ISSN 2676-9042

Vol 6, No 1, 2024.

2024, VI. évf. 1. 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
Abuse | **Abúzus**
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

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 6, No 1, 2024. | **2024. VI. évf. 1. szám**

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

BAUMGARTNER Helga

baumgartner.helga@phd.uni-obuda.hu

Helga BAUMGARTNER, safety engineer, PhD Student at the Doctoral School for Safety and Security Sciences Óbuda University. Her research focuses on face recognition in crime prevention and counter-terrorism.

BAUMGARTNER Helga biztonságtechnikai mérnök, az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területe az arcfelismerés alkalmazása a bűnmegelőzésben és a terrorizmus elleni védekezésben.

BORUZS Hunor

boruzsh@mnbbzrt.hu

Hunor BORUZS, currently a PhD student at the Doctoral School on Safety and Security Sciences at Óbuda University. He graduated from the Police Officer's College as a police administration organizer, and then obtained a certified defence administration manager qualification from the National University of Public Service. He manages and researches complex security and defence systems, but his heart is in man-power protection, including armed security guarding.

BORUZS Hunor jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója. A Rendőrtiszti Főiskolán végzett, mint rendészeti igazgatásszervező, majd a Nemzeti Közszolgálati Egyetemen szerzett okleveles védelmi igazgatási vezető szakképzettséget. Komplex biztonsági és védelmi rendszereket irányít és kutat, de szívügye az élőerős védelem, azon belül a fegyveres biztonsági őrzés.

BUSA Attila József

busa.attila@phd.uni-obuda.hu

Attila József BUSA is currently the student of Óbuda University Doctoral School on Safety and Security Sciences. He graduated from Kecskemét College in 2008 with a bachelor's degree in Computer Engineering and in Engineering Teacher Education. In 2012, he graduated from the University of Public Service in the field of MSc in Safety Engineering. In 2019 he graduated from the Budapest University of Technology and Economics as a Mentor Teacher. Currently working at the Cyber and Information Operations Centre of the Hungarian Defence Forces since its establishment in 2022. In the Cyber Training Division, his daily tasks include the development and coordination of cyber defence training. His main research interests include cybersecurity of critical infrastructures, including the role of user awareness in cyber security incidents.

BUSA Attila József jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója. 2008-ban szerzett főiskolai diplomát a Kecskeméti Főiskolán műszaki informatika, valamint a mérnöktanári szakon. 2012-ben a Nemzeti Közszolgálati Egyetemen végzett Biztonságtechnikai mérnök MSc szakon. 2019-ben a Budapesti Műszaki és Gazdaságtudományi Egyetemen szerzett Mentortanár oklevelet. Jelenleg a Magyar Honvédség Kiber- és Információs Műveleti Központjában dolgozik 2022-es megalakulása óta. A Kiberképzési Alosztályon a mindennapi feladatai közé tartozik a kibervédelmi képzések fejlesztése és koordinálása. Főbb kutatási területe a kritikus infrastruktúrák kiberbiztonsága, azon belül is a felhasználói tudatosság szerepének vizsgálata a kibervédelmi incidenseknél.

ČOVIĆ Zlatko

zlatko.covic@uni-obuda.hu

Zlatko ČOVIĆ is a university professor and researcher at the Doctoral School of Safety and Security Sciences at Óbuda University. He earned his Ph.D. degree in the field of Information Science and Technology. His primary areas of expertise include web pro-

Čović Zlatko az Óbudai Egyetem Biztonságtudományi Doktori Iskola egyetemi oktatója és kutatója. Az informatika területen szerezte meg doktori fokozatát. Fő szakterületei közé tartozik a webprogramozás, mobilalkalmazások fejlesztése,

gramming, the development of mobile applications and integrated web systems, cyberse-curity, the use of hackathons in engineering education, and machine learning in web development. He successfully collaborates with companies engaged in web programming and the development of integrated web systems. During his career, he was worked on more than 30 web-based projects as a web programmer and a project manager. He has participated in several mobility programs during which he conducted lectures. Zlatko Čović is the author and co-author of numerous scientific papers published in journals and presented at conferences. From 2023, he is an external member of the Hun-garian Academy of Sciences.

integrált webrendszerek, kiberbiztonság, a hackathonok alkalmazása mérnöki oktatásban és a gépi tanulás a webfejlesztésben. Sikeresen együttműködik olyan vállalatokkal, amelyek webprogramozással és integrált webrendszerek fejlesztésével foglalkoznak. Pályafutása során több mint 30 webes projektben vett részt webprogramozóként, illetve projektmenedzserként. Részt vett több mobilitási programban, amelyek során előadásokat tartott. Számos tudományos cikk szerzője és társszerzője, melyeket folyóiratokban publikált és konferenciákon mutatott be. 2023-tól a Magyar Tudományos Akadémia köztestület külső tagja.

DÉR AttilaTibor

der.attila@uni-obuda.hu

Attila DÉR is a student at the Doctoral School of Safety Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. He holds a degree in Certified electrical engineer from the Specialization in industrial surveillance and communication systems of Kandó Kálmán Faculty of Electrical of engineer. His research interests include cybersecurity, protection of critical infrastructures in particular energy supply.

DÉR Attila az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktori Iskola hallgatója. Okleveles villamosmérnöki végzettségét a Kandó Kálmán Villamosmérnöki Karán szerezte Ipari felügyeleti és kommunikációs rendszerek specializációján. Kutatási területei a kiberbiztonság, kibervédelem, kritikus infrastruktúrák védelme különös tekintettel az energiaellátásra.

FÜRSTNER Igor

furstner.igor@bgk.uni-obuda.hu

Igor FÜRSTNER earned his PhD degree within the realm of Industrial Engineering and Engineering Management. His primary areas of expertise encompass Integrated Product Development and Mechatronics. Over the recent years, he has actively participated in numerous collaborations with enterprises specializing in Product and Service Development. Notably, Igor Fürstner has delivered lectures at various universities as part of different projects and mobility programs. He has contributed both as an author and co-author to numerous scholarly papers published in academic journals and conference proceedings.

FÜRSTNER Igor ipari mérnöki és műszaki menedzsment területen szerezte meg doktori fokozatát. Fő szakterületei közé tartoznak az integrált termékfejlesztés és a mechatronika. Az utóbbi években aktívan részt vett számos együttműködésben olyan vállalatokkal, amelyek a termék- és szolgáltatásfejlesztésre specializálódtak. Fürstner Igor előadásokat tartott több egyetemen különböző projektek és mobilitási programok keretében. Számos folyóiratokban és konferenciakiadványokban megjelentetett tudományos cikkek szerzője és társszerzője.

GÁL István

Istvan.Gal@stud.uni-obuda.hu

István GÁL obtained a BSc diploma in economics at János Kodolányi University, then he got an MSc degree in Logistics at Széchenyi University in Győr. In 2000, he obtained an executive MBA diploma in economics at Szent István University in Gödöllő, and then he became a student at Óbuda University's Doc-

GÁL István a Kodolányi János Főiskolán szerzett közgazdasági BSc, majd a Széchenyi Egyetemen, Győrben Logisztikai MSc diplomat. 2000-ben executive MBA közgazdasági diplomát szerzett a Szent István Egyetemen, Gödöllőn, majd az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallga-

toral School of Security Studies. He is fluently communicating in English at a high level. He also performed at conferences in Europe and in the United States. He had worked in the automotive industry as a Supply Chain Manager, later as a Managing Director, in Europe and in the United States. He is currently involved in optimizing the purchasing activities of the American International School of Budapest. In his doctoral research the field of interest is the optimization and sustainability of the operation of the material supply chain.

tója lett. Angolul felsőfokon kommunikál. Konferenciákon adott elő Európában, valamint az Egyesült Államokban. Európában és az Egyesült Államokban dolgozott az autóiparban anyagellátási vezetők-, később ügyvezető igazgatóként. Jelenleg a Budapesti Amerikai Nemzetközi Iskola beszerzési tevékenységét biztosítja a lehető legmagasabb szinten. A doktori kutatásának területe az anyagellátási lánc működésének optimalizálása és fenntarthatósága.

HANKA László

hanka.laszlo@uni-obuda.hu

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

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

HIMA Zoltán

Zoltan.Hima@gmail.com

Zoltán HIMA is a doctoral student at István Széchenyi University and has been teaching business accounting for 5 years. He communicates in German at a high level, and uses English at a business level. He has an MBA. He has been actively involved in accounting for almost 25 years and taxation for 20 years. He obtained an IFRS balance sheet professional qualification in accounting, and a tax consultant and certified income tax expert degree in taxation. In addition to accounting and taxation, he specializes in the analysis of company reports and business processes as well as the construction of information systems. The main focus of his doctoral research is the relationship between taxation and the circular economy.

HIMA Zoltán a Széchenyi István Egyetemen doktori hallgató és 5 éve vállalkozási számvitelből óraadó. Németül felsőfokon kommunikál, az angolt pedig üzleti szinten használja. MBA fokozata van. Közel 25 éve foglalkozik aktívan számvitellel és 20 éve adózással. Számvitelből IFRS mérlegképes szakképesítése, adózásból pedig adótanácsadó, valamint okleveles jövedelemadó-szakértői fokozatot szerzett. A számvitel és az adózás mellett, a vállalati beszámolók és az üzleti folyamatok elemzése, valamint az információs rendszerek felépítése a szakterülete. Doktori kutatásában az adózás és a körforgásos gazdaság kapcsolata a fő irányvonal.

KAKUJA Izabella

csigus27@gmail.com

Izabella KAKUJA is currently a doctoral student at the Military Engineering Doctoral School of the National University of Public Service. She graduated from the Police College with a first degree in Criminal Justice,

KAKUJA Izabella jelenleg a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola doktorandusz hallgatója. Első diplomáját a Rendőrtiszti Főiskolán szerezte bűnügyi szakon, majd jogi diplomát

followed by a law degree from Eötvös Lóránd University. She then successfully graduated from both Pázmány Péter Catholic University and Károli Gáspár Reformed University. His research interests are in the field of forensic technical activities in CBRN environments and related procedures.

szerzett az Eötvös Lóránd Tudományegyetemen. Ezután mind a Pázmány Péter Katolikus Egyetemen, mind a Károli Gáspár Református Egyetemen is sikeresen diplomázott. Kutatási területe CBRN környezetben végzett bűnügyi technikai tevékenységek és az azokhoz kapcsolható eljárások.

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.

ŐSZI Arnold

oszi.arnold@bgk.uni-obuda.hu

Arnold ŐSZI, Safety Engineer (MSc), PhD in Military Engineering Sciences, Adjunct Professor at the Bánki Donát Faculty of Mechanical and Safety Engineering – Institute of Safety Science and Cybersecurity. His research area: safety, IT, biometrics, drones, crowd motions.

ŐSZI Arnold Okleveles Biztonság-technikai Mérnök (MSc), a Katonai Műszaki Tudományok Doktora, Az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar – Biztonságtudományi és Kibervédelmi Intézetének Adjunktusa. Kutatási területe: biztonság, IT, biometrikus azonosítás, drónok, embertömegek mozgása.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Professor Zoltán RAJNAI (1962), national cyber coordinator of Hungary, professor at Óbuda University. He obtained his university degree in 1993 and defended his doctorate (PhD) degree in 2001 at the Miklós Zrinyi National Defense University. Since 2015, he has been the dean of the Banki Donat Faculty of Mechanical and Safety Engineering, and the founder and deputy head of the Doctoral School of Safety Sciences. His main research area is cyber security, information security, information and communication and telecommunication systems. He has extended his research to the field of IoT devices and the challenges of digitalization, as well as conducting research on the

RAJNAI Zoltán (1962) professzor, Magyarország nemzeti kiberkoordinátora, az Óbudai Egyetem professzora. Egyetemi diplomáját 1993-ban szerezte, doktori (PhD) fokozatát 2001-ben védte meg a Zrínyi Miklós Nemzetvédelmi Egyetemen. 2015-től a Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar dékánja, a Biztonságtudományi Doktori Iskola alapítója és helyettes vezetője. Fő kutatási területe a kiberbiztonság, az információbiztonság, az infokommunikációs és a telekommunikációs rendszerek területe. Kutatásait kiterjesztette az IoT eszközök, a digitalizáció kihívásainak területére, valamint kutatásokat folytat a katonai kommunikációs rendszerek biztonságára,

security of military communication systems and the security of NATO info communication networks. He manages the foundation and start-up tasks of the Kaposvár Science and Innovation Park, and as its professional leader, he also works on cooperation between industry and higher education.

a NATO infokommunikációs hálózatok biztonságára. Menedzseli a Kaposvári Tudományos és Innovációs Park alapítási és indítási feladatait, annak szakmai vezetőjeként az ipar és a felsőoktatás kooperációján is dolgozik.

SZALAY Zsolt

szalay.zsolt@kjk.bme.hu

Zsolt SZALAY graduated as an electrical engineer from the Budapest University of Technology (BME) in 1995, simultaneously obtained a master's degree in economics from Corvinus University in 1997 and earned his PhD in mechanical engineering at BME in 2002. Member of the Hungarian Academy of Engineering since 2009. He began his career as a software development engineer at Knorr-Bremse and later became responsible for the software development of the fourth-generation EBS systems in Hungary. Since 2005, he has been associate professor at the Department of Automotive Technologies at BME, serving as head of department since 2015. As former Head of Research and Innovation, he participated from the very first sketch in designing, implementing, and launching the ZalaZONE Automotive Proving Ground, which is dedicated to connected, automated and electric vehicle testing and validation. He is the founder and leader of the BME Automated Drive Lab research group, offering beyond state-of-the-art solutions for highly automated and autonomous vehicle systems. His research interest focuses on automated vehicle control beyond dynamic limits and uniquely combining automated mobility systems' virtual and physical testing methodologies.

