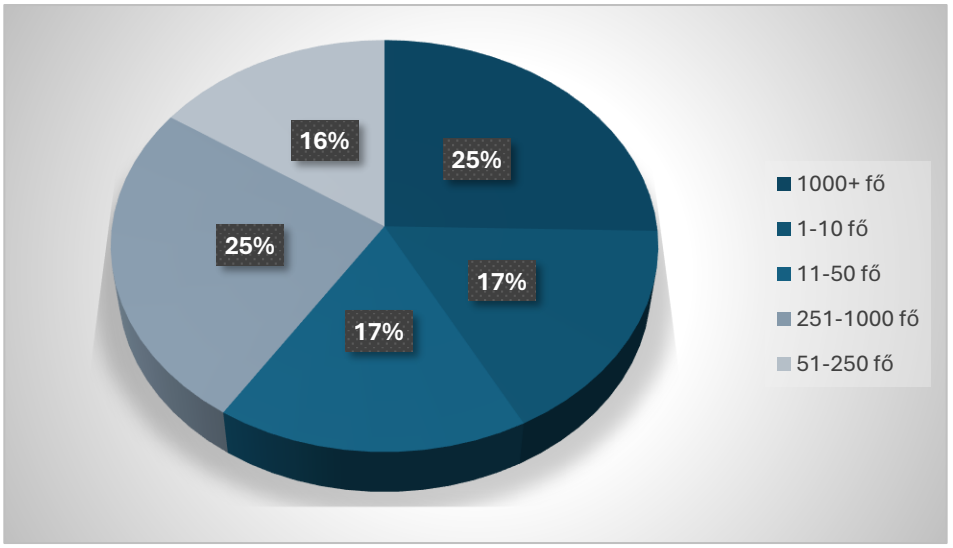
A kérdőív tartalmazott zárt és nyitott kérdéseket is. A skálázott kérdések lehetőséget adtak az objektív mérési eredmények összegzésére, míg a nyitott kérdésben a válaszadók megfogalmazhatták, mely fejlesztési területeket tartják kulcsfontosságúnak a távoli munkavégzés biztonságának javítása érdekében.

A válaszadók iparág szerinti megoszlását az 1. ábra szemlélteti. Az eredmények alapján a kitöltők 40%-a az IT/technológiai és a pénzügyi szektorban dolgozik.



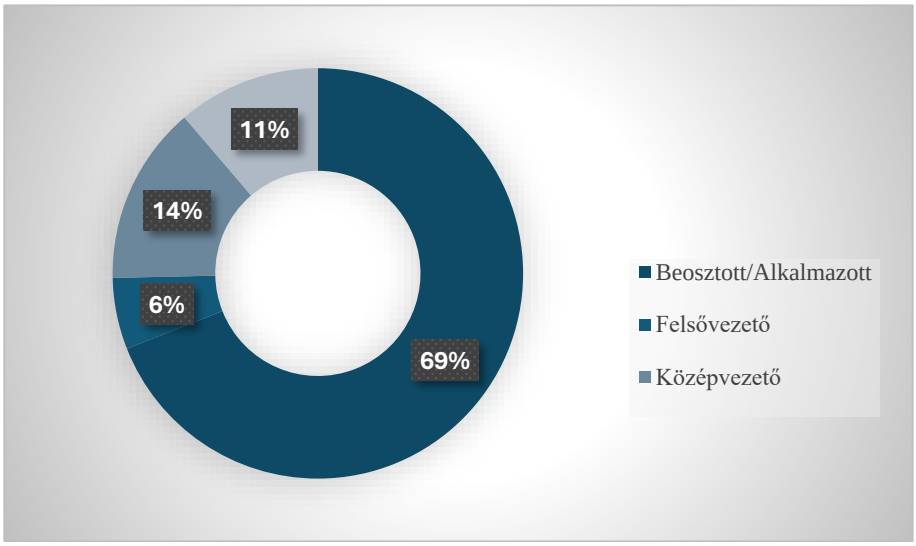
1. Ábra: A válaszadók jelenlegi iparági megoszlása Forrás: Saját kutatás, 2025, N = 71

Az adatgyűjtés során vizsgáltam a kitöltő pozícióját és a vállalat méretét. Egyszeres kitöltési lehetőséget adtam a válaszadóknak, mert ez egyértelműen eldönthető mindenki számára.



2. Ábra: A válaszadók vállalatméret szerinti megoszlása Forrás: Saját kutatás, 2025, N = 71

A válaszadók vállalatméret szerinti eloszlását a 2. ábra mutatja be, amelyből látható, hogy a kitöltők többsége nagyvállalatoknál (1000+ fő) dolgozik, ezt követik a közepes méretű cégek (251–1000 fő), majd a kisebb vállalatok. A legkevesebb válasz a mikro vállalkozások (1–10 fő) kategóriájából érkezett.



3. Ábra: A válaszadók pozició szerinti megoszlása Forrás: Saját kutatás, 2025, N = 71

A munkaköröket vizsgálva (3. ábra) a legtöbben alkalmazotti státuszban dolgoznak, míg a közép- és felsővezetők kisebb arányban szerepelnek a válaszadók között. A vállalkozók és szabadúszók is jelen vannak, de alacsonyabb reprezentációval. Az eredmények azt mutatják, hogy a kutatás résztvevőinek többsége alkalmazottként, jellemzően közép- vagy nagyvállalatoknál dolgozik, amely fontos szempont a távmunka és a biztonság összefüggéseinek értékelésében.

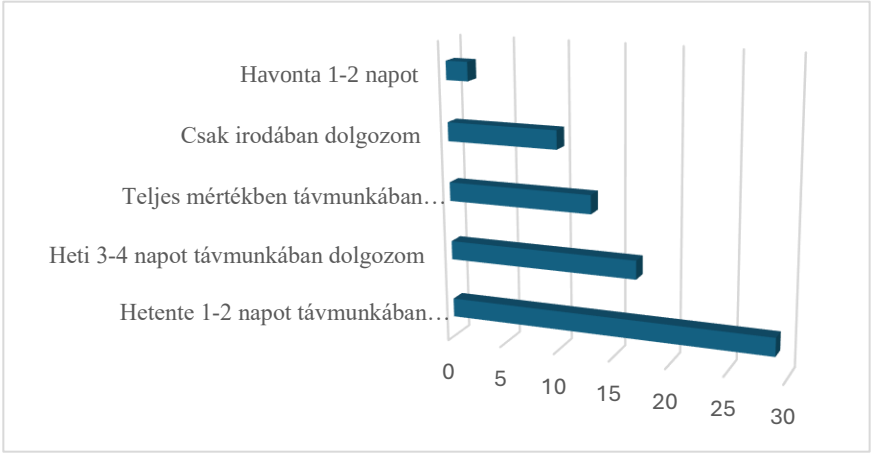
A kutatás hipotézise szerint a távmunka térnyerése új adatbiztonsági és kibervédelmi kihívások elé állítja a munkáltatókat és munkavállalókat egyaránt. Feltételezhető, hogy a kisebb vállalatok nagyobb adatbiztonsági kockázatokkal szembesülnek a korlátozott IT-védelmi intézkedések és alacsonyabb szintű biztonsági oktatás miatt, míg a nagyobb szervezetek fejlettebb technológiai és képzési stratégiákat alkalmaznak a kibertámadások kockázatának csökkentése érdekében. A megfelelő kibervédelmi intézkedések – például a kétfaktoros hitelesítés, VPN-használat és adattitkosítás – valamint a munkavállalók informatikai tudatosságának növelése kulcsfontosságú lehet a távoli munkavégzés biztonságosabbá tételében.

Az összegyűjtött adatokat statisztikai módszerekkel elemeztem, beleértve az eloszlások vizsgálatát, az átlagok és szórások kiszámítását, valamint a különböző változók közötti összefüggések feltárását. Az adatelemzéshez Microsoft Excel szoftvert használtam.

EREDMÉNYEK

A kutatás célja a távmunka munkahelyi biztonságra és adatvédelemre gyakorolt hatásainak feltárása volt. Az alábbiakban a kérdőíves felmérés eredményei kerülnek bemutatásra, amelyek rávilágítanak a távmunka elterjedtségére, a munkavégzés biztonsági kihívásaira és a munkáltatók által biztosított védelmi intézkedésekre.

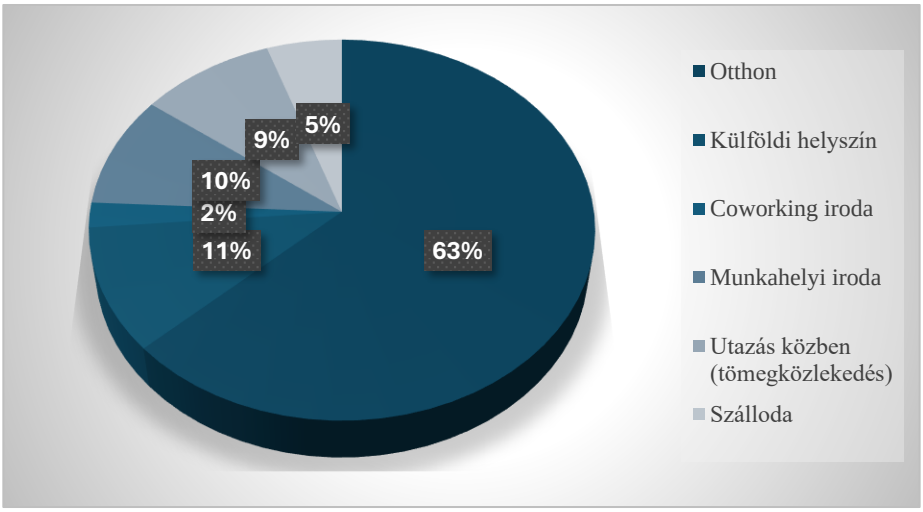
A „Milyen gyakran dolgozik távmunkában?” kérdésre adott válaszok az alábbi ábrán láthatók. A kérdőívben egyetlen válasz megjelölésére volt lehetőség, mivel a kérdésre egyértelmű válasz adható.



4. Ábra: Távmunka gyakorisága Forrás: Saját kutatás, 2025, N = 71

Az eredmények alapján a válaszadók több mint 60%-a rendszeresen dolgozik távmunkában. A leggyakoribb gyakorlat az otthonról végzett munka, amelyet a válaszadók 39,4%-a heti 1–2 napban, 22,5%-a pedig heti 3–4 napban végez.

A távmunkában használt helyszíneket az alábbi ábra szemlélteti. Mivel a válaszadók több lehetőséget is megjelölhettek, az eredmények azt tükrözik, hogy egy személy többféle helyszínen is dolgozhat távmunkában.



5. Ábra: Távmunkára használt helyszínek Forrás: Saját kutatás, 2025, N = 71

Az adatokból kiderül, hogy az otthonon kívüli helyszíneken – például kávézókban, coworking irodákban – végzett munka kevésbé elterjedt, és a legtöbben kizárólag saját lakóhelyükön dolgoznak távmunkában.

A távmunkavégzés elterjedésével az adatbiztonsági kockázatok is növekedtek, így kiemelten fontos annak vizsgálata, hogy a munkavállalók hogyan érzékelik az otthoni munkakörnyezet biztonságát, valamint mennyire érzik magukat felkészültnek egy esetleges kibertámadásra vagy adatbiztonsági incidensre. Kutatásunk célja az volt, hogy feltárjuk a távmunkában dolgozók adatbiztonsággal kapcsolatos percepcióit és a kibertámadásokkal szembeni felkészültségüket.

A vizsgálat során két fő kérdést elemeztünk:

- „Mennyire tartja biztonságosnak az otthoni munkavégzést adatbiztonsági szempontból?"
- „Mennyire érzi magát felkészültnek egy adatbiztonsági incidens esetén?"

A válaszokat egy 1-től 5-ös terjedő Likert-skálán gyűjtöttük, ahol az 1-es érték azt jelentette, hogy a válaszadó egyáltalán nem tartja biztonságosnak vagy felkészültnek magát, míg az 5-ös érték a teljes mértékben biztonságosnak vagy felkészültnek való megítélést jelölte.

Az adatok statisztikai elemzéséhez átlag- és szórásértékeket számítottunk, hogy pontosabb képet kapjunk a válaszok eloszlásáról és az érzékelt biztonsági szintek közötti eltérésekről. Az eredmények segítenek megérteni, hogy a távmunkában dolgozók mennyire érzik magukat biztonságban az otthoni munkavégzés során, illetve milyen mértékben tartják magukat felkészültnek az esetleges kibertámadásokkal szemben.

	Mennyire tartja biztonságosnak az otthoni munkavégzést adatbiztonsági szempontból?	**Mennyire érzi magát felkészültnek egy adatbiztonsági incidens esetén?**
Összesen	71	71
Középérték/átlag	4,32	3,13
Szórás	1,03	1,35
Minimum	1	1
Első kvartilis	4	2
Második kvartilis	5	3
Harmadik kvartilis	5	4
Maximum	5	5

1. Táblázat: Az otthoni munkavégzés biztonságosságának és a kibertámadásra való felkészültség statisztikai mutatói Forrás: Saját kutatás, 2025, N=71

Az eredmények szerint a résztvevők átlagosan 4,32-es értékkel ítélték meg az otthoni munkavégzés biztonságosságát, míg kibertámadás esetén saját felkészültségüket 3,13-as átlagértékre értékelték. A szórás adatokból látható, hogy az egyéni érzékelés jelentős tér el, különösen a kibervédelmi felkészültség esetében.