SZALAY Zsolt 1995-ben okleveles villamosmérnökként végzett a Budapesti Műszaki Egyetemen (BME), ezzel párhuzamosan 1997-ben közgazdasági mesterszakos diplomát szerzett a Corvinus Egyetemen, majd 2002-ben a BME-n gépészmérnöki PhD fokozatot szerzett. A Magyar Mérnökakadémia tagja 2009 óta. Pályafutását szoftverfejlesztő mérnökként kezdte a Knorr-Bremse-nél, majd a negyedik generációs EBS rendszerek szoftverfejlesztéséért felelt Magyarországon. 2005 óta a BME Gépjárműtechnológia Tanszék oktatója, 2015 óta tanszékvezetője. Korábbi kutatási és innovációs vezetőként az első vázlattól kezdve részt vett a ZalaZONE Autóipari Próbapálya tervezésében, megvalósításában és beindításában, amely a hálózatba kapcsolt, automatizált és elektromos járművek tesztelésével és validálásával foglalkozik. Alapítója és vezetője a BME Automated Drive Lab kutatócsoportnak, amely magasan automatizált és autonóm járműrendszerekhez kínál jövőbe mutató megoldásokat. Kutatási érdeklődése a dinamikus határon túl történő automatizált járműirányításra és az automatizált mobilitási rendszerek virtuális és fizikai tesztelési módszereinek egyedülálló módon történő kombinálására összpontosít.

TAKÁCS-GYÖRGY Katalin

takacsnegyorgy.katalin@kgk.uni-obuda.hu

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

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

European Green Innovation and Acta Carolus Robertus, furthermore she is co-chief editor of Hungarian scientific journal of agricultural economics: Gazdálkodás).

Robertus) szerkesztője és szerkesztőbizottsági tagja, valamint a Gazdálkodás című magyar agrárgazdasági tudományos folyóirat társfőszerkesztője.

TICK Andrea

Tick.Andrea@kgk.uni-obuda.hu

Prof. Dr. Andrea TICK is a full professor at Óbuda University Keleti Faculty of Business and Management. She completed her MA in English language and literature, Mathematics and Computer Sciences at József Attila University of Arts and Sciences in Szeged and her BSc in Economics at the College for Foreign Trade in Budapest. She completed her PhD in Military Sciences at Zrínyi Miklós National Defence University. Her PhD and Dr. habil research areas are digital teaching and learning with special cyber security awareness. She has over 25 years' experience in teaching in higher education where she teaches statistics, data analytics, Business Intelligence and ERP system. Her research interests include internet security, cyber security, user behavior regarding digital learning, cyber security awareness and the human factor in cyber security.

Prof. Dr. TICK Andrea az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi tanára. Angol nyelv és irodalom, matematika és informatika szakon a szegedi József Attila Tudományegyetemen szerzett MA diplomát, közgazdasági BSc-t pedig a budapesti Külkereskedelmi Főiskolán. PhD fokozatát a Zrínyi Miklós Nemzetvédelmi Egyetemen szerezte meg hadtudományok szakon. PhD és Dr. habil kutatási területe a digitális tanítás és tanulás, különös tekintettel a kiberbiztonsági tudatosságra. Több mint 25 éves felsőoktatási oktatói tapasztalattal rendelkezik, ahol statisztikát, adatelemzést, üzleti intelligenciát, adatbányászatot és ERP rendszereket tanít. Kutatási területe az internetbiztonság, a kiberbiztonság, a digitális tanulással kapcsolatos felhasználói magatartás, a kiberbiztonsági tudatosság és az emberi tényező a kiberbiztonságban.

TÓTH Bálint

tothb.0920@edu.bme.hu

Balint TÓTH graduated as a vehicle engineer MSc from the Budapest University of Technology (BME) in 2018, where he also earned his BSc on the same subject. Parallel to his MSc studies, he has been involved in the project company of the ZalaZONE automotive proving ground since early 2017. Here, he had the opportunity to work in the field of automotive testing with a special focus on highly automated driving and driver assistance systems. Based on his work, he decided to start his PhD studies, in which this semester is his final one. The title of his research subject is the following: "Methodology of highly automated and autonomous road vehicle testing from the perspective of the test track and related simulation technologies". In 2020, he was requested to establish and manage the new branch office of TÜV Rheinland AG at ZalaZONE and build successful local relationships. Nowadays, the branch office in Zalaegerszeg has become one of the most important proving ground locations of TÜV Rheinland. They are working on several type approval-related projects for highly automated vehicles and driver assistance systems. Hence, he can also combine his industrial work with his research.

TÓTH Bálint 2018-ban diplomázott járműmérnök MSc szakon a Budapesti Műszaki és Gazdaságtudományi Egyetemen (BME), ahol ezt megelőzően a BSc. képzést is elvégezte szintén azonos szakon. A mesterképzéssel párhuzamosan 2017 elejétől a ZalaZONE Autóipari Próbapálya projektcégében dolgozott, ahol lehetősége volt a fejlett vezetéstámogató rendszerek, valamint az önvezető járművek tesztelésének lehetőségeivel mélyebben foglalkozni. A tesztpályán végzett feladatinak köszönhetően döntött a PhD tanulmányainak elkezdése mellett, ahol jelenleg már a képzés utolsó félévében tart. Kutatási témájának címe a „Magasan automatizált és autonóm járművek tesztelésének módszertana a tesztpálya és az ahhoz kapcsolódó szimulációs technológiák szempontjából". 2020-ban felkérést kapott a TÜV Rheinland cégcsoportól, a ZalaZONE-on létesítendő telephely létrehozására, valamint a sikeres együttműködések kialakítására. Napjainkra a zalaegerszegi telephely a TÜV Rheinland egyik legfontosabb tesztpályás lokációjává vált, számos fejlett vezetéstámogató rendszer és önvezető jármű homologizációs vizsgálatain dolgoznak, így ipari és kutatási tevékenysége is szorosan összekapcsolódik.

WU Yue

wuyue.budapest@gmail.com

WU Yue is a Ph.D. student at Doctoral School on Safety and Security Science, Obuda University. She is also an assistant professor at Bánki Donát Faculty of Mechanical and Safety Engineering of Óbuda University. She was hornored as Ambassdor for China in DOSZ Ambassdor Program in 2023. Her research interest is food security and sustainable agriculture. She is the president of Chinese Students and Scholars Association in Hungary at Obuda University.

WU Yue az Óbudai Egyetem Biztonság- és Biztonságtudományi Doktori Iskola hallgatója. Emellett adjunktus az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán. 2023-ban Kína nagyköveteként tüntették ki a DOSZ nagyköveti programjában. Kutatási területe az élelmezésbiztonság és a fenntartható mezőgazdaság. Az Óbudai Egyetem Magyarországi Kínai Diákok és Tudósok Egyesületének elnöke.

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 6, No 1, 2024. | **2024. VI. évf. 1. szám**

CONTENT | TARTALOM

BIOMETRIC DATA IN MACHINE READABLE TRAVEL DOCUMENTS – ICAO DOC 9303

BIOMETRIKUS ADATOK A GÉPPEL OLVASHATÓ ÚTI OKMÁNYOKBAN – AZ ICAO DOC 9303

BAUMGARTNER HELGA[1] – ŐSZI ARNOLD[2]

Abstract

The technological development of the 21st century has brought significant changes in security measures, especially in international travel, where the verification of the identity individuals crossing borders is paramount. The limitations of traditional (non-biometric) passports and the widespread use of biometrics, have led to the emergence of machine readable travel documents. The International Civil Aviation Organization has issued Doc 9303 to standardize these documents and enhance their security. The Doc 9303 thoroughly discusses the requirements and recommendations for machine readable travel documents, facilitating the uniformity of documents issued by different member states. The Doc 9303 also requires the integration of biometrics to machine readable travel documents, significantly increasing global security.

Keywords

International Civil Aviation Organization, Machine Readable Travel Documents, Doc 9303, biometric data

Absztrakt

A 21. század technológiai fejlődése jelentős változásokat hozott a biztonsági intézkedések terén, különösen a nemzetközi utazásokban, ahol határon átlépő személyek személyazonosságának ellenőrzésé kiemelt fontosságú. A hagyományos útlevelek korlátozottsága, és a biometrikus adatok alkalmazásának elterjedése következtében, a géppel olvasható úti okmányok előtérbe kerültek. A Nemzetközi Polgári Repülési Szervezet által kiadott Doc 9303 ezen okmányok egységesítésére és biztonságának növelésére hivatott. A Doc 9303 részletesen tárgyalja a géppel olvasható úti okmányokkal szemben támasztott követelményeket és ajánlásokat, elősegítve ezzel a különböző nemzetek által kiadott dokumentumok egységességét. A Doc 9303 a biometrikus adatok úti okmányokba való integrálását is előírja, amellyel jelentősen hozzájárul a globális biztonság növeléséhez.

Kulcsszavak

Nemzetközi Polgári Repülési Szervezet, Géppel olvasható úti okmányok, Doc 9303, biometrikus adat

[1] baumgartner.helga@phd.uni-obuda.hu | ORCID: 0009-0003-7938-7614 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University |Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

2 oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor, Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering |adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A 21. században tapasztalható nemzetközi utazások robbanásszerű növekedése új biztonsági kihívásokat vet fel. A hagyományos útlevelek korlátozottan alkalmasak a modern biztonsági fenyegetések kezelésére, ezért az új megoldások iránti igény egyre sürgetőbbé vált. A növekvő utazási igények és az ezzel járó biztonsági kockázatok megkövetelik a hatékonyabb és fejlettebb biztonsági intézkedések alkalmazását. A hagyományos útlevélrendszer korlátozottságaival szemben az elektronikus útlevelek egyre inkább előtérbe kerültek, hogy megfeleljenek a modern kihívásoknak.

A Nemzetközi Polgári Repülési Szervezet (angolul International Civil Aviation Organization, továbbiakban ICAO) központi szerepet játszik az útlevélrendszerek fejlesztésében és a biztonsági normák meghatározásában, összehangolva a tagállamok, légitársaságok, repülőterek és utasok érdekeit. Az ICAO tevékenysége hozzájárul a globális erőfeszítésekhez a modern utazási kihívások kezelésében, biztosítva a légiközlekedés biztonságát és hatékonyságát.

Jelen publikáció a géppel olvasható úti okmányok, és azon belül is legfőképpen az elektronikus útlevelek által alkalmazott technikai specifikációkat kívánja ismertetni a teljesség igénye nélkül. Az elektronikus útlevelek döntő szerepet játszottak, és játszanak a mai napig az utazási dokumentáció forradalmasításában, a biztonságosabb és hatékonyabb nemzetközi utazás érdekében.

Az ICAO az Egyesült Nemzetek Szervezetének (továbbiakban ENSZ) szakosított, a polgári légi közlekedésért felelős intézménye, amely 1947-óta dolgozik a nemzetközi polgári légi közlekedés biztonságos és szabályos működtetéséért. Ennek értelmében az ICAO feladata a nemzetközi polgári repülésről szóló egyezmény, más néven a Chicagói Egyezmény felügyelete, valamint a nemzetközi polgári repülési szabványok és ajánlott gyakorlatok (angolul Standards and Recommended Practices, továbbiakban SARPs) és politikák közös alapjának kialakítása. Az ICAO elősegíti a tagállamok közötti együttműködést, a légi közlekedéssel kapcsolatos kihívások kezelését, és kulcsfontosságú szerepe van a légiközlekedéssel kapcsolatos szabályok és szabványok kidolgozásában és bevezetésének figyelemmel kísérésében, amelyhez anyagi, technikai és financiális támogatást is biztosítanak – emellett biztonsági auditokat is végrehajtanak, az előírt szabályok és szabványok bevezetésének és betartásának biztosítása érdekében.

Az ICAO szabályzói kiterjednek a nemzetközi polgári légiközlekedés számos területére, többek között magába foglalja a légiforgalom irányítását, a repülőterek infrastruktúrájával kapcsolatos előírásokat, a légi közlekedés „KRESZ" szabályait, a repülőgépek karbantartására vonatkozó előírásokat, a légi közlekedés környezeti hatásainak, igy a károsanyag és a zajszint által okozott környezeti hatások csökkentését, valamint a pilóták és a földi kiszolgáló egység képzésére vonatkozó szabályokat is. Mindemellett a tagállamok határmenti együttműködésére vonatkozó előírásokkal is találkozhatunk, amely magában foglalja többek között az utazással kapcsolatos előírásokat, mint például az előzetes utasinformációs adatok (angolul Advance Passenger Information, továbbiakban API), vagy az utasnyilvántartási adatainak (angolul Passenger Name Record, továbbiakban PNR) megosztására vonatkozó iránymutatásokat, de ide tartozik az úti okmányokra vonatkozó előírások is. [1]

Mindezen intézkedések és előírások elősegítik a nemzetközi légi közlekedés harmonizációját és biztonságát, valamint elősegítik a fenntartható fejlődést is.

GÉPPEL OLVASHATÓ ÚTI OKMÁNYOK

Az „ICAO Doc 9303" (továbbiakban Doc 9303), más néven „Géppel olvasható úti okmányok" (angolul Machine Readable Travel Documents, továbbiakban MRTDs) az útlevelek, vízumok és egyéb utazással kapcsolatos dokumentumok kialakítását, biztonsági jellemzőit és műszaki előírásait szabályozó dokumentumsorozat. Fejlesztése és továbbfejlesztése döntő szerepet játszott a globális utazási biztonság és hatékonyság fokozásában. A Doc 9303 évtizedek alatt fejlődött ki, és vált a géppel olvasható úti okmányokra vonatkozó nemzetközi szabványok meghatározó dokumentumává. Fejlesztése tükrözi az utazás biztonságának és hatékonyságának fokozása iránti globális elkötelezettséget. A technológia folyamatos fejlődésével az ICAO folyamatosan frissíti a dokumentum sorozatot, biztosítva, hogy az úti okmányok biztonságosak és általánosan elfogadottak maradjanak az egyre gyorsabban fejlődő világban.