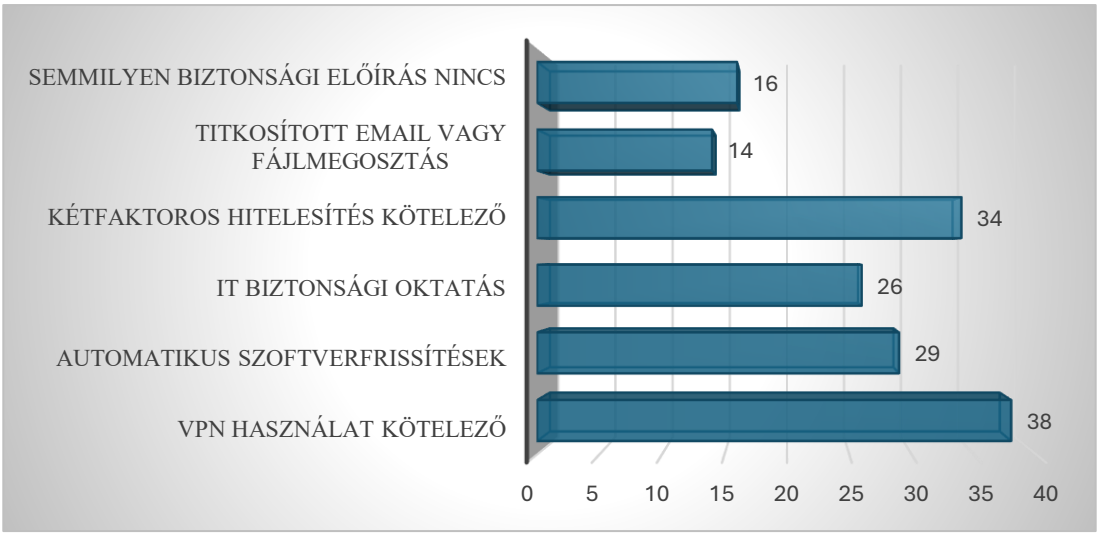
Az alábbi táblázat alapján az adatbiztonsági incidensek előfordulásának aránya és az IT biztonsági oktatásban való részvétel közötti kapcsolat vizsgálható a vállalat méretének függvényében. A cél annak megértése, hogy a nagyobb vállalatok jobban védettek-e az incidensekkel szemben, és hogy az IT biztonsági oktatás befolyásolja-e a kockázatokat.

Vállalatméret	Incidens történt	Összesen vállalt	Incidens aránya	IT biztonsági oktatásban részesült	IT biztonsági oktatásban részesült aránya
1-10 fő	3	12	25%	2	17%
11-50 fő	2	12	17%	6	50%
51-250 fő	1	11	9%	10	91%
251-1000 fő	3	18	17%	14	78%
1000+ fő	1	18	6%	14	78%
Összesen	10	71	14%	46	65%

2. Táblázat: Vállaltméret, adatbiztonsági incidensek és IT biztonsági oktatás összefüggései. Saját kutatás, 2025, N=71

Az eredmények szerint a kisebb vállalatoknál az incidensek előfordulása magasabb (25%), míg a nagyvállalatoknál jelentősen alacsonyabb (6%). Az IT biztonsági oktatásban részesültek aránya szintén méretfüggő: a mikrovállalkozások esetében csupán 17%, míg a nagyobb szervezeteknél 78–91% között mozog. Ez arra utal, hogy a vállalatok méretük növekedésével párhuzamosan egyre nagyobb figyelmet fordítanak a kibervédelemre és a munkavállalók képzésére.

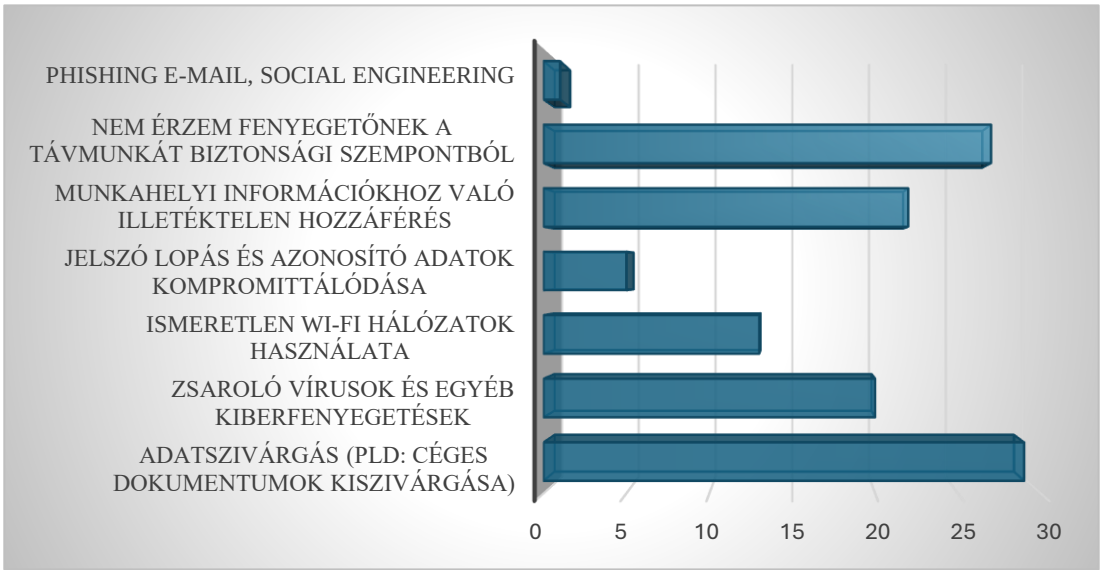
Az alábbi ábra a kibervédelmi intézkedések alkalmazására adott válaszokat szemlélteti. A kérdés többválasztásos volt, így a válaszadók több intézkedést is megjelölhettek, amelyeket távmunkájuk során alkalmaznak. Az ábra az összesített eredményeket mutatja, lehetővé téve a különböző biztonsági megoldások elterjedtségének áttekintését.



6. Ábra: Kibervédelmi intézkedések elérhetősége távmunkában Forrás: Saját kutatás, 2025, N = 71

Az eredmények szerint a munkáltatók általában biztosítanak alapvető védelmi mechanizmusokat, például VPN-t, kétfaktoros hitelesítést, azonban az IT biztonsági oktatás nem minden dolgozó számára érhető el, ami csökkentheti a védelmi intézkedések hatékonyságát.

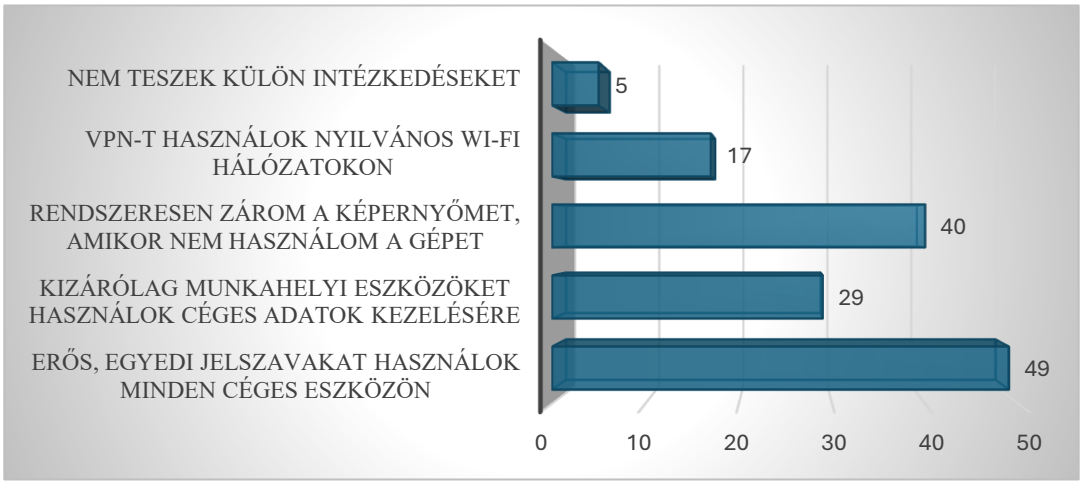
A következő ábra a távmunka során észlelt legnagyobb biztonsági kockázatokat szemlélteti. A kérdés többválasztásos volt, így a válaszadók több kockázati tényezőt is megjelölhettek. Az eredmények összesített formában mutatják, hogy mely biztonsági fenyegetések jelentik a legnagyobb kihívást a távmunkát végzők számára.



7. Ábra: A távmunka során észlelt legnagyobb biztonsági kockázatok Forrás: Saját kutatás, 2025, N = 71

A legnagyobb fenyegetések közé tartozik az adatszivárgás, az azonosító adatok ellopása és a hálózati támadások, amelyek különösen kockázatosak azok számára, akik nem megfelelően védett hálózatokon dolgoznak.

Az alábbi ábra a távmunka során alkalmazott adatbiztonsági intézkedéseket szemlélteti. Mivel a kérdés többválasztásos volt, a válaszadók több intézkedést is megjelölhettek. Az összesített eredmények alapján látható, hogy milyen védelmi gyakorlatokat alkalmaznak a távoli munkavégzés során.



8. Ábra: Intézkedések a saját adatbiztonság érdekében Forrás: Saját kutatás, 2025, N = 71

Az eredmények szerint a legtöbben jelszókezelést és képernyőzárat használnak, míg a VPN és a munkahelyi eszközök kizárólagos használata kevésbé elterjedt. A válaszok alapján szükség lenne további biztonságtudatossági képzésre, különösen azok számára, akik nem alkalmaznak semmilyen védelmi mechanizmust.

A kérdőívben egy nyitott kérdés is szerepelt, amelyben a válaszadók megoszthatták véleményüket arról, hogy mely fejlesztési területeket tartják a legfontosabbnak a távmunka biztonságának javítása érdekében. Az alábbi szófelhő a leggyakrabban említett válaszokat szemlélteti, összegyűjtve a legfontosabb fejlesztési javaslatokat.

9. Ábra: Legfontosabb fejlesztési területek a távmunka biztonságában Forrás: Saját kutatás, 2025, N = 71

A visszajelzések alapján négy fő fejlesztési irány emelhető ki:

- IT biztonsági oktatás és tudatosság növelése
- Otthoni és nyilvános hálózatok biztonságának erősítése
- Biztonságos céges eszközök és szoftverek biztosítása
- Hitelesítési és titkosítási megoldások kiterjesztése

Az adatok azt mutatják, hogy a munkavállalók nagy része a tudatosság növelését és a technikai védelem erősítését tartja a legfontosabbnak. Ennek megfelelően a távmunka biztonságának javítása érdekében olyan komplex stratégia alkalmazása szükséges, amely magában foglalja a technikai intézkedéseket, a szabályozási keretek erősítését és a munkavállalói képzések szélesítését.

A kutatás eredményei alapján komplex stratégiára van szükség, amely ötvözi a technikai védekezési eszközöket és a biztonságtudatossági programokat annak érdekében, hogy a

távmunka biztonságos és fenntartható legyen mind a munkáltatók, mind a munkavállalók számára.

KÖVETKEZTETÉSEK

A kutatás eredményei egyértelműen igazolják, hogy a távmunka elterjedése jelentős kihívásokat teremtett a munkahelyi biztonság és adatvédelem terén. A válaszadók több mint 60%-a rendszeresen végez távmunkát, többségük otthoni környezetben, ahol a munkáltatók által biztosított biztonsági mechanizmusok nem mindig elegendőek a kockázatok hatékony kezelésére. A kutatás eredményei arra utalnak, hogy a kisebb vállalatoknál az adatbiztonsági incidensek előfordulási aránya magasabb (25%), míg a nagyobb vállalatoknál ez lényegesen alacsonyabb (6%), ami összefüggésben állhat az IT biztonsági oktatás eltérő szintjeivel és a védelmi intézkedések különbözőségével.

A távmunka során észlelt legnagyobb kockázatok közé az adatszivárgás, az azonosító adatok kompromittálódása és a hálózati támadások tartoznak, amelyek különösen veszélyesek azok számára, akik nem megfelelően védett hálózatokon keresztül dolgoznak. Bár számos munkáltató biztosít alapvető védelmi mechanizmusokat, például VPN-t és kétfaktoros hitelesítést, az IT biztonsági oktatás még nem ér el minden dolgozót, ami csökkentheti a védelmi intézkedések hatékonyságát. A kutatás eredményei azt mutatják, hogy a kisebb cégeknél a kibervédelmi tudatosság növelése kulcsfontosságú, míg a nagyobb szervezetek esetében a meglévő védelmi stratégiák folyamatos fejlesztésére van szükség.

Az alábbi javaslataim vannak a távmunka biztonságának növelésére:

- IT biztonsági oktatás és tudatosság növelése: Az alkalmazottak folyamatos képzése elengedhetetlen annak érdekében, hogy tisztában legyenek az adatbiztonsági kockázatokkal és a megfelelő védekezési módszerekkel. A rendszeres kibervédelmi tréningek bevezetése segítheti a munkavállalókat a fenyegetések felismerésében és a megfelelő biztonsági gyakorlatok alkalmazásában.
- Kibervédelmi intézkedések fejlesztése: A vállalatoknak érdemes átfogó biztonsági stratégiát kialakítaniuk, amely magában foglalja a VPN-használat kiterjesztését, a kétfaktoros hitelesítés alkalmazását minden távoli belépés esetén, valamint a munkahelyi eszközök és szoftverek titkosítását. Az endpoint security és a folyamatos monitorozás segíthet a potenciális fenyegetések gyors észlelésében és kezelésében.
- Otthoni és nyilvános hálózatok biztonságának erősítése: A kutatás kimutatta, hogy a munkavállalók szoktak kevésbé védett hálózatokon dolgozik, ezért kiemelten fontos az otthoni Wi-Fi hálózatok megfelelő védelme, például erős jelszavak, tűzfalak és biztonságos routerbeállítások alkalmazásával. A vállalatoknak biztosítaniuk kell azokat az eszközöket és útmutatókat, amelyekkel a távmunkát végzők saját otthoni környezetük biztonságát növelhetik.
- Biztonságos céges eszközök és szoftverek biztosítása: A munkahelyi eszközök és a vállalati adatkezelés elkülönítése érdekében célszerű a munkáltatóknak olyan eszközöket biztosítaniuk, amelyeken előre konfigurált biztonsági beállítások és ellenőrzött szoftverek futnak. Az árnyékinformatika (shadow IT) kiküszöbölése érdekében érdemes belső szabályzatokat bevezetni az engedélyezett alkalmazások és hardverek használatára vonatkozóan.

- Hitelesítési és titkosítási megoldások kiterjesztése: Az érzékeny adatok védelme érdekében a vállalatoknak olyan titkosítási technológiákat kell alkalmazniuk, amelyek biztosítják az adatok sértetlenségét és illetéktelen hozzáférés elleni védelmét. A biometrikus azonosítás, hardveres biztonsági kulcsok és fejlett titkosítási protokollok bevezetése hatékony védelmet nyújthat.
- Munkáltatói szabályozás és irányelvek frissítése: A távmunka biztonsági kockázatainak kezelése érdekében a vállalatoknak naprakész belső szabályzatokat kell kidolgozniuk, amelyek egyértelmű iránymutatást adnak a munkavállalóknak a biztonságos munkavégzésre vonatkozóan. Ezeknek az irányelveknek tartalmazniuk kell a távoli munkavégzés során elvárt magatartásformákat, az eszközhasználatra vonatkozó előírásokat, valamint az adatkezelési és incidensjelentési protokollokat.

A kutatás eredményei alapján megállapítható, hogy a távmunka biztonságának növelése egy komplex, többszintű megközelítést igényel, amely ötvözi a technológiai védekezési megoldásokat, a munkavállalók képzését és a szabályozási keretek fejlesztését. A jövőbeli kutatások fókuszálhatnak a kibervédelmi technológiák hatékonyságának elemzésére, valamint a munkavállalók és munkáltatók biztonságtudatosságának hosszú távú alakulására. A megfelelő biztonsági protokollok bevezetésével és folyamatos fejlesztésével biztosítható, hogy a távmunka hosszú távon is fenntartható és biztonságos legyen mind a munkáltatók, mind a munkavállalók számára.

ÖSZEFOGLALÁS

A tanulmány a távmunka elterjedésével kapcsolatos biztonsági kihívásokat vizsgálja, különös tekintettel az adatvédelemre, a kibervédelemre és a munkavállalók biztonságtudatosságára. A kutatás kérdőíves módszert alkalmazott, amely kvantitatív adatokat szolgáltatott a távoli munkavégzés gyakoriságáról, a használt technológiai megoldásokról és a vállalatok által biztosított védelmi intézkedésekről.

Az eredmények rámutatnak arra, hogy a távmunkát végző munkavállalók jelentős része otthonról dolgozik, azonban a biztonsági kockázatok és a védelmi intézkedések alkalmazása szervezeti mérettől függően eltérő. A kisebb vállalatoknál az adatbiztonsági incidensek aránya magasabb, míg a nagyobb cégek hatékonyabb védelmi stratégiákat alkalmaznak, például VPN-t, kétfaktoros hitelesítést és rendszeres IT biztonsági oktatásokat. A legnagyobb biztonsági fenyegetések közé az adatszivárgás, az azonosító adatok kompromittálódása és a hálózati támadások tartoznak, amelyek a távoli munkavégzés során kiemelt figyelmet igényelnek.

A tanulmány kiemeli, hogy a távmunka biztonságának növelése érdekében szükség van az IT biztonsági tudatosság fejlesztésére, az adatvédelmi intézkedések egységesítésére és a munkáltatói szabályozások frissítésére. A kutatás eredményei alapján javasolt lépések közé tartozik az IT biztonsági képzések elérhetővé tétele, az otthoni hálózatok védelmének megerősítése, a munkáltatók által biztosított céges eszközök és szoftverek alkalmazása, valamint a hitelesítési és titkosítási technológiák szélesebb körű bevezetése.

Összességében a kutatás arra hívja fel a figyelmet, hogy a távmunka biztonságos és fenntartható működéséhez átfogó stratégia szükséges, amely ötvözi a technológiai védekezési intézkedéseket, a munkavállalói tudatosság növelését és a szervezeti szabályozás fejlesztését. Az eredmények hozzájárulhatnak a vállalatok adatbiztonsági politikájának kialakításához és a távmunka hosszú távú fenntarthatóságának biztosításához.

FELHASZNÁLT IRODALOM

[1] Cs. Kollár and J. Poór, „Organisations in Digital Age - Information Security Aspects of Digital Workplaces," Management, Enterprise and Benchmarking in the 21st Century, pp. 73-82, 2016.

[2] K. Tardos, Esélyegyenlőség és családbarát vállalati gyakorlatok, mtd Tanácsadói Közösség, Budapest: mtd Tanácsadói Közösség; MTA Társadalomtudományi Kutatóközpont, Szociológiai Intézet, 2014.

[3] T. Venczel-Szakó, G. Balogh and I. Borgulya „Távmunka, home office: hogyan érinti a távolról dolgozás a szervezet intern kommunikációját?," Vezetéstudomány - Budapest Management Review, vol. 52, no. 2, pp. 73-86, 2021.

[4] K. Lazányi and Y. Bilan, „Generation Z on the labour market: do they trust others within their workplace?," Polish Journal of Management Studies, pp. 78-93, vol. 16, no. 1 2017.

[5] Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség (EU-OSHA), „Távmunka a COVID-19-világjárvány idején: kockázatok és megelőzési stratégiák," EU-OSHA jelentés, 2021.

[6] Á. Jarjabka, G. Kuráth, N. Sipos, T. Venczel-Szakó, B. Szabó-Bálint, G. balogh and A. Uhrin, „Rugalmasság, produktivitás vagy elszigeteltség? Avagy a COVID-19 hatása a felsőoktatásban oktatók munkavégzésére," Magyar Tudomány, vol. 181, no.12. pp. 1698-1710, 2020.

[7] F. Pataki-Bittó and Á. Kun, „Exploring differences in the subjective will-being of teleworkers prior to and during the pandemic," International Journal of Workplace Health Management, vol. 15, no. 3, pp. 320-338, 2022.

[8] A. Nagy and T. Z. Wentzel Antal, „A távmunka dogmatikai problémái az elméletben és a gyakorlatban - A távmunka fogalmának megreformálására tett kísérlet," Munkajog, vol. 2024, no. 1, pp. 44-54, 2024.

[9] E. Törő and G. Károlyi, „A távmunkavégzés új szabályai, különös tekintettel a munkavédelmi előírásokra," Munkajog, vol. 2022, no. 2, pp. 15-27, 2022.

[10] T. Forgács, A távmunka elmélete és gyakorlati alkalmazásának lehetőségei, Pécsi Tudományegyetem, 2009.

[11] Nemzeti Kibervédelmi Intézet (NKI), Újragondolt IT biztonsági kockázatelemzés a távmunka viszonylatában, Budapest: (NKI), Nemzeti Kibervédelmi Intézet, 2019.

[12] Nemzeti Kibervédelmi Intézet (NKI), Otthoni munkavégzés és utazás – adatbiztonság a munkahelyen kívül, Budapest: (NKI), Nemzeti Kibervédelmi Intézet, 2019.

[13] A. Beláz, "A magyar kibervédelmi szabályozás továbbfejlesztésének lehetőségei – Különös tekintettel a stratégiaalkotásra", Budapest: Nemzeti Közszolgálati Egyetem, 2017.

[14] A. Lukács, „A távmunka során felmerülő sajátos adatvédelmi kérdések," Szegedi Tudományegyetem, Szeged, 2013.

[15] K. László, „A távmunka és távoli hozzáférés IT biztonsági követelményei – az MNB 12/2020 (XI.6.) számú ajánlása," Hétpecsét Információbiztonsági Egyesület, Budapest, 2020.

[16] P. J. Horváth, É. S. Somossy and T. Tóth, „A decentralizált villamosenergia-rendszerek fejlődésének nemzetközi és hazai szempontjai,” Közgazdasági Szemle,vol. 69, no. 6, pp. 697–720, 2022.

[17] I. Székely and Gy. Vasvári, „Adatvédelem és/vagy adatbiztonság?,” Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest, 2004.

[18] V. Honfi and Z. Illési, „COVID-19, Home Office, Cybersecurity,” Journal of Cybersecurity, 2020.

[19] B. R. Barna, Cs. Kollár and E.D. Oroszi, „A social engineering helye az információbiztonsági auditban,” Biztonságtudományi Szemle, p. 25–41, 2023.

[20] Cs. Krasznay and G. Gyebnár, „Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems,” *Proceedings of the 13th International Conference on Cyber Conflict (CyCon)*, p. 171–188, 2021.

[21] A. Faludi and L. Szabó, „Villamosenergia-rendszer üzeme és irányítása,” Budapesti Műszaki és Gazdaságtudományi Egyetem (BME), Budapest, 2002.

DOI: https://doi.org/10.12700/btsz.2025.7.2.147

ECONOMIC ASPECTS OF FIRE PROTECTION IN A MULTINATIONAL ENVIRONMENT

TŰZVÉDELEM GAZDASÁGI VONATKOZÁSAI MULTINACIONÁLIS KÖRNYEZETBEN

KREPUSKA András István[1] – NAGY Rudolf[2]

Abstract

Business organizations and especially manufacturing companies partially or fully are required to comply with the fire projection standards. Both during the built of the building, both during the maintenance of the building the current requirements must have to be held. In our qualitative research we examined the operation methods of fire protection at manufacturing companies. We paid special attention on the aging of the installed fire protection equipment, and the amortization caused by the improper use of the equipment. We compared the budget of the fire protection equipment, the budget of the manufacturing equipment, and the price income of the company. We represent the lack of production in case of an incidental fire.

Keywords

fire protection, fire projection standard, amortization, budget, lack of production

Absztrakt

Gazdálkodó szervezetek és azon belül is a gyártást végző vállalatok ingatlanjai részben vagy egészben kötelezettek tűzvédelmi előírások betartására. Mind az épület építése során mind az üzemeltetés során az építéskor érvényes követelményeket be kell tartani. Kvalitatív kutatásunkban termelőtevékenységet végző társaságok tűzvédelmi üzemeltetéssel kapcsolatos gyakorlatát vizsgáltuk meg. Külön figyelmet fordítottunk a telepített tűzvédelmi berendezések öregedésére, illetve üzemeltetési hibából adódó amortizációjára. Összehasonlításokat végeztünk a tűzvédelmi berendezések költsége, a termelőeszközök költsége és az árbevétel között. Bemutatjuk egy esetleges tűzeset miatt keletkező termeléskiesést.

Kulcsszavak

tűzvédelem, tűzvédelmi előírás, amortizáció, költség, termeléskiesés

[1] andras.krepuska@zknet.hu | ORCID: 0000-0002-1857-6740 |CEO and leader designer at ZKNet Kft., Budapest, Hungary | ZKNet Kft ügyvezető, vezető tervező, Budapest, Magyarország

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

BEVEZETÉS

Az építményeknek a tűz elleni védekezését és egy kialakult tűz hatásainak korlátozását az építmény passzív és aktív tűzvédelmi berendezéseivel tudjuk biztosítani. A jelenleg is érvényes 1996. évi XXXI. törvény a tűz elleni védekezésről meghatározza a tűz elleni védekezés és a tűzvédelem fogalmát, és kimondja, hogy magánszemélyeknek és gazdálkodó tevékenységet folytató természetes vagy jogi személyeknek is szükséges biztosítani a tulajdonukban lévő ingatlanok és ingóságok, valamint termelőeszközök tűzvédelmi követelményeinek betartását, illetve ezen követelmények ellenőrzésének lehetőségét. [1]

A tűzvédelmi eszközök, illetve berendezések üzemben tartásának szükségessége visszamenőleg is érvényes. A berendezéseket a telepítéskori jogszabályok által megkövetelt szinten és működőképes állapotban kell tartani. A tűzvédelmi törvény nem mondja ki, hogy a tűzvédelmi rendszereknek élettartammal kapcsolatos amortizációjával tervezni szükséges és nem ír elő időtartamhoz kapcsolódó kötelező cserét. Egyes rendszerek részeinek cseréje hazai vagy nemzetközi szabályozás alapján azonban alkalmanként vagy időszakonként szükségessé válhat. Ilyen rendszer komponens csere lehet például a gázzal oltó rendszerek tartályainak nyomástartási vizsgálatából adódó cseréje abban az esetben, ha a tartály a nyomáspróbán további használatra alkalmatlannak bizonyul. [2] Szintén rendszer komponens cseréjének minősül a habbaloltó rendszerek oltóhab koncentrátumának cseréje abban az esetben, ha PFOS vagy PFOA tartalma kimutatható. [3] Az épületek tűzvédelmét teljes életciklusukban szükséges vizsgálni, hogy az elvárt tűzvédelmi szint mindig biztosítható legyen. [4]

Kutatásunk során gazdálkodó szervezetek tűzvédelmi rendszereinek amortizációját vizsgáljuk és ezeknek a rendszereknek a gazdálkodó szervezet tevékenységére gyakorolt lehetséges hatását.