A géppel olvasható úti okmányok fejlődése az 1968-ban kezdődőt, amikor is a megnövekedett légiutasforgalom hatására az ICAO Tanácsa a 7. ülésszakán megalapította az „Útlevélkártyák Bizottságát" (angolul Panel on Passport Cards) melynek feladata volt, hogy kidolgozza a gépi olvasásra alkalmas útlevelek koncepcióját, amelyek a hagyományos útlevelek helyettesítését szolgálták. A bizottság munkásságának köszönhetően az ICAO 1980-ban kiadata a „Gépi olvasásra alkalmas útlevelekre" (angolul Passport with Machine Redable Capacity) vonatkozó iránymutatását, Doc 9303 néven, melyet 1985-ben a Nemzetközi Szabványtestület (angolul International Standard Organization, továbbiakban ISO) a szabványai közé emelt, és napjainkban az ISO/IEC 7501 – Géppel olvasható úti okmányok szabványcsaládként találhatunk meg (angolul ISO/IEC 7501 – multipart standard: Machine Readable Travel Documents). [2] [3]

1984-ben megalakult a „Géppel Olvasható Úti Okmányok Technikai Tanácsadó Csoportja" (angolul Technical Advisory Group on Machine Readable Travel Documents, továbbiakban TAG/MRTD), aminek feladata volt, hogy a korábbi Bizottság feladatát átvéve, az általuk kidolgozott, már meglévő specifikációkat frissítsék és kibővítsék, valamint a vízumra, illetve egyéb más, utazáshoz alkalmazható személy okmányokra való kiterjesztésének kidolgozzák. A TAG tagjai között megtalálhatóak a tagállamok és nemzetközi szervezetek magasan képzett és tapasztalt szakértői, akik a nemzeti szintű, hivatalos dokumentumok és úti okmányok kiállításáért és nyilvántartásáért felelnek, ezzel biztosítva releváns szakértelmet az MRTD-k továbbfejlesztéséhez. A TAG/MRTD-t 2015-ben átnevezték, „Utas Azonosítási Program" (angolul Traveller Identification Programme – TAG/TRIP).

A TAG/MRTD az „Új Technológiákkal Foglalkozó Munkacsoportja" (angolul New Technologies Working Group, továbbiakban NTWG, melyet WG3-nak is szokás nevezni) háromévente összegyűjti, és felülvizsgálja az MRTD-k esetében alkalmazható új technológiákat, és a releváns információkat megosztja a tagállamokkal, melyet az ICAO is figyelembe vesz a szabályzók kialakítása során.

Mivel egyre több esetben fordult elő az MRTD-k, és legfőképpen az útlevelekkel való visszaélések, így 1994-től az NTWG az MRTD-k biztonságának és megbízhatóságának növelésére tett lépéseket, melyek fizikai biztonsági jellemzőkre, biometrikus adatok alkalmazására, és az adattároló eszközök kapacitásának növelésére irányult. [4] [5]

1998-ban az NTWG megkezdte annak vizsgálatát, hogy melyik biometrikus adat(ok) alkalmas(ak) a személyazonosításra és az úti okmányokba való integrálásra, melynek következtében arra jutottak, hogy az arcfelismerés, ujjnyomat alapú azonosítás, illetve

az írisz mintázat alapú azonosítás az, ami alkalmas lehet a géppel olvasható úti okmányokba való integrálásra. Ezzel egyidőben 1998-ban megjelent az első, ujjnyomat képet tartalmazó elektronikus útlevél Malajziában. Bár sok esetben illetik ezt az első biometrikus útlevélnek, nem tekinthető ICAO kompatibilisnek.

A 2001. szeptember 11.-i terrorcselekmények az egész világot megrengették, mely hatással volt nemcsak az egyes tagállamok biztonságpolitikájára, de a bevándorlási-beutazási politikára, és ezzel egyidejűleg a személyi okmányok biztonságosabbá tételére is. Bár a TAG/MRTD munkássága a biometrikus adatok úti okmányokba való integrálásáról ekkorra már többnyire befejeződött, és kidolgozták a biometrikus adatokat tartalmazó úti okmányok technikai specifikációit, a szeptember 11-i események felgyorsították annak adaptációját az egyes tagállamokban.

Az ICAO Tanácsának 2005-ös döntése alapján, mely a tagállamokra nézve kötelező erővel bírt, 2010 április 1-jétől csak olyan géppel olvasható úti okmányokat lehet kibocsátani, amelyek megfelelnek a Doc 9303 szabványnak. Emellett a nem-géppel olvasható úti okmányoknak legkésőbb 2015. november 24-ig érvényüket kell veszteniük.

Jelenleg több, mint 140 tagállam, és nem állami szervezet bocsát ki az ICAO szabályzóinak megfelelő elektronikus útlevelet, amelyből több mint egymilliárd darab van forgalomban a világon.

BIOMETRIKUS ADATOK A GÉPPEL OLVASHATÓ ÚTI OKMÁNYOKBAN

A Doc 9303 egy 13 részből álló dokumentum-sorozat, mely közel ezer oldalon át ír elő, illetve tesz ajánlásokat a géppel olvasható úti okmányok külső és belső tartalmi jegyeire. Összességében a szabványosítás legfőbb előnye, hogy a különböző fejezetekben foglalt előírások betartásával olyan úti okmányok kerülnek kibocsátásra, amelyek hatékony védelmet nyújtanak módosítás, hamisítás vagy másolás ellen, ezzel egységesítve azokat, illetve ezzel biztosítva, hogy a kibocsátott úti okmányokat a tagállamok kölcsönösen elfogadhatónak és megbízhatónak tartsanak. A Doc 9303 fejezeteinek értelmezése csak együtt lehetséges: a fejezetekben leírtakat a fejezetek elején hivatkozott más fejezetekkel együttesen kell értelmezni. [2]

A fejezetek a következők:

1. Bevezető (angolul Introduction)
2. Az MRTD-k tervezésének, gyártásának és kiadásának biztonsági előírásai (angolul Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
3. Az MRTD-re vonatkozó általános előírások (Specifications Common to all MRTDs)
4. Gépi olvasású útlevelekre (MRP-k) és egyéb TD3 méretű MRTD-kre vonatkozó előírások (angolul Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs)
5. A TD1 méretű, géppel olvasható hivatalos úti okmányokra (MROTD) vonatkozó előírások (angolul Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs))
6. A TD2 méretű, géppel olvasható hivatalos úti okmányokra (MROTD) vonatkozó előírások (angolul Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs))

7. Gépi olvasású vízumok (angolul Machine Readable Visas)
8. Vészhelyzeti úti okmányok (angolul Emergency Travel Documents
9. Biometrikus azonosítás alkalmazása és az adatok elektronikus tárolása az eMRTD-kben (angolul Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs)
10. Logikai adatszerkezet (LDS) a biometrikus és egyéb adatok tárolására az érintésmentes integrált áramkörben (IC) (angolul Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC))
11. MRTD-k biztonsági mechanizmusai (angolul Security Mechanisms for MRTDs)
12. Nyilvános kulcsú infrastruktúra MRTD-k számára (angolul Public Key Infrastructure for MRTDs)
13. Látható digitális plombák (angolul Visible Digital Seals)

A következőkben az MRTD-kben alkalmazott biometrikus adatok, és azok védelméről szóló fejezetek kerülnek részletesebben ismertetésre. Azonban fontos megemlíteni, hogy a Doc 9303 nem tekinthető önálló szabályzónak, figyelembe kell venni egyéb szabályzókat is, mint például az Európai Uniós vagy nemzeti szabályzókat, törvényeket is, melyek itt nem kerülnek ismertetésre.

A biometrikus adatok közül a Doc 9303 az arcfelismerés, ujjnyomat alapú azonosítás, illetve az írisz mintázat alapú azonosítást tekinti alkalmasnak az úti okmányokba való integráláshoz, és akképpen határoz, hogy az úti okmányokban az arckép tárolása kötelező, míg az ujjnyomat vagy az írisz képéből alkotott biometrikus adat opcionális, és az adott tagállam döntés alapul alkalmazása. Azonban ezeknek az alkalmazása mindenféleképpen meg kell, hogy feleljen a vonatkozó ISO/IEC 39794 szabványnak – mely felmenő rendszerben felváltja az ISO/IEC 19794:2005 szabványt. Az ISO/IEC 39794 egy nemzetközi szabványcsalád, amely meghatározza a biometrikus adatcsere-formátumok és -protokollok szabványait a biometrikus adatok kódolásához és cseréjéhez.

Az MRTD-ken tárolt kép(ek)et olyan formátumban kell tárolni, hogy abból biometrikus sablont lehessen generálni, és hogy kompatibilis legyen más tagállamok formátumaival az interoperabilitás elősegítése érdekében. A kibocsátó tagállam a képek mellett a biometrikus sablont is tárolhatja az úti okmányon, hogy az utas személyazonossága ellenőrizhető legyen olyan belföldi helyszíneken, ahol a biometrikus rendszer a kibocsátó ellenőrzése alatt áll. [6]

Az adatok tárolására egy beépített érintkezésmentes áramkört, egy chipet kell a dokumentum lapjaiba integrálni, melynek meg kell felelnie az ISO/IEC 14443-ben és ezzel egyidejűleg az ISO/IEC 7816-4 szabványban foglaltaknak A chip minimum kapacitása tekintetében úgy határoz a Doc 9303, hogy annak elegendő nagyságúnak kell lenni ahhoz, hogy a kötelezően tárolt arckép, illetve az MRZ zónában feltüntetett adatokat, valamint az opcionális biometrikus adatokat is képes legyen tárolni – azonban a felső kapacitásra nincs előírás, az a tagállamok döntésén múlik. Az MRTD-k olvasási távolsága maximum 10 centiméter.

Azon géppel olvasható úti okmányokat, amelyben beépített érintkezésmentes áramkör található és képes biometrikus adatok tárolására, elektronikus géppel olvasható úti okmányoknak nevezzük (eMRTD). Ezen okmányokon a chip jelenlétére utaló jelet kell elhelyezni, amelynek kinézete és méretarányai megtalálhatóak a szabványban. Csak azon

MRTD-re kerülhet fel ez a jel, amely érintésmentes integrált áramkört tartalmaz, amely elegendő adattároló kapacitással rendelkezik a kötelező adatelemek tárolására és amelyen az összes bevitt adat a digitális aláírással került védelemre. [6]

Az MRTD-ken elektronikusan tárolt – kötelező és választható – adatok formátuma, illetve struktúráját a Logikai Adatszerkezet (angolul Logical Data Structure, továbbiakban LDS) határozza meg, kötelezően megtalálhatóak az MRTD-n rögzített biografikus információkat, beleértve az MRTD tulajdonosának arcképét kódolt formában, lehetővé téve az egyértelmű azonosítást. Emellett meghatározásra kerülnek azok az elemek is, amelyek különböző MRTD-k esetén választhatóak, mint például a másodlagos biometrikus azonosítójegy kódolt formában vagy a szükség esetén értesítendő személy neve, illetve egyéb, dokumentummal kapcsolatos információk. Az MRTD-ken tárolt adatok esetében meg kell tudni győződni az adatok hitelességéről és valósságáról, valamint arról, hogy illetéktelenek nem férnek hozzá. Ehhez elengedhetetlen a megfelelő titkosítási eljárás alkalmazása. [7]

Az LDS mellett a chip tartalmaz egy dokumentumbiztonsági objektumot (angolul Document Security Object – továbbiakban SO_D) is, amely az MRTD kiállítására jogosult tagállam vagy szervezet digitális aláírását, és az LDS tartalmának hash-algoritmusát tartalmazza. aláírását, és az LDS tartalmának hash-algoritmusát tartalmazza. Az Azon tagállamok melyek rendelkeznek a másik tagállam nyilvános kulcsával vagy az eMRTD dokumentum-aláíró tanúsítványával, ellenőrizheti a dokumentumbiztonsági objektumot, ezzel hitelesítve az LDS tartalmát egyes tagállamok melyek rendelkeznek a másik tagállam nyilvános kulcsával vagy az eMRTD dokumentum-aláíró tanúsítványával (angolul Document Signer Certificate - továbbiakban C_{DS}), ellenőrizheti a SOD-t, ezzel hitelesítve az LDS tartalmát. [8] [9]

Az MRTD-k kiállítására jogosult tagállam vagy szervezet rendelkezik egy úgynevezett aláíró hitelesítő hatósággal (angolul Country Signing Certificate Authority - továbbiakban CSCA), amely az MRTD megszemélyesítését, és a biometrikus azonosítókat tartalmazó tároló elem adatokkal történő feltöltését hitelesíti, Nyilvános kulcsú infrastruktúrával (angolul Public Key Infrastructure, továbbiakban PKI) kell titkosítani. Ez azt jelenti, hogy az adatok bevitele után azt digitális aláírással látják el, amelynek során az aláírás létrehozásához a küldő saját titkos kulcsát használja, a címzett pedig a nyilvános kulcsával ellenőrzi a hitelességet. A Doc 9303 nem határoz meg konkrét módszert, hanem olyan ajánlást fogalmaz meg, amely a későbbi bővítések során is biztosítja a kompatibilitást. [10]

Ahhoz, hogy az egyes tagállamok meg tudjanak győződni egy másik tagállamban kiadott MRTD-k hitelességéről, hozzá kell férniük a másik tagállamok tanúsítványainak technikai specifikációjához, amelyhez szükség van a titkosítás nyilvános kulcsára. amelyet a tagállamok bilaterális egyezmények keretein belül oszthatnak meg egymással. Mivel minden tagállamnak külön-külön kellene létrehoznia ilyen egyezményeket, az ICAO létrehozott egy központi adatbázist (angolul Public Key Directory, továbbiakban PKD), amely multilaterális egyezmény keretein belül könnyíti meg a tagállamok által létrehozott nyilvános kulcsok cseréjét, ezzel egyszerűsítve az MRTD-k hiteleségének ellenőrzéséhez. A PKD-ban jelenleg több, mint 90 tagállam tanúsítványa került elhelyezésre, melyhez a résztvevő tagállamok a multilaterális egyezmény keretein belül szabadon hozzáférhetnek. [11]

A Doc 9303 az MRTD-ken tárolt adatok védelme érdekében a passzív autentikációt (angolul Passive Authentication – továbbiakban PA) és a chiphez való hozzáférés-ellenőrzést (angolul Chip Access Control – továbbiakban CAC) írja elő kötelező elemként. A PA

során a chipen található SOD kerül validálásra a kiállító tagállam vagy szervezet PKI-ja alapján, ami következtében az LDS tartalma olvashatóvá válik, és az adatok hitelesíthetőek.

A CAC olyan biztonsági megoldásokat alkalmaz, amely az MRTD és az olvasó terminál közötti kommunikációt hivatott biztonságossá tenni az adatlopások megelőzésének érdekében, garantálva, hogy a chiphez való hozzáférés csak akkor engedélyezett, ha az ellenőrző rendszer kriptográfiai módon igazolja jogosultságát. Ez történhet például az ellenőrzést végző személy által manuális módon megadva, illetve optikai úton, az MRZ-t beolvasva.

Az MRTD-ken tárolt szenzitív, vagyis a biometrikus adatokhoz való hozzáféréshez egy külön, opcionális hitelesítési folyamat, úgynevezett terminál hitelesítés (angolul Terminal Authentication – továbbiakban TA) szükséges, melynek során a chip ellenőrzi, hogy az olvasó terminál jogosult-e az érzékeny adatok kiolvasására. További biztonsági megoldásként megtalálható az aktív autentikáció (angolul Active Authentication – AA), illetve a chip autentikáció (angolul Chip Authentication – CA), amelyek megakadályozzák a chip másolását, és bizonyítják, hogy az adatok hiteles dokumentumból kerültek kiolvasásra, és hogy a chipet nem cserélték. [8] [12]

Az úti okmány kiállításakor rögzített arckép és biometrikus adatok integrálása az okmányba, valamint ezek megfelelő védelemmel való ellátása lehetővé teszi az utazók személyazonosságának gyors, hatékony és hitelt érdemlő ellenőrzését. Ezen módszer segítségével az úti okmány könnyedén összekapcsolható a jogos tulajdonosával, ezzel megvalósítva az „egy személy, egy okmány” alapelvet. [13]

ÖSSZEFOGLALÁS

A Nemzetközi Polgári Repülési Szervezet (ICAO) által kiadott Doc 9303 – Géppel olvasható úti okmányokra vonatkozó dokumentumsorozat a globális utazási biztonság és hatékonyság fokozásában játszik fontos szerepet azáltal, hogy előírásokat és ajánlásokat fogalmaz meg a géppel olvasható úti okmányok tartalmára és formátumára vonatkozóan. Ennek következtében az okmányok nem csak gyorsabb és hatékonyabb azonosítást tesznek lehetővé, hanem a hamisítás és az okmányokkal való visszaélés elleni küzdelemben is kulcsszerepet játszanak

A Doc 9303 három féle biometrikus adatot tart megfelelőnek az MRTD-kben való alkalmazáshoz, amelyek az arcfelismerés, ujjnyomat alapú azonosítás, illetve az írisz mintázat alapú azonosítás - ennek értelmében az arckép rögzítése kötelező, míg az ujjnyomat, illetve íriszkép rögzítésé opcionális. A Doc 9303 közvetlen nem rendelkezik ezen adatok rögzítésének módjáról, azonban előírja, hogy a tárolt képeknek olyan formátumúaknak kell lenniük, amelyekből biometrikus sablon generálható, illetve előírja azt is, hogy ezeknek a formátumoknak kompatibilisnek kell lenniük a többi tagállam által használt formátumokkal az interoperabilitás biztosítása érdekében.

A biometrikus adatok géppel olvasható úti okmányokban való alkalmazásához hosszú út vezetett, azonban a folyamatos fejlesztések következtében a nemzetek határainak átlépése, és a repülés is biztonságosabbá vált az évek során. A tartalmi és formai jegyekre vonatkozó előírások és ajánlások meghatározása és betartása következtében olyan egységes géppel olvasható úti okmányok kerülnek forgalomba, melyeket a tagállamok kölcsönösen elfogadhatónak és megbízhatónak tartsanak, amely megkönnyíti a személyazonosság ellenőrzését, jelentősen hozzájárulva ezzel a globális biztonság növeléséhez.

FELHASZNÁLT IRODALOM

[1] PELSER, Albert, ICAO – *The Postal History of ICAO, Annex 9 – Facilitation* [Online] link

[2] *ICAO Doc 9303. Machine Readable Travel Documents Part 1: Introduction* (Eight Edition), [Online] link

[3] MOLNÁR, Ákos – *Nemzetközi szabványosítás, avagy az „ICAO 9303" ajánlás története* – Rendőrségi Tanulmányok 2018/03, A Rendőrség Tudományos Tanácsának Folyóirata, [Online] link

[4] CHATWIN, Charles: *The story of standardisation. A history of ICAO and ICAO Document 9303,* Keesing Journal of Documents, 2011, [Online] link

[5] American National Standards Institute*: ICAO ePassport Case Study – ICAO Adopts JTC 1/SC 37 Standards to Support Biometric Technology for Machine Readable Travel Documents,* [Online] link

[6] *ICAO Doc 9303. Machine Readable Travel Documents Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs* (Eight Edition), [Online] link

[7] *ICAO Doc 9303. Machine Readable Travel Documents Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)* (Eight Edition), [Online] link

[8] *ICAO Doc 9303. Machine Readable Travel Documents Part 11: Security Mechanisms for MRTDs* (Eight Edition), [Online] link

[9] JÓNÁS, Katalin – *Biometrikus azonositók az okmányokban* – SZIMfónia – az NBSZ Szakértői Intézet Műhelymunkái, 2022, [Online] link

[10] *ICAO Doc 9303. Machine Readable Travel Documents Part 12: Public Key Infrastructure for MRTDs* (Eight Edition), [Online] link

[11] *The ICAO Public Key Directory – Secure Cryptographic Authentication of chip-based traveller information* [Online] link

[12] KUS, Burak Can – *Use of Electronic Identity Documents for Multi-factor Authentication* – Master's Thesis, University of Tartu, Institute of Computer Science, 2021 [Online] link

[13] BUSCH, Christoph – *Scope of 3rd Generation Passport Standards and relationship to ICAO* [Online] link

CHANGES IN THE CROP WORLD MARKET: WHAT WILL BE THE FOOD SUPPLY WITHOUT THE RUSSIA-UKRAINE WAR?

VÁLTOZÁSOK A TERMÉNY VILÁGPIACÁN: MILYEN LESZ AZ ÉLELMISZERELLÁTÁS AZ OROSZ-UKRÁN HÁBORÚ NÉLKÜL?

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

Abstract

After COVID-19 and the ongoing war between Russia and Ukraine, we have suffered the most severe food crisis since 2007/2008 world financial and economic crisis. However, the two countries at war are significant world food suppliers, indicating the negative influence of war on food security. In this research, we aimed to predict the main crop export quantity in Ukraine for the period 2022 (the year when the war started) till 2024. We used time series analysis as a research methodology and Matlab software to carry out the analysis. In the end, we found that Russia and Ukraine are estimated to play increasingly important roles in the world food supply regarding wheat, maize, barley, and sunflower seed. This research result can also be a solid basis for the future comparative study on the influence of the Russia-Ukraine war on the world food supply.

Keywords

food supply, food security, crop export quantity, time series analysis, Russia-Ukraine war

Absztrakt

A 2007/2008-as élelmiszerválságot követően a COVID-19 járvány után a világ a folyamatban levő orosz-ukrán háború idején szenvedi el ismét egy élelmiszer válság következményeit. A háború két résztvevő országa a világ alapvető élelmiszer ellátója. A kialakult élelmiszer krízis is mutatja a háború negatív hatásait. Ebben a kutatásban arra törekedtünk, hogy megjósoljuk Ukrajnában a fő terményexport mennyiségét a 2022-től (a háború kitörésének évétől) 2024-ig tartó időszakra. Kutatási módszertanként idősoros elemzést használtunk. Azt találtuk, hogy Oroszország és Ukrajna a becslések szerint egyre fontosabb szerepet fog játszani a világ élelmiszerellátásában a búza, a kukorica, az árpa és a napraforgómag tekintetében. Ez a kutatási eredmény szilárd alapja lehet annak a jövőbeni összehasonlító vizsgálatnak is, amely az orosz-ukrán háború világ élelmiszerellátására gyakorolt hatását vizsgálja.

Kulcsszavak

élelmiszerellátás, élelmiszer biztonság, gabonaexport, idősor analízis, Orosz-Ukrán háború

[1] wuyue.budapest@gmail.com | ORCID: 0000-0003-0349-5654 | PhD candidate, Óbuda University, Doctoral School on Safety and Security Sciences; Assistant Teacher, Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering | PhD hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola; tanársegéd, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] hanka.laszlo@uni-obuda.hu, hanka.laszlo@uni-nke.hu | ORCID: 0000-0002-9129-7481 | associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, University of Public Service, Faculty of Military Science and Officer Training | egyetemi docens, ÓE Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar

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

INTRODUCTION

The acute food insecurity crisis continues to grow, and the rate is alarming from the increasing number of people in food insecurity who need urgent life-saving food assistance and livelihood support in 2022 [1], [2]. Acute food insecurity refers to people being unable to obtain enough food, resulting in lives or livelihoods in immediate danger. Chronic hunger describes a person suffering from an extended period of lack of adequate calories (diet energy) basis of a normal, active, and healthy life. The Prevalence of Undernourishment is used as an indicator to estimate the extent of hunger in the world by FAO. And hunger can also be regarded as undernourishment. Integrated Food Security Phase Classification (IPC) and the Cadre Harmonisé are the internationally-accepted measures of extreme hunger.

Global Network Against Food Crises (GNAFC), an international alliance of the United Nations, the European Union, and governmental and non-governmental agencies [1], was launched by the European Union, Organization of Food and Agriculture (FAO), and World Food Program (WFP) at the 2016 World Humanitarian Summit (WHS). The co-founding and core steering members are the European Commission for International Partnerships (DG INTPA) and European Civil Protection and Humanitarian Aid Operations (DG ECHO), the Organization of Food and Agriculture (FAO), and the World Food Program (WFP). The aim of the Global Network Against Food Crises (GNAFC) is to tackle the root causes of food crises, prevent, prepare for, and respond to the food crisis, promote sustainable solutions, and achieve the Zero Hunger goal of the Sustainable Development Agenda 2030 [2], [3].

However, even though we are trying to handle the food security risks, we still cannot avoid some catastrophic influences, such as the war between important world food supply countries.

In the face of the severe food crisis, we aimed to know how important Ukraine and Russia [4] are in the world food supply, which are the countries at conflict, and the other important world food supply country's role in the future world food supply such as China [5]. Due to the war happening in Ukraine, obviously, agriculture got a profound negative influence in Ukraine, but Russia's agriculture as well. Therefore, our observation data is from 2010 to 2021, the last year before the war started. And we predicted the main crop export quantity from 2022 (when the war started) to 2024. In the end, we can conclude the importance of Ukraine and Russia in the world food supply if there is no war between them and the other country, such as China. On the other hand, when the war finishes, the value of our research result can provide a basis to compare with the real crop export quantity so that we can conclude the influence of war on the world food supply from the perspective of the important world food supply countries at war such as Ukraine and Russia. And if the conflict can also influence other important world food supply country that is not at war, where we take China as an example. Further study can contribute to the topic of how important it is to avoid the risks from war to world food security.

REVIEW OF THE LITERATURE

According to the Annual Global Report on Food Crises announced by Global Network Against Food Crises (GNAFC) [2] in Figure 1 in May 2022, the main drivers of food crises are conflicts and insecurity, weather extremes, and economic shocks. In 2021, nearly

193 million people were exposed to acutely food insecurity and need urgent assistance across fifty-three countries and territories. This number has leaped by eighty percent since 2016, with around 108 million across forty-eight countries. According to the World Food Programme (WFP) estimation, close to 323 million people will suffer acute food insecurity due to the war in Ukraine in 2022 [4].

Figure 1. Numbers of people in Crisis or worse (IPC/CH Phase 3 or above) or equivalent by the key driver in 2021

Both Russia and Ukraine, the countries at war, are among the important top producers of agricultural commodities, such as foodstuffs and fertilizers, to the world population. Especially, Russia is also an important global oil and gas supplier [4]. In 2021, Russia and Ukraine (either or both of them) will be among the top three global exporters of wheat, maize, rapeseed, sunflower seeds, and sunflower oil, and Russia will also play the leading role as world's exporter of nitrogen fertilizers, potassium fertilizers, and phosphorous fertilizers. Many countries heavily rely on imported foodstuffs and fertilizers from the export of Russia and Ukraine to meet their consumption demands. Between 2016/7 and 2020/21 (Figure 2), the significant contribution of Russia and Ukraine combined to global production is from two main aspects: the cereal sector and the oilseed sector. During this time, the two countries contributed over half of the world's output of sunflower oil on average. The global rapeseed output is 6%, and the global soybean output is 2%. In the cereal complex, the share of barley, wheat, and maize in world production accounted for 19%, 14%, and 4%, respectively [6]. From 2018 to 2020, Ukraine supplied 50% sunflower seed oil to the whole global market [7].

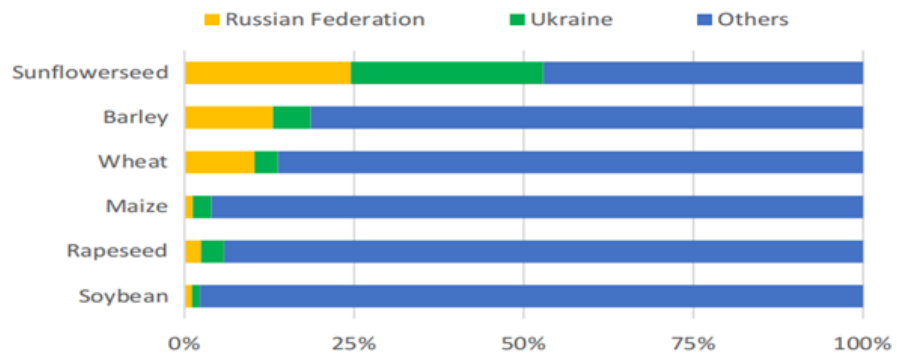


Figure 2. Russia Federation and Ukraine share in global production of selected crops 2016/17-2020/21 Avg.)

As a large agricultural developing country, China has huge amounts of crop production [8], and China's total crop output is among the top ranking in the world [9]. China is feeding a 1.41 billion population [10], with one-fourth of the world's grain yields but less than 10% of the world's arable land [8], [11]. In 2021, China's total crop yield was 682,85 million tons, ranking first in the world. And Russia took fourth place, Ukraine was ninth. At the same time, China was the biggest country to import grain and the third country to export grain [5]. And the total cereal yield in 2021 was 632,76 million tons, such as barley, wheat, maize, etc. [12]. In terms of producing cereals, cotton, fruit, vegetables, meat, poultry, eggs, and fishery products yield, China has hit first in the world output [8].