A KUTATÁSI MÓDSZER BEMUTATÁSA

A kutatással alapvető célunk bemutatni, hogy egy multinacionális ipari környezetben megvalósított tűzvédelem a létesítménynek egy olyan része, aminek kialakításának és fenntartásának költségei elenyésző mértékűek a létesítmény egyéb költségekhez és a termelő vállalt bevételeihez mérten. A tűzvédelemre, mint „kötelező rossz” kiadásra tekintenek. Felvetésünk, hogy az évek múlásával a minimálisan megkövetelt szinten karbantartott és üzemeltetett rendszerek sérülékennyé válnak. Kvalitatív kutatásunk során multinacionális ipari termelő cégek bevételeit és kiadásait vizsgáltuk meg a tűzvédelem szemszögéből. A kutatáshoz mélyinterjúkat készítettünk, valamint a helyszíneken végeztünk feltáró jellegű állapot és adatrögzítéseket.

A VIZSGÁLT SZERVEZETEK ISMERTETÉSE

Kutatásunk során három különböző méretű és tevékenységű gazdálkodó szervezeteket vizsgáltunk. A gazdálkodó szervezetek méret alapján közép és nagyvállalkozások multinacionális hátérrel. Az összes vizsgált társaságra igaz, hogy:

- üzemeltetnek ingatlant, ahol gazdasági tevékenység folyik
- ingatlanok rendelkeznek aktív és passzív tűzvédelmi rendszerekkel

Tevékenységük alapján több műszakos gyártás zajlik. A nettó éves árbevétel 2022-es nyilvános adatok alapján 32.9 Mrd Ft és 97.8 Mrd Ft között alakult.

A társaságok kérésének megfelelően sem nevet, sem a beazonosításhoz felhasználható adatokat nem közölhetünk.

Tevékenység	Társaság I	Társaság II	Társaság III
	Speciális oldószer gyártás	Műanyag granulátum gyártás	Autó alkatrész gyártás
Nettó árbevétel 2022 (Mrd Ft)	32.9	97.8	56.2
Vizsgált tűzszakasz mérete (m^2)	1990	2850	41500
A vizsgált tűzszakaszban készített termék százalékos megoszlása az összes termékhez képest	~70%	100%	100%
A vizsgált tűzszakaszban készített termék százalékos megoszlása a teljes termeléshez képest	~56%	~65%	100%
Beépített tűzjelző rendszer	van	van	van
Beépített tűzoltó rendszer	nincs	van	van
Hő és füstelvezetés	van, gépesített	van, gravitációs	van, gravitációs
Tűzszakasz tűzvédelmi határolásai	TvMI 1.4:2020.07.20 szerint	TvMI 1.1:2015.03.05 szerint	nem megfeleltethető TvMI alapján

1. Táblázat: Társaságok alapadatainak ismertetése, saját szerkesztés

A VIZSGÁLT ÉPÍTMÉNYEK BEMUTATÁSA

A társaságok üzemeltetett ingatlanjai vasbeton szerkezettel megvalósított szendvicspanel falazatú egy és többszintes építmények. Az építmények telepítése szerint 1996 és 2022 közöttiek. Az építmények tűzvédelmi követelményei a 35/1996. (XII. 29.) BM rendelettel kiadott OTSZ és az 54/2014 (XII.5) BM rendelettel kiadott OTSZ alapján kerültek

meghatározásra. Az építmények jelentős korkülönbsége miatt egy épületen belül egy tűzszakaszra koncentráltan végeztük a vizsgálatokat. *A tűzszakasz: az épület, a speciális építmény, a szabadtéri tárolóterület meghatározott része, amelyet a szomszédos építmény- és térrésztől tűzterjedés ellen védetten alakítanak ki.* [5]

A vizsgálat mérete egybevág az 54/2014 (XII.5) OTSZ rendelkezéseivel is, mert az építmények tűzvédelmi berendezéseinek tervezése során a tűzvédelmi tervezés kiindulási feltételei, hogy az építmény tűzvédelmi megoldásait egyidejűleg egyetlen, az építmény tetszőleges pontján keletkező tűz károsító hatásainak figyelembevételével kell tervezni és méretezni.

Az objektumok telekhatáron mechanikai védelemmel rendelkeznek, az élőerős őrzés mind a három gyár esetében 0-24h-ban biztosított. A tűzjelző központok vagy másodkezelők az őrség mellet kerültek elhelyezésre. A tűzjelző rendszer felügyelete elsősorban éklőerővel biztosított. Kettő gyárban tűzoltósági átjelzés üzemel, egy gyárban a tűzoltóság értesítése telefonon történik.

A gyárak nem rendelkeznek létesítményi tűzoltósággal.

TÁRSASÁGOK TŰZVÉDELMI HELYZETÉNEK ÁTTEKINTÉSE

A gyárakban az aktív tűzvédelmi berendezések kapcsán megtalálható tűzjelző rendszer. A jelenleg használatos modern tűzjelző rendszerek közös ismertetője, hogy címzett kivitelű és intelligens rendszerek. Ez azt jelenti, hogy minden egyes tűzjelző rendszerelem saját egyedi azonosítóval rendelkezik és az eszközök állapotainak felügyelete és megjelenítése valós időben és folyamatosan történik. A tűzjelző berendezések nagy biztonságot nyújtó rendszerek, amik a jogszabályi környezet és a gyártói előírások keretein belül képesek üzemelni. [6]

Az I. és II.sz gyárakban jogszabályi kötelezés alapján épült ki tűzjelző rendszer, a III.sz gyárban építéskor beruházói belső előírás alapján létesült, majd folyamatosan fejlesztésre került. A vizsgálat időpontjában mind a három üzemben címzett kivitelű intelligens tűzjelző rendszer üzemel. A II. és III.sz gyárakban beépített oltóberendezés azon belül is sprinkler rendszerű automata vízzeloltó berendezés létesült. Alkalmas arra, hogy a védett térben kialakuló tüzet a tervezéskor meghatározott védőfelületen kontrollálja a tervezett üzemidő alatt. [7] A sprinkler rendszerek tűz kontrollra történő tervezése jelentős alapelv béli különbség a gázzal oltó rendszerekhez képest, ahol a sikeres oltásra kell méretezni a rendszert. [8]

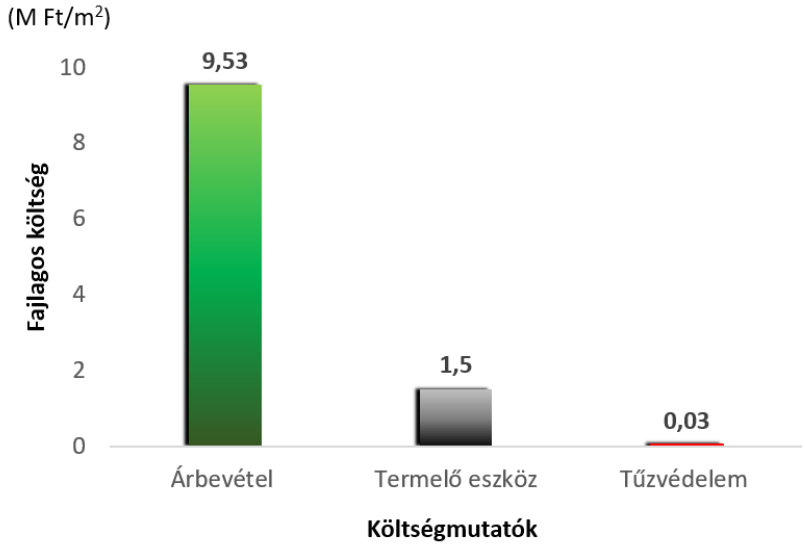
A vizsgált tűzszakaszok határolása téglafallal, illetve szendvicspanellel történik. A téglafal és a tető kapcsolata az I. és II. számú gyárak esetében megfeleltethető tűzvédelmi műszaki irányelv ajánlásainak. Az I. számú társaságnál gépesített hő és füstelvezetés valósult meg, míg a II. és III. sz társaságoknál gravitációs módon történik a hő és füstelvezetés. A hő és füstelvezetés állapota a tűzjelző rendszeren csak a II.sz társaságnál jelenik meg. A jelenleg érvényes hő és füstelvezetéssel kapcsolatos TvMI új telepítésű HFR rendszerek esetében követeli meg a rendszerek állapotának megjelenítését [9] Az I.sz gyár esetében a HFR rendszer nem ad hiba átjelzést a tűzjelző rendszerre. A II.sz gyár HFR rendszere két irányú kapcsolatban áll a tűzjelző rendszerrel, míg a III.sz gyár HFR rendszere csak kézi működtetésű, a tűzjelző rendszertől független.

KÖLTSÉGADATOK A TŰZVÉDELEM ÖSSZEVETÉSÉBEN

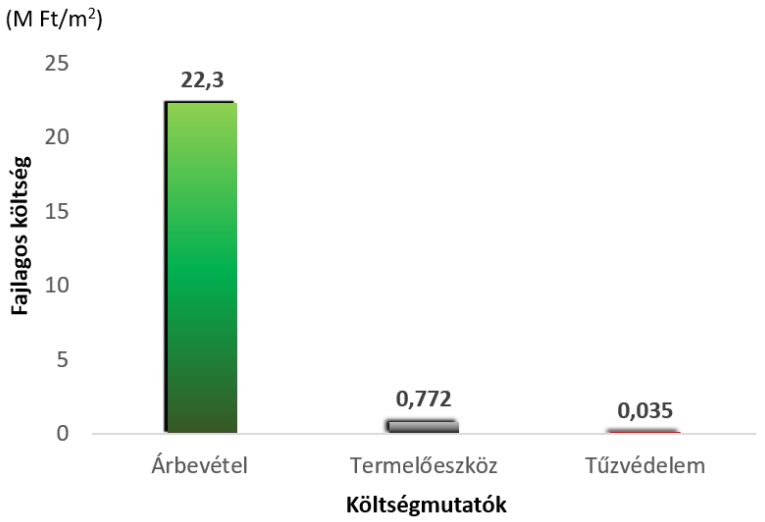
A társaságokról általánosan elmondható, hogy megrendelésre termelnek ezáltal hosszú távú késztermék felhalmozás nem történik. A 2022-es évben elért árbevétel a 2022-es gyártási kapacitást és vevői megrendeléseket tükrözik. A 2022-es évre vonatkozólag 254 munkanap van nyilvántartva.

Gazdasági mutatók	Társaság		
	I.	II.	III.
Egy munkanapra vetített árbevétel (M Ft)	129,53	358,03	221,25
Vizsgált tűzszakaszban alkalmazott termelőeszközök megközelítő költsége (M Ft)	~3000	~2200	~110000
Vizsgált tűzszakasz mérete (m^2)	1990	2850	41500
A vizsgált tűzszakaszban m^2-re eső termelőeszközök megközelítő költsége (M Ft)	~1,5	0,772	~2,65
A vizsgált tűzszakaszban végzett termelési tevékenység m^2-re eső árbevétele (M Ft)	~9,53	~22,3	~1,35
A vizsgált tűzszakaszban telepített aktív tűzvédelem bekerülési költsége (M Ft)	~60	~100	~280
A vizsgált tűzszakaszban telepített aktív tűzvédelem megközelítő bekerülési költsége egy m^2-re vetítve (M Ft)	~0,03	~0,035	~0,007

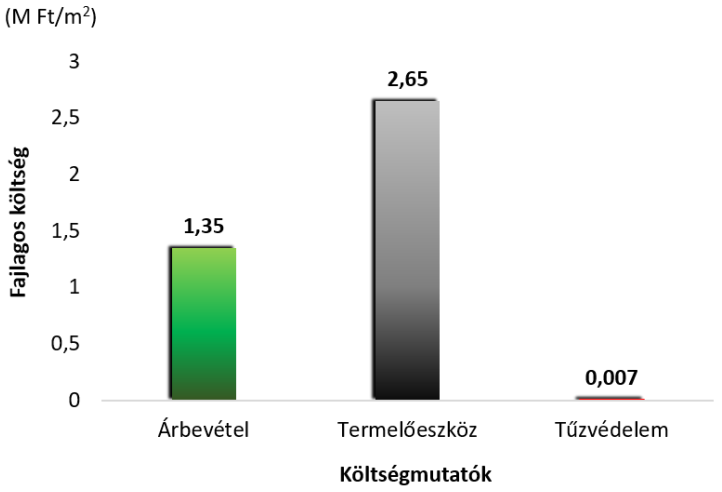
2. Táblázat: Az egy négyzetméterre eső bevételek és költségek bemutatása, saját szerkesztés



1. Ábra: Társaság I egy négyzetméterre eső bevételek és költségek ábrázolása, saját szerkesztés



2. Ábra: Társaság II egy négyzetméterre eső bevételek és költségek ábrázolása, saját szerkesztés



3. Ábra: Társaság III egy négyzetméterre eső bevételek és költségek ábrázolása, saját szerkesztés

TŰZBIZTONSÁG ISMÉRVEINEK ELEMZÉSE

A társaságok részéről szolgáltatok adatok mellett a vizsgált tűzszakaszok feltáró vizsgálata során számos az alkalmazott tűzvédelmet negatívan érintő átalakítást tártunk fel. Mind a három társaságnál megfigyelhető, hogy a termelés átalakításakor a tűzvédelem vagy nem lett módosítva, vagy nem lett megfelelően módosítva a megváltozott tűzvédelmi veszélyekhez. A feltárt hiányosságok rögzítését követően a társaságokkal egy második interjú készült, ami egy lehetséges bekövetkező káresemény hatását vizsgálja a termelésre vonatkozólag.