Nevertheless, China, Russia, and Ukraine are critical players in the world food system. Any shocks to these countries will bring the world population to a catastrophic stage. Therefore, it is our inevitable responsibility to pay attention to unpredictable insecurity issues, such as the COVID-19 pandemic and the war between Russia and Ukraine.

To gauge the influence of the war on the world food supply and avoid the risks from war to world food security, from the view of the Russia-Ukraine war, firstly, we need to notify their important roles in the world food supply in the future from the main crop export quantity if there is no Russia-Ukraine war, such as wheat, maize, barley, and sunflower seed. The next step is to compare the predicted main crop export quantity to the real data. The following section outlines the research methodology used to predict the data for 2022-2024.

TIME SERIES ANALYSIS OF OBSERVED DATA

This research was conducted in May 2022 amid the ongoing war between Russia and Ukraine, and the aimed data are from main crop products export quantity (2010-2021) in Ukraine, Russia, and China from FAOSTAT (Food and Agriculture Organization Corporate Statistical Database) [13]. In order to make sure the research results are accurate, the main crop export quantity from these three countries comes from the same data source, FAOSTAT. In this research, we aimed to predict the future world food supply if there is no Russia-Ukraine war from two perspectives, important world food supply countries at war and the important world food supply country not at war. We chose Ukraine and Russia because they are important world food supply countries [4], [6], [7], but at the same time, they are the countries at war. We chose China as an example because there is no war, and it is also an important world food supply country [5], [8], [11].

The annual time series data pertaining to wheat, maize, barley, and sunflower seed export quantity. After observing the main crop export quantity taken sequentially from 2010 to 2021. The observed and analysed data for Russia, Ukraine and China can be seen in Table 1, Table 2, and Table 3 respectively.

	Russia			
	wheat	**maize**	**barley**	**sunflower**
2010	11848321	230041	1541613	9644
2011	15185953	721626	2067324	113824
2012	16088832	2196553	3430077	274747
2013	13796347	2599289	2324981	79842
2014	22139263	3487880	4009568	90634
2015	21234225	3697593	5294968	60291
2016	25326784	5324066	2862500	186523
2017	33025971	5178687	4632057	313637
2018	43965626	4784344	5441666	87093
2019	31873170	3119665	3940653	713990
2020	37267014	2289269	4963402	1369907
2021	27366370	2936350	3962674	92427

Table 1 Observed data for crop export quantity from Russia in tons for years 2010-2021

	Ukraine			
	wheat	**maize**	**barley**	**sunflower**
2010	4302773	2888339	4593353	307993
2011	4097309	7806319	2144736	406070
2012	8679388	15630889	2582018	282097
2013	7762279	16729468	2339530	70209
2014	10543788	17556531	4165877	73896
2015	13451830	19048697	4629500	47690
2016	17920945	17275407	4801693	196583
2017	17314278	19394541	4855317	73230
2018	16373389	21440629	3597474	58704
2019	13901207	25362998	2386784	101314
2020	18055673	27952483	5046350	187900
2021	19394934	24539480	5344594	84176

Table 2 Observed data for crop export quantity from Ukraine in tons for years 2010-2021

	China			
	wheat	**maize**	**barley**	**sunflower**
2010	72	127420	13419	145857
2011	39808	136123	6279	169608
2012	29	257414	4589	184224
2013	2563	77714	1075	190432
2014	962	20247	116	175714
2015	5302	12455	65	252045
2016	10538	12248	37	296050
2017	9971	69040	64	409684
2018	7344	12205	66	463545
2019	8524	26070	297	480380
2020	33	2675	196	508017
2021	4396	6814	48	426984

Table 3 Observed data for crop export quantity from China in tons for the years 2010-2021

As an example, data series considering Russia is depicted in Figure 3.

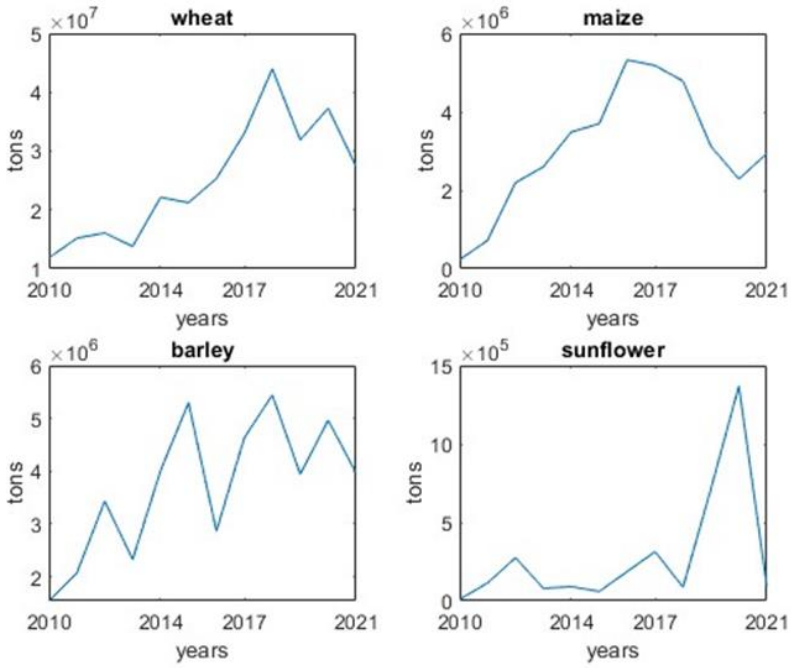


Figure 3 Crop export quantities from Russia in tons for years 2010-2021

A time series analysis has been applied to making forecasts to examine these data. The main perspective in this article is predicting export quantity for the next few years for every crop type for examined countries. The data series summarized in Table 1 can be considered a time series, and the same is true for the other two examined countries. For time series analysis, there exists a commonly applied, sophisticated model, the Box-Jenkins method (ARMA, ARIMA, SARIMA, etc. process) [14], [15] but on the one hand, for these methods, data series must be stationary, which means that expected value (mean) and standard deviation must be constant over time. Considering observed data (for example, Figure 3. for Russia), it is obvious that these data series are not stationary. Expected value and standard deviation change in time. On the other hand, in this analysis, there are only 12 pieces of data in one-time series, which is not sufficient for ARMA, ARIMA, etc. analysis, and for these methods, much more data would be required.

Therefore for modeling and analyzing data series for crop quantities and making predictions, a different mathematical tool, the Holt-Winters exponential smoothing additive model, has been applied [16]–[19]. The mathematical form of this exponential smoothing method is as follows. Every time series data yt is decomposed for three additive terms:

$$y_t = l_t + S_t + e_t$$

Where lt is a general "level" term, St is the seasonal component if, in the time series, a seasonal behavior can be identified, and the final term et is the error component that expresses the uncertainty of the model. For these quantities (except for the error term), a recursion equation system is constructed. This system, in the most general form, is as follows:

$$l_t = \alpha\left(y_t - S_{t-T}\right) + \left(1-\alpha\right)\left(l_{t-1} + b_{t-1}\right)$$
$$b_t = \beta\left(l_t - l_{t-1}\right) + \left(1-\beta\right)b_{t-1}$$
$$S_t = \gamma\left(y_t - l_t\right) + \left(1-\gamma\right)S_{t-T}$$

If, in the time series, a trend (increasing or decreasing) can be identified, the quantity bt is used for modeling the slope of the time series. In the above-given system, T is a time period of the seasonal component, if there exists such a component at all. The Holt-Winters model is identified by the constants α, β and γ. These parameters are chosen from interval [0, 1] independently. For the best-fitting model, the least squares method can be applied to find the best parameters. The effect of these constants for the model is that every predicted value will be a weighted average of previous observations. If the parameter equals 0, the current observation is ignored absolutely; therefore, previous observations will be dominant, and if the parameter equals 1, previous observations are ignored, and the current observation will be dominant. The basic problem is finding the balance between the effect of current and previous observations [16, 17].

The method, in general, is the following. On the basis of observed data, using the least squares method for giving parameters α, β, and γ, the system given above is used for modeling the observed time series and predicting values for the next few years. According to this method, the forecast for the time t + k is given by the formula:

$$y_{t+k} = l_t + kb_t + S_{t+k-nT}$$

Considering Figure 3, it is obvious that examined data series does not contain a seasonal component, and it is also valid for the data series of the other two countries. But some trends can be identified in every series. Therefore in the analysis, a simplified version of the Holt-Winters method was applied. The seasonal component must be deleted from recursion. The simplified system is summarized as follows:

$$l_t = \alpha y_t + \left(1-\alpha\right)\left(l_{t-1} + b_{t-1}\right)$$
$$b_t = \beta\left(l_t - l_{t-1}\right) + \left(1-\beta\right)b_{t-1}$$
$$0 \le \alpha, \beta \le 1$$
$$y_{t+k} = l_t + kb_t$$

In this simpler and more applicable model, the prediction is given by a linear function. The last slope bt is used for forecasting data for the next few years. The initial value of the recursion is obvious for the level component lt, which are observed values y1, y2, etc. The initial value for the slope component can be the first observed slope or the average of the first two or three slopes:

$$b_1 = y_2 - y_1;\ or\ b_1 = \frac{y_3 - y_1}{2};\ or\ b_1 = \frac{y_4 - y_1}{3};$$

In this analysis, the last option was used. The software Matlab has been applied for calculations to carry out the time series analysis and make predictions. In the following section, the result of the analysis will be presented considering every examined country and

cereal. Basically, the behavior of every data series is similar, which can be seen in the figures in section 4, independently of the examined country. Therefore for every data series, the same algorithm has been applied.

In order to know the main crop export quantity if there is no Russia-Ukraine war, the time series analysis predicted the year 2022, when the war started. Considering the ongoing war, data are only predicted until 2024 since the further forecast could be unreliable. In the end, the research result can be compared to the real main crop export quantity from the year 2022, and we will be able to see the influence of Russia-Ukraine war on world food supply.

FORECASTING EXPORT QUANTITIES

The time series data on the main crop export quantity was collected from the 2010-2021 trend data from Ukraine, Russia, and China, including wheat, maize, barley, and sunflower seed. The time series data analysis has been carried out in every case, and the result is demonstrated below for the forecasting period 2022-2024.

Main crop export quantity from 2010-2021 and forecasting for years 2022-2024 in Ukraine

From the FAOSTAT data, the Ukrainian wheat export quantity was only 4 million tons in 2010, and it increased to 19 million tons in the 2021 year by year. The Ukrainian maize export quantity was 2 million tons in 2010, increasing almost ten times after ten years. The Ukrainian barley export quantity remained relatively stable, with 4 million tons in 2010 and 5 million tons in 2021. In 2010, the Ukrainian sunflower seed export quantity was 307 thousand tons, and in 2021 dropped to 84 thousand tons.

A. The forecasting of Ukrainian wheat export quantity for 2022-2024

Year	2022	2023	2024
Forecast (tons)	16373389	13901207	18055673

Table 4 Forecasting results of wheat export quantity for 2022-2024 in Ukraine

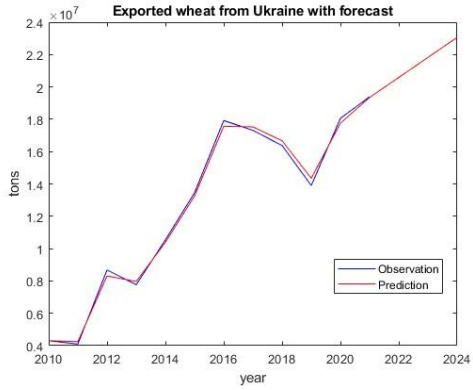


Figure 4 Observed and fitted data series on wheat export quantity in Ukraine

B. The forecasting of Ukrainian maize export quantity for 2022-2024

Year	2022	2023	2024
Forecast (tons)	27664165	30195585	32727006

Table 5 Forecasting results of maize export quantity for 2022-2024 in Ukraine

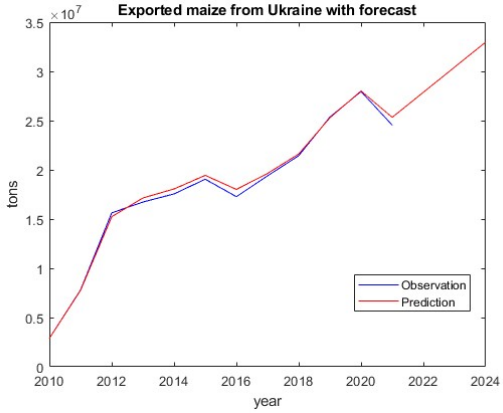


Figure 5 Observed and fitted data series on maize export quantity in Ukraine

C. The forecasting of Ukrainian barley export quantity for 2022-2024

Year	2022	2023	2024
Forecast (tons)	5210667	5140722	5070777

Table 6 Forecasting results of barley export quantity for 2022-2024 in Ukraine

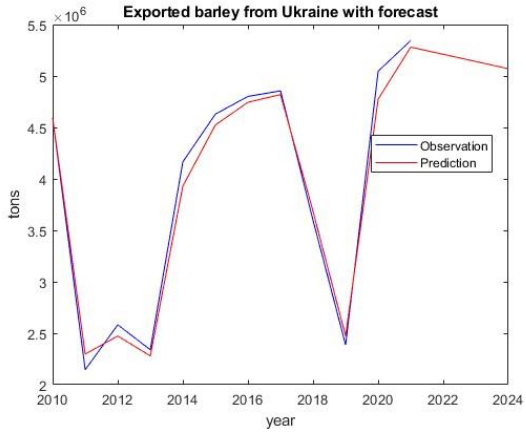


Figure 6 Observed and fitted data series on barley export quantity in Ukraine

D. The forecasting of Ukrainian sunflower seed export quantity for 2022-2024

Year	2022	2023	2024
Forecast (tons)	76607	59842	43078

Table 7 Forecasting results of barley export quantity for 2022-2024 in Ukraine

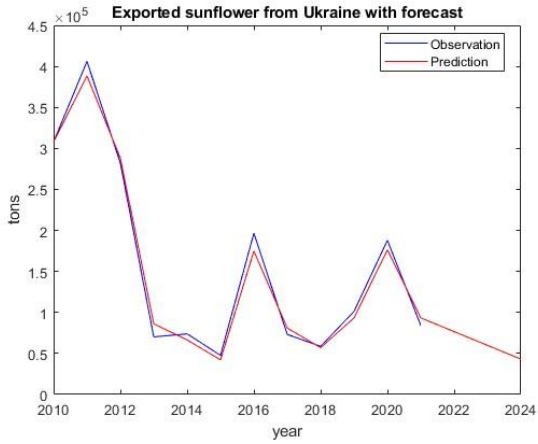


Figure 7 Observed and fitted data series on sunflower export quantity in Ukraine

Main crop export quantity from 2010-2021 and forecasting for 2022-2024 in Russia

As mentioned in this research, Russia is one of the main contributors to the world food supply chain. Between 2016/7 and 2020/21, Russia and Ukraine contributed over half of the world output of sunflower oil on average, and the global share of barley, wheat, and maize among the world production accounted for 19%, 14%, and 4%, respectively. Ukraine and Russia combined contributed barley, wheat, and maize to world production, accounting for 19%, 14%, and 4%, respectively. Russian wheat export quantity

A. The forecasting of Russian wheat export quantity for 2022-2024

Year	2022	2023	2024
Forecast (tons)	29339606	30171704	31003802

Table 8 Forecasting results of wheat export quantity for 2022-2024 in Russia

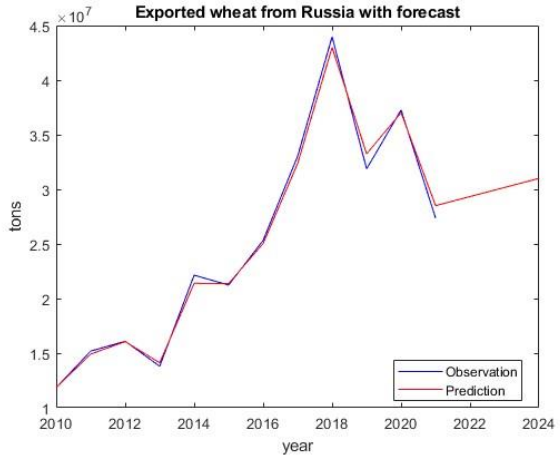


Figure 8 Observed and fitted data series on wheat export quantity in Russia

B. The forecasting of Russian maize export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	3193331	3588229	3983126

Table 9 Forecasting results of maize export quantity for 2022-2024 in Russia

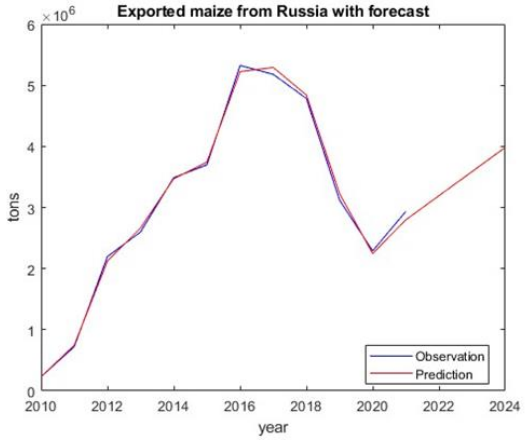


Figure 9 Observed and fitted data series on maize export quantity in Russia

C. The forecasting of Russian barley export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	4252687	4432529	4612370

Table 10 Forecasting results of barley export quantity for 2022-2024 in Russia

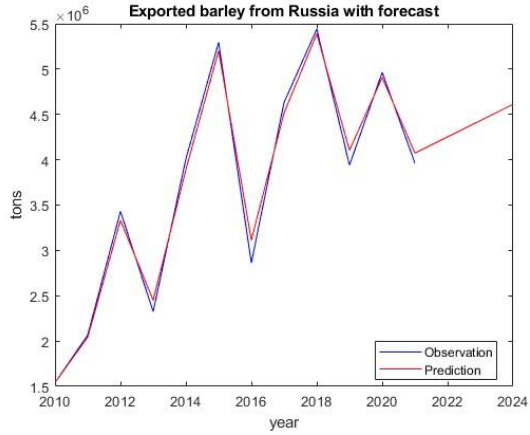


Figure 10 Observed and fitted data series on barley export quantity in Russia

D. The forecasting of Russian sunflower seed export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	220129	228691	237253

Table 11 Forecasting results of sunflower seed export quantity for 2022-2024 in Russia

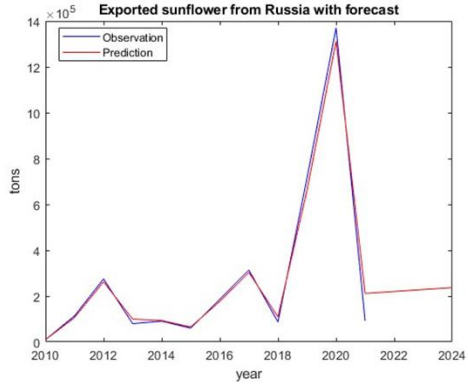


Figure 11 Observed and fitted data series on sunflower export quantity in Russia

Main crop export quantity from 2010-2021 and forecasting for 2022-2024 in China

Besides Russia and Ukraine, China also plays an important role in crop production. China is a large developing agricultural country with a huge amount of crop production. The wheat export quantity was not stable during the period from 2010-2021. The biggest wheat export quantity can reach 4 thousand tons in 2021, and the smallest can be just 29 tons in 2012. Similarly to the Chinese maize and barley export quantity from 2010 to 2021. The Chinese maize export quantity was 12 thousand tons in 2010 and 6 thousand tons in

2021. The Chinese barley export quantity experienced the highest value of 13 thousand tons in 2010 and the smallest value of 37 tons in 2016. The Chinese barley export quantity was 48 tons in 2021. However, the Chinese sunflower seed export quantity kept increasing from 145 thousand tons in 2010 and 426 thousand tons in 2021.

A. The forecasting of Chinese wheat export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	4281	4515	4749

Table 12 Forecasting results of wheat export quantity for 2022-2024 in China

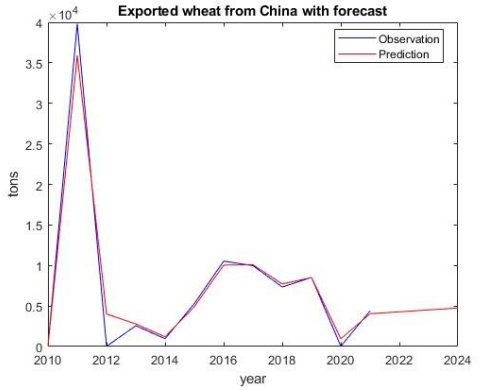


Figure 12 Observed and fitted data series on wheat export quantity in China

B. The forecasting of Chinese maize export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	4521	3790	3059

Table 13 Forecasting results of maize export quantity for 2022-2024 in China

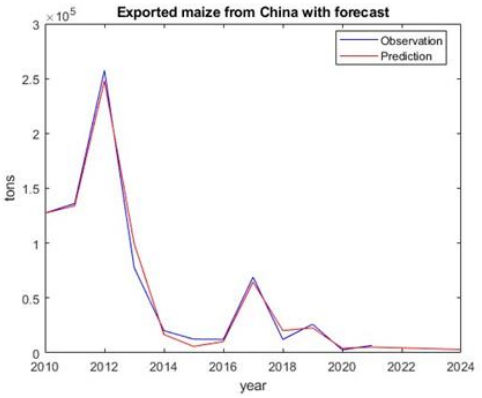


Figure 13 Observed and fitted data series on maize export quantity in China

C. The forecasting of Chinese barley export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	-	-	-

Table 14 Forecasting results of barley export quantity for 2022-2024 in China

Unfortunately, due to the characteristics of the data series, the time series predicting model does not work! The algorithm forecasts negative values as predictions for every possible parameter, which is obviously not acceptable.

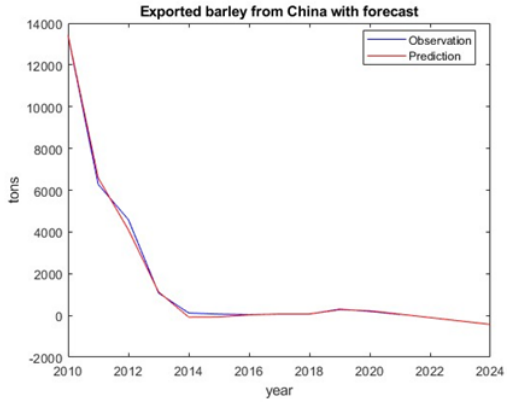


Figure 14 Observed and fitted values series on barley export quantity in China

D. The forecasting of Chinese sunflower seed export quantity for 2022-2024

Year	**2022**	**2023**	**2024**
Forecast (tons)	459916	480637	501359

Table 15 Forecasting results of sunflower seed export quantity for 2022-2024 in China

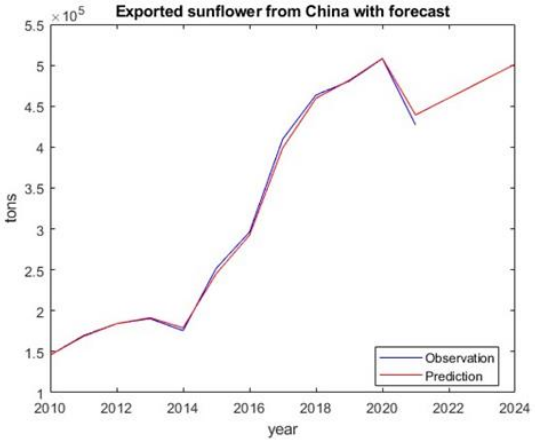


Figure 15 Observed and fitted values series on barley export quantity in China

DISCUSSION

Implications

Based on the main crop export quantity data from FAOSTAT for 2010-2021 investigated in Russia, Ukraine, and China, the time series analysis concluded the forecasting for 2022-2024. We used Matlab software to predict the main crop export quantity from Russia, Ukraine, and China. Russia, Ukraine, or a combination of them will be very important food suppliers to the world, from the aspects of wheat, maize, barley, and sunflower. China will be an important player in the world's sunflower seed supply.

In Ukraine, the wheat and maize export quantity is expected to increase yearly, while the barley and sunflower seed export quantity is projected to decrease for 2022-2024. But the amount after decreasing is still high. Other experts projected that the Ukraine maize export in 2022/23 will be 23.5 million tons [20], while our model shows 25 million tons.

Russia will still play an important role in the world food supply, especially in the world wheat, barley, and sunflower seed supply. Our model predicted in the year 2022-2024, the wheat, maize, barley, and sunflower seed export quantity in Russia would keep increasing. Some experts predicted the export of wheat in Russia in 2022/23 will be between 200 thousand to 43 million tons (Reuters, 2022), making Russia the largest wheat export country (Aleksahhina, 2022), and our model shows a similar number, 30 million tons. The Russian sunflower seeds export quantity is estimated to reach 800 thousand tons (Russia, 2022), which is higher than our model estimation of 200 thousand tons.

In addition to the dominant world food suppliers, Russia and Ukraine, other huge agricultural countries, such as China, are also crucial. During the period 2022-2024, the role of China is predicted to be important still for the world food supply from the aspects of wheat, maize, barley, and sunflower seed. The wheat, maize, and barley export quantity is projected to decrease steadily, but the sunflower seed export quantity will increase. It means that China's role is not as significant as Russia and Ukraine to the world food supply regarding wheat, maize, and barley, but Chinese sunflower seed export is crucial to the world.

Limitations and Suggestions

As discussed in the introduction, firstly, our research result can predict the importance of the important agricultural countries Ukraine, Russia, and China to the world food supply if there is no Russia-Ukraine war. Then the research result can be a good base for further studies. Due to the time limit, we cannot access the official data about the main crop export quantity in these countries. Therefore, we cannot compare the data if there is war and no war to see the influence of war on the world food supply. But the future researcher can compare the data from our research to the real data. And further study will contribute to the importance of avoiding the risks from war to world food security, considering the importance of world food supply countries at war and not at war.

CONCLUSION

Russia and Ukraine will be crucial world food suppliers for main crop products, such as wheat, maize, barley, and sunflower seed. Unfortunately, these two important world food supply countries are still in a long-term conflict, pushing global food security into a worse situation. China will also play an important role in the world's sunflower seed supply for the world. As a result, this research can provide suggestions to the Russian and Ukrainian policymakers to develop micro and macro policies and crop production strategies for future food security and food sustainability. At the same time, other food and agricultural products export countries should also realize their responsibility for the world food supply. In order to realize a sustainable future and food security, everyone is considered an active contributor.

REFERENCES

[1] 'Global Report on Food Crises: acute food insecurity hits new highs', Newsroom, 2022. https://www.fao.org/newsroom/detail/global-report-on-food-crises-acute-food-insecurity-hits-new-highs/en (accessed May 25, 2022).

[2] 'This sixth annual Global Report on Food Crises', Global Network Against Food Crises (GNAFC), 2022. Accessed: May 25, 2022. [Online]. Available: http://www.fightfoodcrises.net/fileadmin/user_upload/fightfoodcrises/doc/resources/GRFC_2022_FINAl_REPORT.pdf

[3] 'What is the Global Network Against Food Crises', What is the Global Network Against Food Crises. http://www.fightfoodcrises.net/about/en/ (accessed May 25, 2022).

[4] Arif Husain, Friederike Greb, and Stefan Meyer, 'Projected increase in acute food insecurity due to war in Ukraine', Mar. 2022. Accessed: May 26, 2022. [Online]. Available: https://docs.wfp.org/api/documents/WFP-0000138155/download/

[5] 'China's grain output ranks first in the world, and it is also the world's largest grain importer and third grain exporter.(中国粮食产量世界第一，也是世界第一粮食进口国，第三粮食出口国)', Apr. 02, 2022. ttps://www.163.com/dy/article/H3UKV9NU053784A2.html (accessed May 26, 2022).

[6] 'The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the current conflict', FAO, Mar. 2022. [Online]. Available: https://www.fao.org/3/cb9236en/cb9236en.pdf

[7] 'How will Russia's invasion of Ukraine affect global food security? | IFPRI : International Food Policy Research Institute', Feb. 24, 2022. https://www.ifpri.org/blog/how-will-russias-invasion-ukraine-affect-global-food-security (accessed May 27, 2022).