Társaság I. feltáró vizsgálata során rögzített adatok:

A technológia bővítésnek telepítése során keletkező füst éles riasztást generált a tűzjelző rendszerben. A riasztások miatt a terület tűzjelző rendszere többször is lekapcsolásra kerül. A többszöri hamis riasztás miatt a munkát végző személyzet nem veszi kellő komolysággal a tűzjelzést. A keletkezett füst miatt több érzékelő cseréje vált szükségessé.

A tűzszakaszokon átmenő technológiai vezetékek miatt oldalfalak és födémek lettek átfúrva, amelyek szakszerű tűzgátló visszajavítása nem történt meg.

A tűzszakasz HFR berendezésének tervezésekor nem lett figyelembevéve a várható telítettsége a légtérnek. Füstpróbával szimulálva bizonyítható, hogy a technológia akadályozza a megfelelő légáramot

A technológiai csővezeték építésekor a már meglévő csővezeték megsérült, a csövekből kijutó oldószer fizikailag károsította a csővezeték alatt telepített tűzjelző nyomvonalat és érzékelőt.

A technológia bővítésekor egy robbanásveszélyes tér kialakítása is történt. A zónabesorolás alapján a robbanásveszélyes terület nem terjed ki a termelés többi részére, viszont a nem megfelelően kialakított átvezetéseknél zónakiterjedés jön létre. A zóna kiterjedése a nem robbanásbiztos kivitelű tűzjelző hálózatra is hatással van.

Társaság I. második interjú során rögzített adatok:

Társaság I. termelési eszközei egyedileg készülnek megrendelésre. A jelenleg használt technológia telepítése folyamatosan zajlott a felmérést megelőző 24 hónapban, úgy, hogy az alkalmazott rendszerek szállítása folyamatosan történik. Az I.sz társaságnak nincs más országban ilyen jellegű termelési tevékenysége ezért tartalékberendezések áttelepítése nem lehetséges.

A teljes termelő tűzszakaszban fellépő tűzkár esetén a termeléskiesésből adódó kár várható maximális mértéke ~ 36,84 Mrd forint, a berendezések mai áron számított kár értéke ~6 Mrd forint. A várható kár összesített összege egy négyzetméterre vetítve ~ 21,57 millió forint.

Az I.sz társaság esetében anyagi kárral járó tűzeset még nem történt. A technológia folyamatos telepítéséből adódóan az alkalmazott tűzvédelem több ponton is amortizálódik.

Társaság II. feltáró vizsgálata során rögzített adatok:

A technológia telepítése miatt keletkező füst éles riasztást generált a tűzjelző rendszerben. A riasztások miatt a terület tűzjelző rendszere többször is lekapcsolásra kerül. A többszöri hamis riasztás miatt a munkát végző személyzet nem veszi kellő komolysággal a tűzjelzést. A keletkezett füst, valamint a technológiához felhasznált porok miatt több érzékelő cseréje szükséges folyamatosan.

A gyártósorok okozta szennyeződés miatt időszakonként gőzborotvás takarítást végeznek. A takarítás során több alkalommal is sérültek kézi jelzésadók.

Egy új gyártósor telepítésekor kialakított erősáramú kábeltálca nyomvonal kapcsolóhelyiségen történő átvezetése nem lett szakszerűen tömítve. A technológia üzemszerű füstképződése a kapcsolóhelyiség gázzaloltó rendszerét már több alkalommal is aktiválta. A gázzaloltót sikerült az oltási folyamat előtt deaktiválni, viszont az oltórendszert későbbeikben csak kézi aktiválással üzemeltették.

Társaság II. termelési eszközei egyedileg készülnek megrendelésre. A jelenleg használt technológia több gyárukban is használatos, a gyárakban rendszeresített technológiai sablonterv szerint kerülnek legyártásra és összeszerelésre. A kapott információk alapján egy gyártósor pótlása megközelítőleg két hónap alatt valósulhat meg a meglévő tartalék alkatrészek segítségével. A teljes gyártási kapacitás pótlása megközelítőleg egy éven belül kivitelezhető. A vizsgált tűzszakaszban nedves sprinkler oltóberendezés került telepítésre, a tervezéskor megállapított legkedvezőtlenebb védőfelület 260m2.

Egy esetleges tűz során a sprinkler rendszer aktiválódása a teljes fedő felületen kontrollálni képes a kialakult tüzet, az tovább nem terjed. Ebben az esetben az egy m2-re vetített termelés kiesés ~22,3 millió forint. A védőfelületre vetített termelés kiesés mértéke ~ 0,5798 Mrd forint. A termelőeszközök tekintetében egy gyártósor helyigénye alacsonyabb, mint az aktiválódó fedő felület mérete. A megadott adatok alapján így a termelőeszközökben keletkező kár mértéke maximálisan ~200,694 millió forint. A várható kár összesített értéke egy m2-re vetítve ~3,0019 millió forint, ahol a sprinkler rendszer védőfelületét vesszük alapul.

A II. sz társaság vizsgált tűzszakaszában már történt olyan tűzeset, ahol a sprinkler rendszer aktiválódott. A gyártósor felett elhelyezett sprinkler védelemből egy darab sprinklerfej aktiválódott és sikeresen kontrollálta a tüzet. A gyártósor javítása még aznap megtörtént, raktáron lévő tartalék eszközökkel lehetett a hibát orvosolni.

Társaság III. feltáró vizsgálata során rögzített adatok:

A gyártási folyamat részeként használatos préselési technológia folyamatos tűzveszélyt jelent. Ezt a technológiát nem tudja a gyártó jelenleg kizárni a gyártási körből. A kockázat miatt a technológia telepítésekor CO_2 gázzaloltó rendszer lett telepítve az elszívó rendszer védelmére. Az elszívó rendszer folyamatos időszakos takarítást igényelne a lerakódó szennyezett olaj miatt, ez viszont nem történik meg kellő rendszereséggel. Az elmúlt években több tűzesetet is a technológiai elszívás begyulladása okozta.

Társaság III. termelési eszközei részben egyedileg kerülnek legyártásra, részben általánosan használatos gyártó gépek. A kapott információk alapján a teljes gyártási ciklus két párhuzamosan felépített gyártósoron valósul meg, ahol az egymást követő gépek a gyártmány egy következő állapotának előállításáért felelősek. Egy soron egy gép meghibásodása elviekben a gyártási ciklus megállásához vezethet. Ez az anyaggazdálkodással, illetve a párhuzamosan üzemelő gyártósorra történő kapacitás átterheléssel részben kiküszöbölhető. A vizsgált tűzszakaszban nedves sprinkler oltóberendezés került telepítésre, a tervezéskor megállapított legkedvezőtlenebb védőfelület 260m2.

Egy esetleges tűz során a sprinkler rendszer aktiválódása a teljes fedő felületen kontrollálni képes a kialakult tüzet, az tovább nem terjed. Ebben az esetben az egy m2-re vetített termelés kiesés ~1,35 millió forint. A védőfelületre vetített termelés kiesés mértéke ~ 0,351 Mrd forint. A megadott adatok alapján így a termelőeszközökben keletkező kár mértéke maximálisan ~0,676 Mrd forint. A várható kár összesített értéke egy m2-re vetítve ~3,95 millió forint, ahol a sprinkler rendszer védőfelületét vesszük alapul.

A III. sz társaság vizsgált tűzszakaszában már történt olyan tűzeset, ahol a sprinkler rendszer teljes védőfelületén aktiválódott. A kialakult tűz elsődlegesen a tetőt károsította az éghető szigetelés miatt. A sprinkler védelem a technológiát sikeresen megvédte.

KONKLÚZIÓ

Kutatásunk során kvalitatív módon vizsgáltuk meg három ipari termelő vállalt egy-egy tűzszakaszának tűzvédelmét és a tűzszakaszban történő gazdasági tevékenységet. A vizsgált tűzszakaszokban a társaságok éves árbevételét adó késztermékek nagy százaléka készül. Megállapítottuk, hogy a területeke védelmére telepített aktív tűzvédelmi rendszer költsége jelentősen alulmarad mind a telepített technológia, mind a késztermék területre vonatkoztatott költségéhez képest.

Feltáró jellegű vizsgálatokat folytattunk a helyszíneken és a kapott eredmények alapján egy második interjút készítettünk. Az interjú során a már feltárt hiányosságok fényében vizsgáltuk egy esetleges tűzeset hatásait a termelésre. Számszerűsítettük, hogy milyen jellegű bevétel kiesések prognosztizálhatóak. Minden esetben elmondható, hogy a termelésben használt technológia pótlása még a legjobb esetben is több hónapos termeléskiesést okoz. A vizsgált társaságok nincsenek felkészülve egy nagy mértékű tűzesetet követő gyors helyreállítási munkára.

Kettő társaságnál a beépített oltórendszer igazolt módon a kialakult tűz terjedését sikeresen kontrollálta és elősegítette az oltást. Egy társaság esetében a technológiára szerelt oltórendszernek átlagosan 7 havonta be kell avatkoznia a kialakuló tűz oltásához.

Megállapítottuk, hogy a tűzjelző rendszerek tervezése során a felhasznált technológia okozta szennyeződések, illetve hatások nem lettek kalkulálva az érzékelők kiválasztásánál. Ennek a hiánya későbbiekben jelentősen növeli a téves jelzések számát. A magas számú téves jelzés, az emberi reakció időt növeli.

Az épületek építésekor alkalmazott építészeti tűzvédelmi megoldások tervezésekor nem lettek a későbbi technológiai fejlesztési szükségletek kalkulálva. A gyártási kapacitás növelése egyértelműen károsítja a passzív és aktív tűzvédelem hatékonyságát. Csökken a sértetlen falfelületek mérete, a tűzgátló falátvezetések nincsenek megfelelően helyreállítva. A falátvezetések számának növekedésével nő a hibalehetőségek száma is. A hő és füstelvezető rendszerek hatékonyságát nagyban rontja a légtérben telepített technológiai csővezetékek és tartószerkezetük. A megnövekedett számú technológia több karbantartási munkát igényelne, aminek hiányából adódóan megnő a tűzkockázat és tűzeset is alakult ki.

További kutatási irányként jelöljük meg az épületek aktív és passzív tűzvédelmének élettartam szintű változáskövetés szükségességét a felhasznált technológia változásának szemszögéből.

FELHASZNÁLT IRODALOM

[1] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

[2] 213/2019. (VIII. 27.) Korm. rendelet a nyomástartó berendezések, rendszerek és létesítmények műszaki-biztonsági hatósági felügyeletéről

[3] 376/2020. (VII. 30.) Korm. rendelet a környezetben tartósan megmaradó szerves szennyező anyagokról szóló, 2019. június 20-i (EU) 2019/1021 európai parlamenti és a tanácsi rendelet végrehajtásával kapcsolatos egyes rendelkezésekről

[4] Somogyi T., Bérczi L., Hatékony és komplex tűzvédelem létfontosságú rendszerek és létesítmények esetében. Védelem Tudomány – VII. évf., (3), (2022) 47-63.

[5] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról, https://mabisz.hu/tajekoztato-a-vagyon-es-muszaki-biztositasokrol/
[6] Mohai Á., A tűzjelző berendezések típusainak megnevezése. Hadmérnök, X. évf. (3), (2015) 32-42.
[7] K. Frank, , N.Gravestock, M. Spearpoint, et al. A review of sprinkler system effectiveness studies. Fire Sci Rev 2, 6 (2013). https://doi.org/10.1186/2193-0414-2-6
[8] MSZ EN 15004-1:2019 - Beépített tűzoltó berendezések. Gázzal oltó berendezések. 1. rész: Tervezés, kivitelezés és karbantartás
[9] Krepuska A., Nagy R., A hő- és füstelvezető rendszerek vezérlésének sajátosságai. Védelem tudomány: Katasztrófavédelmi online tudományos folyóirat, VIII. évf., (1), (2023) 25-46.,

DOI: https://doi.org/10.12700/btsz.2025.7.2.157

STUDY OF THE IMPACT OF DIFFERENT FIRE OPERATING CONDITIONS ON THE PUBLIC WATER SUPPLY FOR FIREFIGHTING

ELTÉRŐ TŰZESETI ÜZEMÁLLAPOTOK KIHATÁSÁNAK VIZSGÁLATA A VEZETÉKES OLTÓVÍZ--ELLÁTÁSRA

NAGY Rudolf[1]

Abstract

Fire prevention is a series of solutions to protect life and property from the ravages of an outbreak of flames. The use of modern technology and engineering in fire protection has made today's environment much safer. However, given the fact that the threat of fire has not yet been completely eliminated, and that we cannot completely eliminate combustible materials or the causes of fires from our lives, we must always face up to all remaining fire risks. We must therefore be prepared for the outbreak of fire, the burden of which we obviously cannot place on firefighters alone. It is essential that the fire-fighting personnel who arrive at the scene of the fire are able to fight the flames on the basis of the conditions that support fire-fighting, and a well thought-out supply of extinguishing water is an important contribution to this as a condition for intervention during the establishment of the fire. In his paper, the author describes some of the technical details and challenges of implementing in public utilities.

Keywords

fire, water, supply, utility, fire fighting

Absztrakt

A tűz elleni védekezés egy sor az élet-, és vagyonvédelem szolgálatában alkalmazott megoldással igyekszik elejét venni az elszabadulni készülő lángok pusztításának. A korszerű műszaki megoldások tűzvédelemben történő felhasználásának köszönhetően a mai környezetünk jóval biztonságosabbá vált. Tekintettel azonban arra tényre, hogy a tűz jelentette fenyegetés továbbra sem szűnt meg teljesen, és sem az éghető anyagokat, sem pedig a tűzkeletkezési okokat nem tudjuk teljesen kizárni az életünkből, ezért valamennyi maradó tűzkockázattal szembe kell néznünk. A tűz lehetséges kitörésével tehát számolnunk kell, amelynek terhét nyilvánvalóan nem háríthatjuk egyedül a tűzoltókra. Ezért lényeges, hogy a káreset helyszínére a kiérkező szerkocsi állománya a tűzoltást támogató körülményekre támaszkodva tudják felvenni a harcot az elharapózó lángokkal, melyhez a létesítés során a beavatkozás feltételeként fontos hozzájárulást jelent az oltóvízellátás. Ennek közművek általi megvalósítása egyes szakmai részleteit és kihívásait mutatja be a szerző írásában.

Kulcsszavak

tűz, víz, ellátás, közmű, intenzitás, tűzoltás

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

BEVEZETÉS

A természet emberi megfigyelései is már elemi erővel ruházták fel a tüzet és a vizet. Ennek egy az Arisztotelészi világképben való megtestesülése, hogy e két „összetevőt" a világot alkotó négy elem közé sorolta a levegő és föld mellett. Az anyagi világnak ezen máig rettegett pusztító hatásaiban markánsan megmutatkozó két megjelenési formájának a szembeállítása ősi idők óta támpontja a tűz elleni küzdelemnek.

Az emberi tudatba beleégett ösztönös tűzhaláltól és vízbe fulladástól való félelem annyira meghatározója az emberi társadalomnak, hogy még a kereszténységbe is áthagyományozódott. Szent Flórián személyében is egy mindkettőt összekapcsoló vértanú képezi a tűzoltók védőszentjét. A vértanúságát bemutató ábrázolásokban rendre szerepel a lángokat vízzel leöntő, csodatévő római katona és vízbe fojtásának eszköze, a malomkő. Mindezek alapján érthető, hogy nem csak a hiedelmek világban antagonisztikus kettejük kölcsönhatása, de a tűz elleni védekezésben is máig a legáltalánosabb alkalmazott oltóanyag a víz. [1]

Bár a víz valóban egy oltástechnikai szempontból egy kifejezetten sok előnyös tulajdonsággal rendelkező oltóanyag, azonban ez önmagában nem elégséges a mai viszonyok között. Ahhoz, hogy a tűzzel szemben eredményesen vehessük fel a harcot a megfelelő anyagi minőség mellett az oltóvíz felhasználásához kötődő sok egyéb tényezőt is figyelembe kell venni. [2] Kiindulnunk azonban a jelenben is az alapvető természettudományi ismeretekre építő műszaki megfontolásokból kell. [3]

A tűzvédelem és benne az oltóvíz felhasználásával végrehajtott tűzoltás, ahogyan az előzőekben láthattuk valóban nem egy újkeletű dolog, mégis mára egy technikailag dominált, és jelentős részben mérnöki megközelítést igénylő kérdéskör. [4] Ugyanakkor szorosan kötődnie kell azokhoz a környezeti viszonyokhoz is, amelyek közepette, magát az oltást a víz felhasználásával kívánjuk megvalósítani. Ennek szembeötlő - bár kissé kisarkított - példája a súlyosan vízhiányos időszakokban vagy az erdőkben kitörő tüzek oltása. [5] Igaz utóbbiak esetében ezt a kihívást meg inkább tetézi a tűzhelyszínek nagykiterjedésű erdőkben való körülményes megközelíthetősége. Sokszor még a nagy terepjáró képességű erdőtüzes szerekkel való beavatkozást is ellehetetlenítő domborzati viszonyoknak köszönhetően nem marad más, mint a légi tűzoltás még összetettebb eszközrendszerét igénybe venni. [6] Azonban még az említett nagy vízszállító kapacitással rendelkező légi tűzoltó eszközök sikeres taktikai alkalmazásának a záloga az oltóvíz hozzáférhetősége és hatékony felhasználása. [7]

Következésképpen bármely taktikai helyzetben a tűzoltás számára az oltóvíz vételezésének kialakítása elsődleges követelmény. Ráadásul olykor a szükséges mennyiséget még az oltóvíz külön tűzi-víz tárolók kapacitásaival is kiegészítve lehet csak biztosítani. [8] Sőt a jogszabályi előírások betartásával természetes vízforrások is számba vehetők. Ebből a célból a létesítési előírásoknak[2] megfelelően oltóvíz-intenzitás mértékének oldaláról figyelembe vehető a sprinklerrendszerek működtetéséhez rendelkezésre álló oltóvíz is. [10]

Megállapítható tehát, hogy egy olyan komplex feladat, mint a tűzoltás, még ha az egy jelentős tűzoltó technikai segítségével megvalósuló beavatkozás is, nem nélkülözheti bizonyos feltételek előzetes megteremtését például az oltóvíz tekintetében. Az erre alapozó tűzoltástaktika alkalmazásának hatékonysága jelentős részben a létesítési előírások szerinti

[2] OTSZ: 72, 73 §, [9]

követelmények teljesülésén múlik. Ellenben az oltás során történő hozzáférést már a használati szabályok érvényesítésével kell biztosítani. [11]

AZ OLTÓVÍZ-ELLÁTÁS TŰZVÉDELMI SZEMPONTJAI

A tűzmegelőzés céljait szolgáló létesítési és a használati szabályokban foglalt előírások meghatározzák a tűzoltói beavatkozások sikeres végrehajtásának feltételeit. Ezek szisztematikus rendben sorra veszik azokat a műszaki-technikai elemeit a létesítendő építménynek, melyek előzetes megtervezése és követelmények szerinti kivitelezés megteremtheti a hatékony tűzoltás alapját. Kezdve a tűzesethez történő vonulás végfázisában a helyszín megközelíthetőségétől, a szükséges mentési és tűzoltási taktikai helyzet igényelte eszközök telepítéséhez nélkülözhetetlen felvonulási terület kialakításán át, egészen a felderítés, mentés és tűzoltás garantált megvalósíthatóságáig bezárólag.

Ez utóbbi feladat teljesítéséhez a feltételrendszeren belül kulcsfontosságú az oltóanyag-ellátás kérdésének a létesítés egyéb, a tűzvédelmet érintő szempontjainak átgondolt vizsgálata. Az e tekintetben számba veendő kritériumok bázisát a tűzbiztonság megteremtésének alapkövét adó kockázatértékelés képezi. A jelenlegi szabályozási környezetben a kockázati osztályba sorolás felállítandó, úgynevezett kockázati mátrixban megjelenített tényezőknek a várható tűzterhelésben és tűzterjedésben szerepet játszó elemei szavatolják az oltóanyag rendelkezésre állásának adekvát megállapítását.

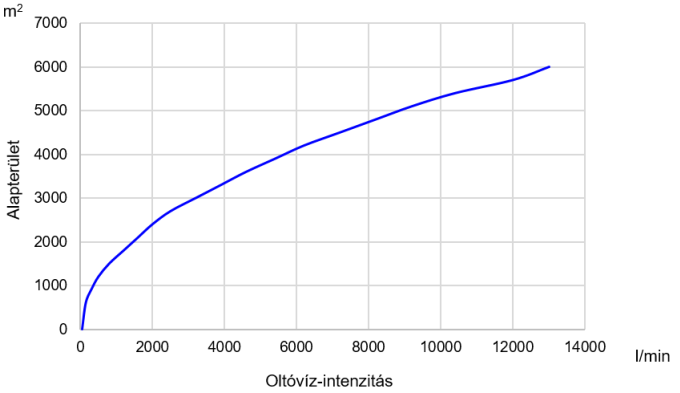
Az ezzel a módszertannal megállapított alábbi négy szintet állították fel:

- **N**agyon **A**lacsony **K**ockázat (NAK),
- **A**lacsony **K**ockázat (AK),
- **K**özepes **K**ockázat (KK),
- **M**agas **K**ockázat (MK).

A lehetséges elkülönülő tűzhelyszínek, mint kockázati egységek tűzveszélyének változó dimenziójú együtt hatását helyesen csak konzervatív biztonsági felfogással hozhatjuk közös nevezőre. Az így kialakított szemlélet alapján a kockázati egységek legkritikusabb szintje diktálta oltóanyag-szükségletet kell biztosítani a kivonuló beavatkozók számára. Hiszen ennek a mértékadó tűzszakasznak a kockázati osztályba sorolási metódusát alkalmazó megközelítésnek a tűzvédelmi összefüggésrendszere megjelenik más létesítési előírásokban is. Ez a lehetséges tűzdinamikáját lekövetni szándékozó kategóriarendszerben az oltóvíz-intenzitás adott időintervallumban történő folyamatos fenntartásában tükröződik vissza. Eszerint a kockázatok fokozódásával párhuzamban a félórás bázis szintől ezt a lépcsőt alapul véve 30 perces időtartománnyal négy lépésben növelve rendre emelkedik az előírt követelmény. [9]

Persze ezt szinkronban kell alkalmazni a tűz lehetséges, a létesítmény mértékadó tűzszakasz besorolását adó konkrét fizikai kiterjedéssel, hisz annak nagysága a tűz térbeli kifejlődése lehetőségének alapvetésként kezelt határait is definiálják, köszönhetően az azt további tűzterjedéstől lezárni hivatott tűzgátló épületszerkezeteknek. Az ugyan ezen elvek mentén megállapított mértékadó tűzszakaszok alapterületének nagyságrendi felosztását az 1. ábrán szemléltetett függvény dinamikáját követve alakították ki. Mindezeken túl megállapítható, hogy a szükséges oltóvíz biztosításának nem kevésbé fontos részlete a használati és egyéb a létesítményüzemeltetéssel kapcsolatba hozható előírások maradéktalan betar-

tása. Ideértve a vízszerzés lehetőségeinek további összetevőit adó oltóvíz-források hozzáférhetőségét és azok berendezéseit, valamint a fenntartás rendszeres karbantartási követelményeit, illetőleg a tűzoltóvíz-források állandó készenlétét azok előírt rendben történő műszaki-technikai kritériumok szerinti felülvizsgálatával.



1. ábra: Az oltóvíz-intenzitás követelményeinek változásaés a mértékadó tűzszakasz alapterületének függvényében
Forrás: OTSZ [9] nyomán szerkesztette a szerző

A TŰZIVÍZ-ELLÁTÁS KIALAKÍTÁSÁNAK ELGONDOLÁSA LAKÓKÖRNYEZETBEN

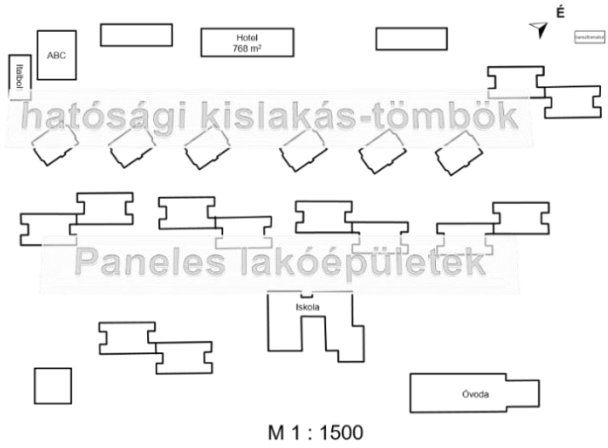
Az ebből a megfogalmazásból is kiolvasható céltételezés alapján rögzíthető, hogy a vonatkozó szabályrendszer alapján [12] megállapított tűzoltói beavatkozás esetén az átlagosnak tekinthető I-es és I-es kiemelt riasztási fokozat[3] alapján kirendelt eszközök alapirányítással történő végrehajtásához önmagában is elegendők. Azonban az ezeknél jóval összetettebb taktikai feladatok megoldásakor azonban már a magasabb csoportirányítási vezetési struktúrában az oltóanyag ellátását (ideértve az oltóvizet is) a háttérparancsnoknak kell szerveznie. [14] Az ennél is bonyolultabb beavatkozásoknál ugyanis a tűzoltásnak ilyenkor minden esetben a tűz diktálta egyedi körülmények szerinti lehetséges taktikai eljárásai szervezeti oldalról is differenciáltabb felépítésű struktúrában valósíthatók csak meg. [15]

Az ezek megvalósításához a tűzoltás céljára elengedhetetlen oltóvíz mennyiségét számítással is megállapíthatjuk, de ez a beavatkozás kapcsán végzendő felderítés során nem kivitelezhető.