[8] ‘China at a glance | FAO in China | Food and Agriculture Organization of the United Nations’. https://www.fao.org/china/fao-in-china/china-at-a-glance/en/ (accessed May 26, 2022).
[9] Y.-S. Yuan, Z.-Y. Cao, Y.-T. Chen, P.-L. Gong, G.-H. Huang, and L. He, ‘Efficiency Analysis of the Crop Production in China in 2019 and 2020: Role of Uncertainty Perceptions in COVID-19’, Discrete Dynamics in Nature and Society, vol. 2022, pp. 1–6, May 2022, doi: 10.1155/2022/7044474.
[10] ‘China: total population 1980-2024’, Statista. https://www.statista.com/statistics/263765/total-population-of-china/ (accessed May 18, 2022).
[11] ‘Food Security in China（中国的粮食安全_白皮书_中国政府网）’, 104 2019. http://www.gov.cn/zhengce/2019-10/14/content_5439410.htm (accessed May 26, 2022).
[12] ‘Announcement of the National Bureau of Statistics on Grain Production Data in 2021 (国家统计局关于 2021 年粮食产量数据的公告)’, Dec. 2021. http://www.stats.gov.cn/tjsj/zxfb/202112/t20211206_1825058.html (accessed May 26, 2022).
[13] ‘FAOSTAT-Crops and livestock products’. https://www.fao.org/faostat/en/#data/TCL (accessed Mar. 02, 2023).
[14] Box-Jenkins, ‘Time Series Analysis, Forecasting and control’, Wiley, 2016.
[15] G. E. P. Box, GWILYM M. JENKINS, GREGORY C. REINSEL, and GRETA M. LJUNG, ‘Time Series Analysis’, p. 709, 2016.
[16] Puah YJ, Huang YF, Chua KC, and Lee TS, ‘River catchment rainfall series analysis using additive Holt–Winters method’, Journal of Earth System Science, vol. 125, no. 2, pp. 269–283, 2016.
[17] Holt CC, Forecasting seasonals and trends by exponentially weighted moving averages. Int. J. Forecasting, 2004.
[18] Lynwood A., Johnson, L.A, Montgomery, D.C, and Gardiner, J.S., Forecasting and Time Series Analysis. 2nd Edition. McGraw-Hill,Inc, 1990.
[19] ‘Time series Forecasting using Holt-Winters Exponential Smoothing’, School of Information Technology, 2004.
[20] A. Yeromin, ‘Ukraine’s 2022-23 corn exports may reach 30mn t: market | Argus Media’, Mar. 30, 2023. https://www.argusmedia.com/en//news/2434547-ukraines-202223-corn-exports-may-reach-30mn-t-market (accessed May 11, 2023).
[21] Reuters, ‘Sovecon ups forecast for Russia’s 2022/23 wheat exports’, Reuters, Aug. 29, 2022. Accessed: May 11, 2023. [Online]. Available: https://www.reuters.com/markets/asia/sovecon-ups-forecast-russias-202223-wheat-exports-2022-08-29/
[22] Z. Aleksahhina, ‘Russia is estimated to be the largest wheat exporter in 2022/23’, Jun. 07, 2022. https://www.mintecglobal.com/top-stories/russia-is-estimated-to-be-the-largest-wheat-exporter-in-2022/23 (accessed May 11, 2023).
[23] ‘Russia: sunflower seeds export volume 2022/23’, Statista, Oct. 26, 2022. https://www.statista.com/statistics/1264495/russia-export-volume-of-sunflower-seeds/ (accessed May 11, 2023).

REDUCING RISKS OF THE AUTOMOTIVE PRODUCTION

AZ AUTÓIPARI TERMELÉS KOCKÁZATAINAK CSÖKKENTÉSE

GÁL István[1] – HIMA Zoltán[2] – TICK Andrea[3]

Abstract

The automotive industry faces several production risks that individually affect its operational efficiency and the quality of the manufactured product. This article examines the potential risks of automotive production. It presents the strategies that can be used to reduce the mentioned risks. We examine the adequacy of workforce training and regulation in both general and critical areas, along with supply chain management, quality control, financial and production risks. Effective management of uncertainties is a key activity for car manufacturers, as maintaining high production standards and preserving their reputation against competitors is extremely important. Continuous development and preventive measures with stakeholders are key. By regulating the indicated collaborations, car manufacturers can strengthen their production processes and their sustainability in a dynamically developing industry.

Keywords

financial risks, HR risks, logistics risks, production's risk, quality risks, automotive industry

Absztrakt

Az autóipar számos termelési kockázattal szembesül, amelyek külön-külön is befolyásolják a működési hatékonyságát és az előállított termék minőségét. Ez a cikk az autóipar termelésének lehetséges kockázatait vizsgálja. Azokat a stratégiákat mutatja be, amelyek használatával csökkenthetők a megemlített kockázatok. Megvizsgáljuk a munkaerő képzésének és szabályozásának megfelelősségét általános és kritikus területeken is, az ellátási lánc menedzsment, minőségellenőrzés, pénzügyi- és termelési kockázataival együtt. Az autógyártók számára a bizonytalanságok hatékony kezelése kulcsfontosságú tevékenység, hiszen a magas gyártási színvonal fenntartása és a versenytársakkal szembeni hírnevük megőrzése rendkívül fontos. A folyamatos fejlesztés és a megelőző intézkedések az érdekelt felekkel kulcsfontosságúak. A feltüntetett együttműködések szabályozásával az autógyártók megerősíthetik gyártási folyamataikat és azok fenntarthatóságát is egy dinamikusan fejlődő iparágban.

Kulcsszavak

HR kockázatok, logisztikai kockázatok, minőségi kockázatok, pénzügyi kockázatok, termelés kockázatai, autóipar

[1] Istvan.Gal@stud.uni-obuda.hu| ORCID: 0000-0002-6592-0110 | purchaser, American International School of Budapest | beszerző, Amerikai Nemzetközi Iskola Budapest

[2] Zoltan.Hima@gmail.com | ORCID: 0009-0009-8251-6871 | PhD Student, Széchenyi István University | PhD hallgató, Széchenyi István Egyetem

[3] Tick.Andrea@kgk.uni-obuda.hu | ORCID: 0000-0002-3139-6509 | professor, Keleti Károly Faculty of Business and Management, Óbuda University | egyetemi tanár, Keleti Károly Gazdasági Kar, Óbudai Egyetem

BEVEZETÉS

Az autóipar, a globális gyártás sarokköve, számos olyan kihívással néz szembe gyártási folyamatai során, amelyek stratégiai kockázatcsökkentő intézkedéseket igényelnek. A technológiai fejlődés, a piaci dinamika és a külső tényezők folyamatosan fejlődnek, így az autógyártás zavartalan és hatékony működésének biztosítása minden eddiginél összetettebbé és kritikusabbá vált. Ez a cikk az autógyártáshoz kapcsolódó különféle kockázatokat tárgyalja, és feltárja azokat a proaktív stratégiákat, amelyeket az iparág vezetői alkalmaznak e kihívások mérséklésére. A szén-dioxid-kibocsátás csökkentését, a sokszínűség előmozdítását, a munkavállalók biztonságának biztosítását és a helyi közösségekkel való együttműködést célzó kezdeményezések bebizonyították, hogy képesek szilárd beszállítói kapcsolatokat ápolni és csökkenteni a kockázatokat [1].

Az autógyártás dinamikus világában a kockázatok sokféle formát ölthetnek, beleértve az ellátási lánc megszakadásait, a technológiai hibákat, a szabályozási változásokat és az emberi hibákat. Ezen tényezők mindegyike befolyásolhatja a gyártás ütemezését, a minőségi szabványokat és az általános működési hatékonyságot. Következésképpen az iparág kénytelen innovatív és adaptív megközelítéseket alkalmazni, hogy eligazodjon ezekben a kihívásokban és megőrizze piaci pozícióját. Azonban nem csak kényelmi szempont az externáliák és a piaci erő mérséklésének együttes beépítése az árképzési mechanizmusba [2]. Ennek a tanulmánynak a célja, hogy rávilágítson az autóipar termelési kockázatainak sokrétűségére, valamint az e kockázatok hatékony mérséklésére alkalmazott különféle stratégiákra. Véleményünk szerint az intelligens hálózatok nem pusztán technológia, hanem összefonódó technológiák komplex összessége, amelyek drasztikus változtatásokat igényelnek mind a felhasználói viselkedésben, mind a társadalomban [3]. Az intelligens hálózatok létrehozása segíti a teljes ellátási lánc működését, a folyamat kezdetétől a folyamat végéig.

Ahogy elmélyülünk az autógyártás kihívásainak és megoldásainak összetett hálójában, a kockázatcsökkentési stratégiák árnyalt megértése fog megjelenni [4]. A valós példák, az iparági trendek és a kialakulóban lévő legjobb gyakorlatok vizsgálatával az olvasók értékes betekintést nyerhetnek abba, hogy az autóipar miként kezeli proaktívan a gyártási kockázatokat, hogy biztosítsa a tartós sikert egy folyamatosan változó környezetben. A következő szakaszok konkrét kockázatcsökkentő stratégiákkal foglalkoznak, bemutatva ezek hatását a termelés ellenálló képességére, valamint az autóiparra gyakorolt szélesebb körű következményeket.

KOCKÁZATCSÖKKENTÉSI STRATÉGIÁK

HR kockázatcsökkentési stratégiák

A HR egy kritikus részleg, amely a szervezet legnagyobb eszközének, a szervezet alkalmazottainak kezelésével foglalkozik [5], a megfelelőségi- és jogi foglalkoztatási szabályokkal. Ezek következményei perek, pénzbírságok vagy büntetések, amelyek befolyásolják a vállalat versenyképességének megítélését, létét és fejlődését [6].

Tehetségkezelési kockázatok léphetnek fel egy üzemben, ha a felvételi folyamatban nem megfelelő a toborzás, és a felvételi folyamat alkalmatlan jelöltek kiválasztásához vezet. Végül ez az áramlás hatással lesz a csapat teljesítményére. Megjelenhetnek a munkavállalói kapcsolatok kockázatai is [7], pl. viták, konfliktusok és rossz munkavállalói kapcsolatok alakulnak ki. Mindezek hatással lehetnek a munkahelyi környezetre és a termelékenységre.

Előfordulhat, hogy hiányzik a hatékony kommunikáció, ami félreértésekhez és elégedetlenséghez vezethet az alkalmazottak körében.

A kockázatok a képzés és a fejlesztés területén is megjelenhetnek. A nem megfelelő képzési programok azt eredményezhetik, hogy a munkaerő nem rendelkezik a feladataik hatékony ellátásához szükséges készségekkel. Az alkalmazottak fejlesztésére való elégtelen összpontosítás a karrier növekedési lehetőségek hiányához vezethet [8], ami befolyásolja a morált és a munkaerő megtartást is. A cégnek folyamatosan figyelnie kell erre a jelenségre, és cselekednie kell, ha bármilyen állapotromlásból eredő figyelmeztetés jelenik meg.

Az adatbiztonsági és adatvédelmi kockázatok rendkívül fontosak egy ellátási lánc esetén [9]. A munkavállalói adatok nem megfelelő kezelése adatvédelmi kockázatot jelent, ezért jogi következményekkel járhat. A General Data Protection Regulation-t (GDPR) erre a célra fejlesztették ki, amelynek betartását a HR osztály biztosítja. A kiberbiztonsági fenyegetések a HR-rendszereket is veszélyeztethetik. Összességében ez adatszivárgáshoz és személyazonosság-lopáshoz vezethet [10]. Az utódlás tervezésének kockázata olyan kockázat, amelyre hajlamosak vagyunk nem gondolni egy cégalapításkor. Különböző okok miatt azonban biztosítani kell az utódlást a munkaerő lecserélésekor is. Ha egyáltalán nem, vagy nem megfelelő módon gondoskodunk időben az utódlásról, veszteségeket szenvedünk.

A kártérítési és juttatási kockázatok akkor jelennek meg, ha tisztességtelen kártérítési gyakorlat történik. Elégedetlenséghez, demotivációhoz vezethetnek az alkalmazottakban, hatásuk azonnal meglátszik tevékenységük eredményességében. A rosszul megtervezett vagy kommunikált juttatási csomagok szintén befolyásolhatják az alkalmazottak morálját és megtartását. Ennek előfordulását is folyamatosan ellenőrizni kell.

Az üzemeltetői oldali kockázatokat, az energiaválságból adódó árváltozásokat tekintik a legnagyobb kockázatnak, ami akár a jövőben is lehetséges, ahogy most pl. az Orosz-Ukrán háború jelenthet kockázatot néhány ellátási rendszerben [11]. Adott esetben a jelenlegi fogyasztási szint mellett a városnak energiatöbblete is lehet, ami értékesíthető, piaci áron a jövőben, ezért célszerű lehet megvizsgálni az energiaközösségek által kínált lehetőséget [12].

A munkahelyi egészségügyi és biztonsági kockázatok olyan típusú kockázatok, amelyek minden munkavállalóra vonatkoznak, függetlenül az általa végzett munkától. A biztonságos és egészséges munkakörnyezet biztosításának elmulasztása balesetekhez, sérülésekhez és jogi felelősségvállaláshoz vezethet. A munkavédelmi előírások betartását egy munkavédelmi képviselő követeli meg, aki mélyreható munkavédelmi ismeretek nélkül is fontos szerepet tölthet be egy vállalkozás munkavédelmében [13].

nem tartása szankciókat vonhat maga után. Megléte olyan fontos, hogy az ideiglenesen érkező látogatók is kötelesek betartani a biztonsági előírásokat [14].

Az elavult HR-rendszerekre való támaszkodás a HR-folyamatok hatékonyságának csökkenéséhez és hibáihoz, valamint a nem megfelelő kiberbiztonsági intézkedésekhez és a HR-adatokhoz való jogosulatlan hozzáféréshez vezethet. Az autóiparban tapasztalható nagy verseny rávilágít erre a kockázatra, hiszen biztosítania kell, hogy a jövőben is megmaradjanak a piaci sikerei.