Az elmondottakból kiviláglik, hogy bármely tűzhelyszínt érintő esetben a tűzoltói beavatkozás oltóvíz közműhálózatról történő biztosítását jelentő feltételének kialakítása alapkövét a várható tűzkockázatok szerinti körülményeket adják. Ehhez azonban természetszerűleg az adott épített környezetben a terület vezetékes vízhálózatának megtervezéséből kiindulva juthatunk el, melyhez a jelentkező kommunális vízigényeket kell alapul venni. Ez esetben a vízi közmű ellátási igényeinek felméréséhez a vizsgálandó településrész fogyasztási mutatóiból indulhatunk ki. Ennek jelen tanulmányban szerepeltetett alaprajzi vetületét az 2. ábra szemlélteti.

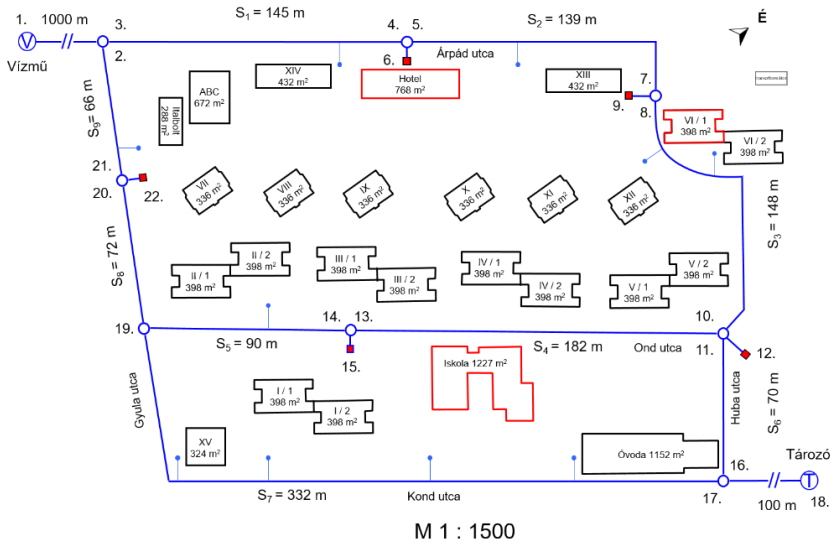
[3] A beavatkozások 90-95 %-át teszik ki. [13]

A kiválasztott lakókörnyezetben beépített terület vezetékes vízhálózatának megtervezése számítógépes célprogram támogatásával a jelentkező kommunális vízigények figyelembe vételével. Ezt követően a hálózat terhelésének vizsgálatát is el kell végezni az érintett terület mértékadó feltételezett tűzesete szükséges vízigénye jelentkezése mellett.



2. ábra: Vizsgált lakóövezet alaprajza
Forrás: szerkesztette a szerző

A mintául szolgáló terület vízi közmű hálózata által kiszolgálandó igények felmérésében jelentkező elsődleges feladat a hálózati struktúra részletes vizsgálata. A jelen tesztkörnyezetben a hálózat hurkolt rendszerben került kialakításra. A vízellátás szempontjából lényeges dimenzionális elem, hogy a vizsgálandóként szolgáló hálózat egy nagy forgalmú főútról lecsatlakozó két párhuzamos utca, valamint az őket merőlegesen összekötő további két mellékutca által határolt közel 6 hektárnyi területre lett ráültetve.

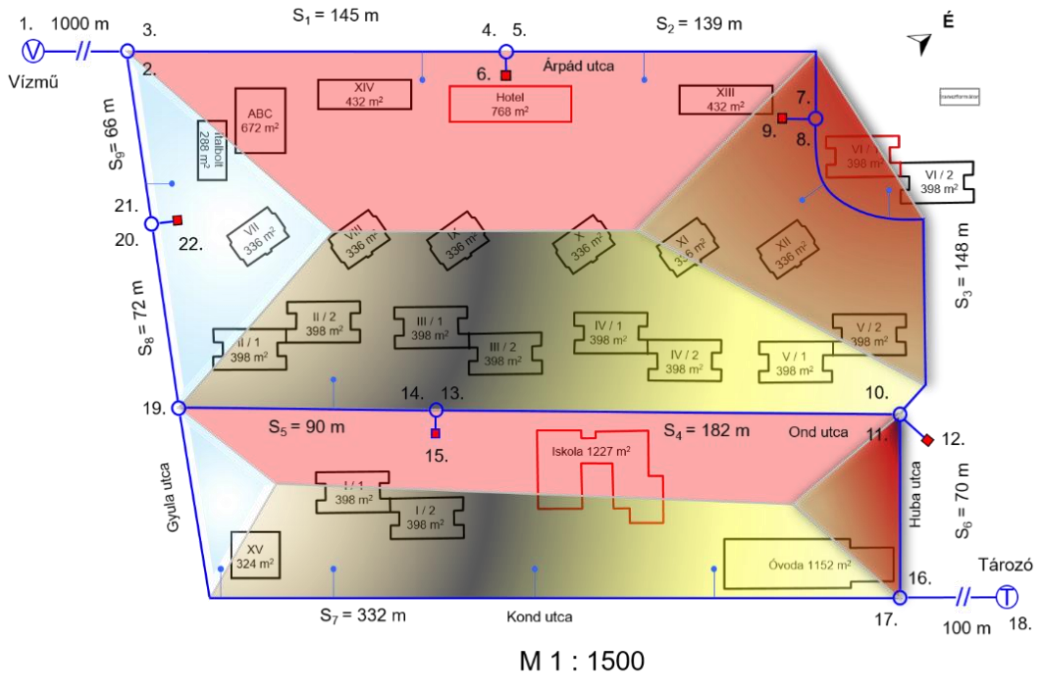


3. ábra: Tesztkörnyezet tervezett vízhálózatának vázlata
Forrás: szerkesztette a szerző

A lakótelep terhelési oldalról kiemelt jelentőségű épületcsoportját adják a 10 emeletes panelházak. Emellett a lakókörnyezet több alacsonyabb számú fogyasztási végponttal rendelkező 2 szintes 4, illetve 6 lakásos társasházakból álló épületet is magában foglal. Ezen felül kereskedelmi egységek, valamint iskola, óvoda és szálloda is van az övezetben.

A kis területen elterülő, viszonylag nagyszámú lakos ellátásának biztonsága szempontjából előnyt jelent a kitermelést végző vízművet és az ennek teljesítményét fokozott hálózati terhelés időszakában kiegészíteni hivatott tározót is magában foglalva kiépült rendszer. Amint az a 3-as ábrából is kitűnik ez a két közmű komponens a vizsgált terület átellenes végein telepített az időszakosan jelentkezhető ellentétes irányú megtáplálásra építve.

A vázoltakhoz hasonlóan a mai települések infrastruktúrájának szerves részét képező vízi közműveknél nem csak a fő vezetéket, de az arról lecsatlakozó hálózati elemeket is ugyanígy körbe vezetik. A rendszer ennek folytán lényegesen nagyobb megbízhatósággal rendelkezik az ellátási területen esetlegesen bekövetkezhető üzemzavarok és nem utolsó sorban a tűzeseti üzemállapotokban jelentkezhető többletvízkivétel során is. Azonban a rendszerben kialakított földfeletti tűzcsapokon való oltóvíz-kivétel céljából történő tűzoltó szerek megtáplálása és az oltósugarak optimális megtelepítéséhez mérlegre kell tenni a hálózati szakaszok és az oltandó épületek egymáshoz való elhelyezkedését is. [16] Az oltóvíz-ellátás tűzeseti kivételére szolgáló földfeletti tűzcsapjainak a várható terhelés szerinti differenciált kiosztásával a beavatkozás oltóvíz-szükséglete kielégíthető. Az ezt megalapozó metodikák egyike a szögfelezők módszere, melynek a tesztkörnyezetre vetített megvalósulását a 4-es ábra illusztrálja.



4. ábra: Szakaszmenti fogyasztás meghatározása szögfelezők módszerével tesztkörnyezetben
Forrás: szerkesztette a szerző

Ezzel együtt is tervezési vonatkozásokat illetően különös figyelmet érdemlő kérdés, hogy a hálózati leágazásokban a vízkivétel mennyiségileg megoszlik a csomóponti törvényhez igazodóan. Emellett a hálózat kialakításának tekintettel kell lennie a csőhálózat vezetékeinek méreteire is, amely viszont műszakilag van összefüggésben a vízkivétel mennyiségi feltételeivel. [17]

Állandó lakosok számának meghatározása

$$\mathbf{N = L \times n}$$

ahol:

N – lakosok száma [fő]

L – lakások száma [lakás]

n – laksűrűség, értéke: **2,3** [fő/lakás]

Kiindulásként először a lakások számát kell megadnunk, amelyhez ismerni kell az épületek strukturális kialakítását. Ezt az 1. táblázatban foglaltam össze.

Ssz.	Épülettípus	Számuk	Lépcsőház darabszáma	Szintszám	Szintenkénti lakóegység	Összesen
1.	Panel	6	2	11	6	792
2.	Kislakás-tömb	7	1	3	4	84
3.	Sorház	2	1	3	8	48
4.	**Összesen**:					**924**

1 Táblázat: Lakóövezet lakásszámának épületek szerinti megoszlása.

$$L = \mathbf{924}\ [\text{lakás}]$$

Mindezekből az alábbiak szerint az állandó lakosok száma statisztikailag 2125 főnek adódik.

$$N = 924\ (\text{lakás}) \times 2{,}3\ (\text{fő/lakás}) = \mathbf{2125}\ [\text{fő}]$$

Napi átlagos vízfogyasztás számítása

$$\mathbf{Q_d = N \times q}$$

ahol:

Q_d – napi átlagos vízfogyasztás

q – napi átlag fogyasztás, értéke: **220** [l/fő/nap]

$$Q_d = 2125\ [\text{fő}] \times 220\ [\text{l/fő/nap}] = 467500\ [\text{l/nap}] = \mathbf{467{,}5}\ [\text{m}^3/\text{nap}]$$

Legnagyobb napi lakossági vízfogyasztás kiszámítása

$$\mathbf{Ql_{d,max} = Q_d \times \beta}$$

$Ql_{d,max}$ – napi legnagyobb lakossági vízfogyasztás
β[4] – egyenlőtlenségi tényező (lakótelepi övezet), értéke: **1,7** *(dimenzió nélküli szám)*

$$Ql_{d,max} = 467{,}5\ [m^3/nap] \times 1{,}7 = \mathbf{794{,}75}\ [m^3/nap]$$

Ehhez jön az alapfokú közintézményeken (óvoda, általános iskola, ABC) felül beszámítandó 200 ágyas, négy csillagos szálloda 350 [l/vendégágy/nap/] középértéken számítva összesen **további 70** [m^3/nap] fogyasztást generálva. Tehát mindösszesen:

$$\mathbf{Q_{d,max}} = 794{,}75\ [m^3/nap] + 70\ [m^3/nap] = \mathbf{864{,}75}\ [m^3/nap] = \mathbf{10{,}0}\ [l/s]$$

Normál üzemállapotok

A vízfogyasztás okozta időszakosan jelentkezhető többletigények tározók segítségével történő térfogatok kiegyenlítéséhez megfelelő számú szivattyú üzembe állítása szükségeltetik. A szivattyúk dinamikus igénybevétele üzemidőben kifejezve a lakossági fogyasztási időszakok magasabb vízigényét adó napszakaira esik. Ennek inverzeként a tározó töltése és így a későbbi többlet kapacitások ilyetén feltételének megteremtése, a kommunális vízelvétel alacsonyabb mennyiségi tételekkel jellemezhető óráiban történik. [18]

A tározók feltöltése tűzeseti üzemállapotokban jelentős többlettel járul hozzá az oltóvíz-intenzitás előírt tartamú megtartásához, amint az az 1. táblázat megjelölt soriból is kiviláglik.

OLTÓVÍZIGÉNY MEGÁLLAPÍTÁSA

A közműhálózat különféle üzemállapotaira vonatkozó számvetések igen összetettek. A jelen tesztkörnyezet vizionált rendszerére vonatkoztatott, és az 1 táblázatban szereplő az eltérő tűzeseti üzemállapotokkal korreláló adatsorok kiszámításához célszoftverek vehetők igénybe. Persze a számítási módszer a szolgáltatási környezet és a statisztikai fogyasztási mutatók alapján lehetővé teszi annak manuális elvégzését is, de ennek teljes összefüggésben történő ismertetése nem tárgya ezen írásnak. A gyakorlatában a megfelelő vízkivétel lehetőségének a megállapítására időszakosan ellenőrző méréseket hajtanak végre a közműszolgáltató munkatársai.

Az érintett terület oltóvízigénye a hatályos OTSZ előírásai alapján számítható. A területen jellemzően 2 emeletes lakóházak, illetve 10 emeletes lakótelepi panelházak találhatóak. A földszintes épületek, így az Óvoda, az ABC és az italbolt redukált alapterülete megegyezik az alapterülettel. A mértékadó tűzszakaszok területe a szállodánál, valamint 2 szintes lakóépületeknél 30 %-kal, míg a panelházak esetében 40 %-kal csökkentésre kerültek. A számított értékeket, az 1-es táblázat részletezi.

[4] Forrás: [18]

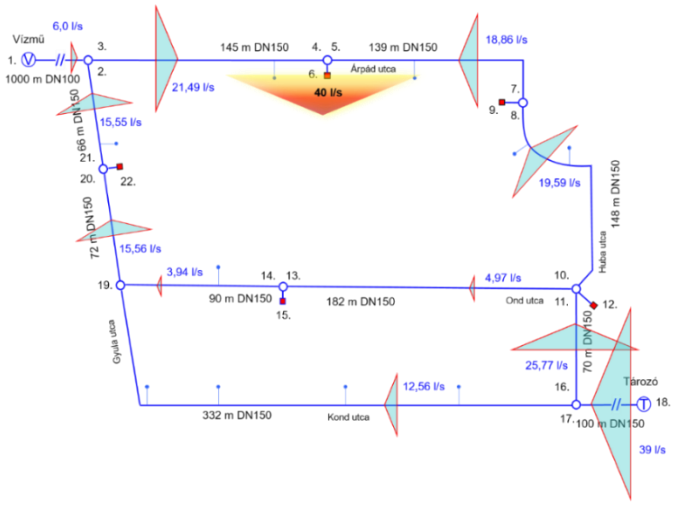
Épület		Szint				Csökkentés mértéke [%]	Csökkentett terület [m²]	Oltóvíz				
		Szám	Terület [m²]					Szükséges		Hálózati	Tározóból	
			Brutto	Netto	Össz			[l/min]	[l/s]	[l/s]	[l/s]	[m³]
I/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
II/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
III/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
IV/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
V/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
VI/	1	11	398	338	3718	40	2231	2700	45	35	10	72
	2	11	398	338	3718	40	2231	2700	45	35	10	72
VII		3	336	286	858	30	601	1500	25	35	-	-
VIII		3	336	286	858	30	601	1500	25	35	-	-
IX		3	336	286	858	30	601	1500	25	35	-	-
X		3	336	286	858	30	601	1500	25	35	-	-
XI		3	336	286	858	30	601	1500	25	35	-	-
XII		3	336	286	858	30	601	1500	25	35	-	-
XIII		3	432	367	1101	30	771	1500	25	35	-	-
XIV		3	432	367	1101	30	771	1500	25	35	-	-
XV		3	324	276	828	30	580	1500	25	35	-	-
Iskola		2	1227	1043	1502	–	1502	2100	35	35	-	-
Óvoda		–	1152	1152	1152	–	1152	1800	30	35	-	-
Szálloda		4	768	653	2612	30	1828	2400	40	35	5	36
ABC		–	672	672	672	–	672	1500	25	35	-	-
Italbolt		–	288	288	288	–	288	900	15	35	-	-

2 Táblázat: Oltóvíz szükségletek a lakóövezetben található épületek mértékadó tűzszakaszainak alapján.

A tesztkörnyezet adta fentebb bemutatott adatsoraiból nyilvánvalóan a legkedvezőtlenebb mutatószámokat eredményező számsorokat kell alapul venni, ha reálisan meg akarjuk ítélni a hálózat óltóvíz-kivételével járó tűzeseti üzemállapotainak kihatásait. Ezt támasztják alá, hogy a területen lehetnek olyan tűzeseti viszonyok, ahol csupán csak a meglévő hálózatból kivett vízmennyiséggel nem biztosított az előírt oltóvíz-intenzitás. Ezért tározó igénybevétele indokolt.

Vagyis ezeket az állapotokat tesztállapotként az alkalmazott célprogramban felhasználva eljuthatunk az 5-ös, 6-os és 7-es ábrákon vázolt rendszerállapotokhoz. Az ott jelzett adatok igazolják, hogy a kialakított tesztkörnyezet képes kielégíteni az oltóvíz-ellátást igényeit, az adott körülmények között előállható legkritikusabb esetekben is.

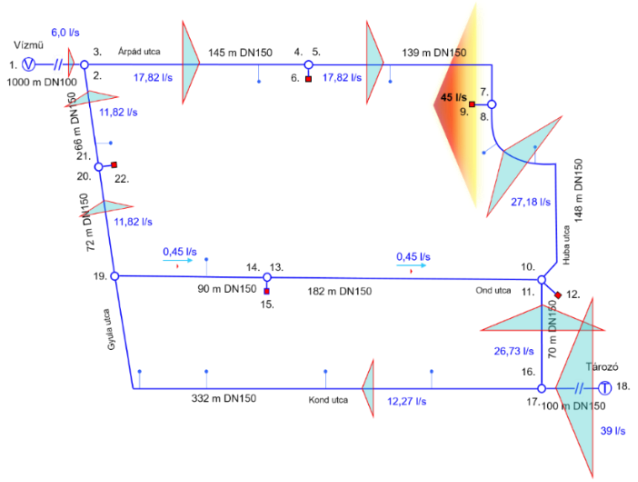
Üzemi állapotok megjelenítése



5. ábra: Szálloda tűzesetének szcenáriójára épülő üzemállapot
Forrás: szerkesztette a szerző

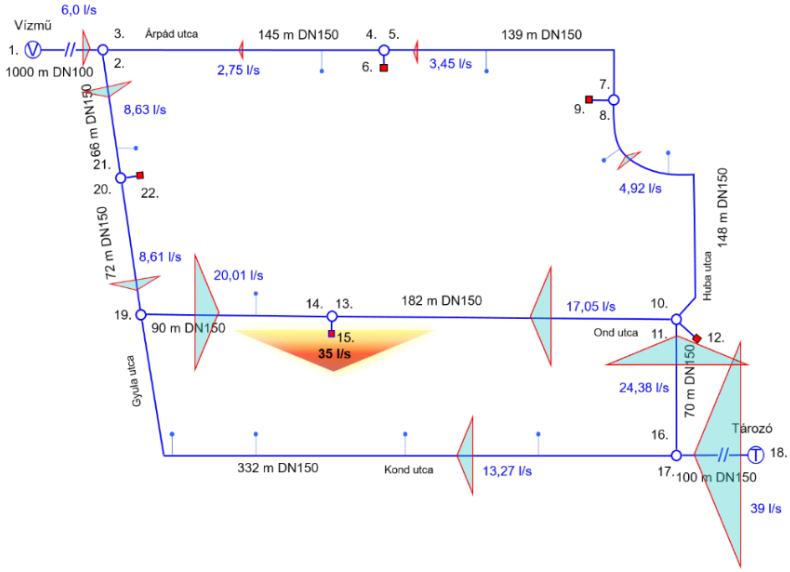
A vízhálózat 6-os csomóponti elemeként feltüntetett föld feletti tűzcsapból történő oltóvíz-kivétel vizsgálatának indokaként szolgál nem csak a jelentősnek mondható mértékadó tűzszakasz, de a rendeltetés szerinti Közepes Kockázati besorolás miatti előírt oltóvíz-intenzitás tartós biztosításának kötelme is.

Láthatóan a hálózat igénybevétele, emellett is képes kiszolgálni a fogyasztói igényeket is, bár érthető módon a hurkolt hálózat középső szakaszán a tározóból történő rásegítés ellenére is komoly mértékben visszaesik a szállított vízmennyiség az oltás időtartamára. Különösen nagy a hálózati szolgáltatási kapacitások visszaesésében a 10 emeletes paneles lakóház tűzesetét vizsgálva, ami ugyancsak a középső szakaszt jelentő leágazás szolgáltatási képességeit rontja le.



6. ábra: Lakóépület tűzesetének szcenáriójára épülő üzemállapot
Forrás: szerkesztette a szerző

Ennél valamelyest jobb a helyzet az iskolai tűzeset hálózati terhelésével kapcsolatos ellátási viszonyokat illetően, persze ez a célprogram számításai alapján adódó alacsonyabb oltóvíz-intenzitásnak is köszönhető.



7. ábra: Iskola tűzesetének szcenáriójára épülő üzemállapot
Forrás: szerkesztette a szerző

KÖVETKEZTETÉSEK

A tűzvédelem és különösen a megelőzése terén a mérnöki módszerek egyre nagyobb teret hódítanak. Ugyanakkor egyértelmű, hogy a műszaki fejlődés biztosította jelentős technikai vívmányok felsorakoztatása a tűzzel szemben nem kezelhetők elszeparáltan más tűzvédelmi kérdésektől. Ilyen formán a tűzoltás feltételeinek megteremtéséből kiindulva a tűzoltás eszközrendszerében is lényegi előrelépést eredményezett a közműhálózatok mind szélesebb körű kiépülése. Ezáltal a tűzoltás kiemelt problémáját a tűz leküzdésének egyik legfontosabb eszközének az oltóvíznek rendelkezésre állása megoldásával egyre hatékonyabbá tette a beavatkozásokat.

Azonban a tűzvédelemben jelentkező kihívások, mint amilyen a lítium-cellák tűzveszélye stb. az egyéb oltóanyagok mellett napjainkban még inkább megnövelte az oltóvíz jelentőségét. Sőt biztosan állíthatjuk, hogy az elkövetkezőben sem fog csökkenni a szerepe a tűzoltásban. Ezt a kihívást csak tetézi, hogy ennek az olcsó, és kifogyhatatlannak hitt oltóanyagnak a mennyiségét az éghajlatváltozás és az azzal járó tartós aszályok jelentősen befolyásolhatják. Ezért mára az oltóvíz-ellátásban még inkább felértékelődik a kiszámítható műszaki-technikai paraméterekkel létesített közműhálózatok jelentősége. Kiemelkedik ezek közül, hogy segítségével igen nagy távolságra is könnyedén eljuttatható az oltóvíz.

Ehhez viszont a kommunális igények kielégítése mellett a tűz elleni védekezés megkövetelte feltételeknek is meg kell feleltetni a közmű hálózatokat, melynek megvannak az előzőekben ismertetett módjai. Ezen tűzoltási feltételek bármely tűzeseti üzemállapotban igazolt megmegteremtésével sikerrel lehet az élet-, és vagyonvédelem követelményeinek eleget tenni.

FELHASZNÁLT IRODALOM

[1] Berki I., *„Ecce ego christianus sum” (Én magam is keresztény vagyok). Szent Flórián vértanú, a védőszent*. Rendvédelem-történeti Hírlevél, ISSN 1785-3257 XXV. évf. 47-50. o., https://doi.org/10.31628/rth.xxv.2015.47-48-49-50n.281-286p, 281-286. o. 2015.

[2] Kuti, R.; Földi, L., *A beépített vízköddel oltó rendszerek újabb alkalmazási lehetőségeinek feltárása*. Hadmérnök 3: 2 pp. 60-66. , 7 p., 2008.

[3] Nagy R., *A felületi feszültség jelenségének változó környezet- és tűzvédelmi dimenziói*. Biztonságtudomány szemle, V. évf. 4. szám, 2023.

[4] Nagy R., *Változó tendenciák a tűzvédelem és biztonságtechnikai mérnökképzés integritásában*. in Jubileumi konferencia a biztonságtechnikai mérnökképzés indításának 30. évfordulója alkalmából, Kiss G., ed., Budapest,: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, ISBN: 978-963-449-329-7, 2024.

[5] Bányai T., Pántya P., *Településeken kívül eső lakott ingatlanok tűzoltói beavatkozásainak sajátosságai egy konkrét eset elemzésével*., Hadmérnök, 15(2), 2020.

[6] Restás, Á., *A légi tűzoltás hatékonyságának tűzoltástaktikai megközelítése*. Haditechnika 58: 2 pp. 61-67. , 7 p. https://doi.org/10.23713/HT.58.2.11, 2024.

[7] Nagy R., Alexandrov, O., *Légi eszközök alkalmazásának ukrajnai gyakorlata kiterjedt erdőtüzek oltásában*. Repüléstudományi Közlemények, (21)4, 2009.

[8] Bíró, T., Hoffmann, I., Kátai-Urbán, M., *Oltóvíz felfogó és tároló létesítmények tervezése és létesítése német útmutató alapján*. Hadmérnök 14 : 2 pp. 111-122., 12 p., 2019.

[9] 54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról.

[10] Nagy, R., *A termikus jelenségek alkalmazása a tűzjelzésben*. Biztonságtudományi Szemle 6: 1 pp. 101-114. , 14 p., 2024.

[11] Herczeg, G., Restás, Á., *Tűzoltó-vízforrások hozzáférhetőségének jelentősége*. Védelem Tudomány: Katasztrófavédelmi Online Tudományos Folyóirat 5 : 1 pp. 37-52. , 16 p., 2020.

[12] 39/2011. (XI. 15.) BM rendelet a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól

[13] Magyar Tűzoltó Szövetség, *Magyar Tűzoltó Szövetség javaslata a katasztrófa- és tűzvédelmi beavatkozások fejlesztésére 2017. december*, https://www.tuzoltoszovetseg.hu/letoltes/document/312-magyar-tuzolto-szovetseg-javaslata-a-katasztrofa-es-tuzvedelmi-beavatkozasok-fejlesztesere-2017-december.pdf, 2017.

[14] BM OKF, *6/2016. (VI. 24.) BM OKF utasítás a Tűzoltás-taktikai Szabályzat és a Műszaki Mentési Szabályzat kiadásáról*, 2016.

[15] Rácz S., *a tűzoltói beavatkozások súlyponti erőmegosztásának vizsgálata*, Hadmérnök XII. Évfolyam „KÖFOP” szám: 92-107., 2017.

[16] TvMI 4.4:2024.02.01. *Tűzoltó egységek beavatkozási feltételeinek biztosítása*

[17] Komjáthy L., *Középmagas és magas épületek tűzvédelmi sajátosságai*, Műszaki Katonai Közlöny, XXI. évfolyam, különszám 2011. https://folyoirat.ludovika.hu/index.php/mkk/article/view/2842/2099, (letöltve: 2025. 02. 19.)

[18] Török L., *Tervezési segédlet település vízellátása tanulmányterv elkészítéséhez*, http://vki.ejf.hu/letoltes/194/szabadon/Torok_Laszlo_tervezesi_segedlet.pdf, (letöltve: 2014. 01. 27.)

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