E kockázatok mérséklése érdekében kell a szervezeteknek befektetniük határozott álláspontot képviselő HR-politikákba, tájékozódniuk kell a munkaügyi törvények változásairól, elő kell mozdítaniuk a pozitív munkahelyi kultúrát, valamint rendszeresen felül kell

vizsgálniuk és frissíteniük kell a HR-folyamatokat a legjobb gyakorlatokhoz való igazodás érdekében. A HR munkatársak rendszeres képzése és a szervezeten belüli hatékony kommunikációs csatornák szintén kulcsfontosságúak a HR-rel kapcsolatos kockázatok kezelésében.

Kockázatcsökkentés az ellátási láncban

A logisztikai részleg számos vállalkozás kulcsfontosságú eleme, felelős az áruk és anyagok mozgásának irányításáért az ellátási láncban. Számos kockázat befolyásolhatja a logisztikai műveletek hatékonyságát és eredményességét. Ezen kockázati tényezők mindegyike az autóiparban valójában kihívást jelent, amelynek sikeresen meg kell felelni [15].

Az ellátási láncban előfordulhatnak fennakadások [16], amelyek a teljes tevékenység működését befolyásolják. Ennek a problémának számtalan oka lehet, ami sokféle lehet és számos hatással lehet a termelésre és a késztermékek előállítására.

A természeti katasztrófák, geopolitikai események vagy váratlan zavarok olyan problémák, amelyek alapvetően kívül esnek a gazdasági társaságon, de befolyásolhatják az áruk és anyagok áramlását, ami késedelmet, hiányt és végül a termelékenységet is befolyásolhatja [17].

A készletgazdálkodási kockázatok hatással lehetnek a termelékenységre [18]. A túl vagy alul készletezett készlet pénzügyi veszteségekhez vezethet. A pontatlan kereslet-előrejelzés és a nem hatékony készletkezelési folyamatok hozzájárulnak ezekhez a kockázatokhoz. Az alapanyagok beszerzését szabályok szabályozzák, az előrejelzéstől a tényleges szállításig, a megfelelő fuvarparitások kiválasztásával és kölcsönös elfogadásával.

A növekvő üzemanyagköltségek, a hosszabb tengeri-, közúti-, vagy légi szállítás, valamint a kapcsolódó vámkezelési vagy egyéb szállítási előírások változása szintén befolyásolhatja a logisztikai költségeket [19]. Előfordulhatnak szállítási kockázatok, például szállítási késések [20], balesetek [21], vagy meghibásodások is, amelyek megzavarhatják az áruk időben történő szállítását . Mintegy 23900 hajó kelt át a Suezi csatornán a tavalyi évben ami közel 3 hajót jelent minden órában [22].

A technológiai és informatikai kockázatok azok a kockázatok, amelyek a logisztikai műveletek nyomon követésére és irányítására használt technológiát képviselik. A logisztikában nagy a függőségük, és rendszerhibákkal, kiberbiztonsági fenyegetésekkel és adatszivárgással kapcsolatos kockázatokat hordoz magában [23].

Szállítói és szállítói kockázatok is felmerülhetnek. A korlátozott számú beszállítóra vagy korlátozott számú megfelelő beszállítóra való támaszkodás olyan kockázatoknak teheti ki a szervezetet, mint például az ellátási lánc megszakadása, minőségi problémák vagy hirtelen költségnövekedés [24].

A szabályozásnak való megfelelés kockázata a következő okok miatt merülhet fel. A vámszabályok, kereskedelmi korlátozások vagy egyéb szállítási előírások be nem tartása késedelmet, bírságot és jogi következményeket vonhat maga után. Ezeket figyelembe kell venni a tevékenység tervezésekor. Kapacitás és erőforrás korlátok. A nem megfelelő infrastruktúra, az elégtelen raktárterület vagy a képzett személyzet hiánya kapacitáskorlátokhoz vezethet, és befolyásolhatja a logisztikai műveletek hatékonyságát.

A deviza- és pénzügyi kockázatok is befolyásolhatják a hatékonyságot. A valutaárfolyamok ingadozása hatással lehet a nemzetközi szállítási költségekre és a logisztikai mű-

veletek általános pénzügyi teljesítményére. Hiszen az igénybe vett szolgáltatások ellenértékét meg kell fizetni, és az árfolyam bármilyen változása likviditási problémákat is okozhat [25].

Környezeti kockázatok merülhetnek fel [26]. A környezeti problémákkal kapcsolatos fokozott tudatosság a logisztikai műveletek környezeti hatásainak fokozott figyelemmel kíséréséhez vezetett. A környezetvédelmi előírások be nem tartása pénzbírsággal és a szervezet hírnevének károsodásával járhat. Összességében a versenyképességet érintheti ez a probléma, ezért mielőbb meg kell szüntetni.

Kommunikációs és együttműködési kockázatok merülhetnek fel az ellátási lánc különböző érintettjei között. A beszállítók, gyártók, forgalmazók és szolgáltatók közötti nem hatékony kommunikáció és együttműködés félreértésekhez és zűrzavarhoz vezethet [27].

Munkaerő- és humánerőforrás-kockázatok alatt a következő kockázatokat értjük: a szakképzett munkaerő hiánya, sztrájkja, vagy egyéb munkával kapcsolatos probléma megzavarhatja a logisztikai osztály működését [28]. Ez felmerülésükkor kellemetlen lehet, de hosszú távú működési kockázatot is jelenthet.

E kockázatok mérséklése érdekében a szervezeteknek robusztus kockázatkezelési stratégiákat kell alkalmazniuk, fejlett logisztikai technológiákba kell befektetniük, diverzifikálniuk kell a beszállítókat, és készenléti terveket kell kidolgozniuk az esetleges zavarokra. A rendszeres nyomon követes, a kulcsfontosságú érdekelt felekkel való együttműködés, valamint a szabályozások és piaci feltételek változásairól való tájékozottság szintén elengedhetetlen a hatékony kockázatkezeléshez a logisztikai osztályon.

Kockázatcsökkentés a termelésben

A termelési kockázatok azokra a potenciális kihívásokra és bizonytalanságokra utalnak, amelyek hatással lehetnek a vállalkozáson belüli gyártási vagy termelési folyamatokra [29]. Ezek a kockázatok befolyásolhatják az áruk időben történő és hatékony előállítását, és következményei lehetnek a szervezet általános teljesítményére.

Az ellátási lánc zavarai hatással vannak magára a termelésre. Az ellátási lánc megszakításai, például a nyersanyagok vagy alkatrészek szállításának késése, megzavarhatják a gyártási ütemtervet, és hiányhoz vezethetnek. A gyártás leállítása vagy későbbi időpontra való áthelyezése hatással van a pontos szállításra, ami a további megrendelések beérkezését is befolyásolja [16].

A kereslet ingadozása hatással van a teljes vállalati termelésre [26]. A piaci kereslet változásai túltermeléshez vagy alultermeléshez vezethetnek, ami befolyásolja a készletek szintjét, és potenciálisan pénzügyi veszteségekhez vezethet. Ha ez csak átmeneti probléma, akkor is jelentős költségekkel járhat.

A minőség-ellenőrzési kérdések jelentős kockázatokkal is járnak. A gyártási folyamat hibái vagy következetlenségei nem megfelelő minőségű termékeket eredményezhetnek, ami a vásárlók elégedetlenségéhez, visszaküldéshez és a vállalat jó hírnevének esetleges károsodásához vezethet [30]. Ezért ennek a kockázatnak a vizsgálata állandó tevékenység.

A berendezés meghibásodása problémákat okozhat a késztermék előállítása során. A gyártás során a nem megfelelő mennyiségű gyártóberendezés rendelkezésre állásának hiánya is okozhat nem megfelelő számú termék előállítást. A gyártóberendezések meghibásodása leálláshoz, késésekhez és megnövekedett karbantartási költségekhez vezethet [31].

A munkaerőhiány vagy a sztrájkok akadályozhatják a termelést. A szakképzett munkaerő hiánya vagy a munkával kapcsolatos egyéb zavarok befolyásolhatják a termelési kapacitást és a hatékonyságot. Munkaerő nem mindig áll rendelkezésre, ezért erre a lehetőségre fel kell készülni. A szabályozási megfelelési kockázatok a tevékenység első percétől jelen vannak. Az iparági előírások vagy termékszabványok be nem tartása pénzbírságot, visszahívást vagy jogi következményeket vonhat maga után [32].

A kockázatok másik típusa a technológiai és automatizálási kockázat, amely a technológiától és az automatizálástól való függőséget jelenti [33], és a kockázatokat rendszerhibákhoz, kiberbiztonsági fenyegetésekhez, valamint az állandó frissítések és karbantartások szükségességéhez társítja.

Az energia- és erőforrásköltségek rendelkezésre állása szintén kiemelt jelentőségű [34]. Az energia- és nyersanyagár-ingadozások hiánya befolyásolhatja a termelési költségeket és a jövedelmezőséget. A nem megfelelő termelési kapacitás vagy a termelési folyamat szűk keresztmetszete korlátozhatja a szervezet azon képességét, hogy megfeleljen a keresletnek [35]. Azonban a termeléstervezési osztály kell rendelkezzen megfelelő képességekkel, hogy a problémát meg tudja oldani. A Termeléstervezési Osztálynak szoros kapcsolatban kell működnie a termeléssel.

Előfordulhatnak természeti katasztrófák és környezeti kockázatok is. Az olyan események, mint a földrengések, árvizek vagy más természeti katasztrófák, megzavarhatják a termelési létesítményeket és az ellátási láncokat. A környezeti aggályok [36]a termelési folyamatokat is befolyásolhatják [23], így a cél ezek elkerülése.

Egy új termék bevezetésének kockázata is fennállhat a termelés során [37]. Az új termékek bevezetése bizonytalansággal jár a piaci elfogadottság, a termelés méretezhetősége és a lehetséges előre nem látható kihívások tekintetében.

A szellemi tulajdon kockázatait is törvény védi. Emellett a szellemi tulajdon védelmével kapcsolatos kockázatok is felmerülhetnek [38]. Különösen azokban az iparágakban van jelen ezen kockázat, ahol a szabadalmaztatott technológiák vagy eljárások kritikusak a termelés szempontjából, így indokolt a nagyobb erőforrások felhasználása.

A valutaárfolyamok ingadozása a valuta- és nemzetközi kereskedelmi tevékenységekből adódó kockázatok közé tartozik [39]. Ez befolyásolhatja az importált nyersanyagok és szolgáltatások költségeit, valamint az exportált áruk versenyképességét.

A termelési kockázatok mérséklése érdekében a szervezeteknek átfogó kockázatkezelési stratégiákat kell alkalmazniuk. Ez magában foglalja az ellátási láncok rendszeres nyomon követését, a minőség-ellenőrzési intézkedésekbe való befektetést, a berendezések karbantartását, a beszállítók diverzifikálását, valamint a piaci feltételek és szabályozások változásairól való tájékoztatást. A folyamatos fejlesztési kezdeményezések, az alkalmazottak képzése és a készenléti tervezés szintén kulcsfontosságú elemei a hatékony termelési kockázatkezelésnek.

Kockázatcsökkentés a minőségbiztosításban

A termelés minőségi kockázatai azokra a potenciális kihívásokra és bizonytalanságokra utalnak, amelyek veszélyeztethetik az előállított áruk minőségét [40]. A magas minőségi szabványok fenntartása kulcsfontosságú egy vállalkozás sikeréhez és hírnevéhez.

A hibás anyagok vagy alkatrészek gyártási nehézségeket okozhatnak [41]. A rossz minőségű vagy hibás alapanyagok és alkatrészek minőségileg nem megfelelő termékek előállításához vezethetnek. A nem megfelelő minőség–ellenőrzési folyamatokkal való működés kockázatos. A nem megfelelő vagy nem hatékony minőség-ellenőrzési folyamatok hibákat vagy következetlenségeket okozhatnak a gyártási folyamatban, ami nem megfelelő termékhez vezethet.

A gyártóberendezések, például a gyártógépek vagy berendezések hibái a végtermék meghibásodásához vezethetnek, ha nem észlelik és kezelik azonnal [42]. A termelés ezért minden nap a műszak kezdetén ellenőrzi a rendelkezésre állást. Meg kell említeni az emberi tévedés kockázatát is. A dolgozók által a gyártási folyamat során elkövetett hibák, mint például a nem megfelelő összeszerelés vagy mérési hibák, veszélyeztethetik a termék minőségét.

A nem megfelelő képzés kockázata egyben a termék megfelelőségének kockázata is. A gyártó személyzet nem megfelelő képzése olyan hibákhoz vezethet, amelyek befolyásolják a termékek minőségét, funkcionalitását, és ebből következően a termékek keresletét és a termékek funkcionalitását, és ennek következtében csökken a kereslet [43]. Az ellátási lánc problémák akkor fordulhatnak elő, ha a minőség romlik, ha problémák vannak a beszállítókkal, például a nyersanyagok nem egyenletes minősége vagy késések előfordulása az ellátási láncban.

Ezen a területen a környezeti tényezők is kockázatot jelenthetnek. A gyártási folyamatok érzékenyek lehetnek a környezeti feltételekre, és olyan tényezők, mint a hőmérséklet, a páratartalom vagy más környezeti változók befolyásolhatják a termék minőségét. A szabályozási megfelelés indokolta az autóiparban különféle szabványok megalkotását [44], mint például az ISO TS/16949, majd később az IATF szabvány. Az iparági előírások és minőségi szabványok be nem tartása pénzbírságot és a vállalat jó hírnevének károsodását vonhatja maga után. A kockázatok a folyamat dokumentálásának hiányában rejlenek. Ez az említett ISO specifikációkat jelenti. A hiányos vagy elavult folyamatdokumentáció eltérésekhez vezethet a gyártási folyamatban, ami befolyásolja a termék minőségét.

A tesztelési és ellenőrzési hibák kockázatot jelentenek. Ha a tesztelési és ellenőrzési eljárások nem szigorúak, vagy nem megfelelően hajtják végre, a hibák észrevétlenül maradhatnak, ami a nem megfelelő termékek kibocsátásához vezethet. A terméktervezés megváltoztatása kockázatokkal is jár [45]. A specifikációiban bekövetkezett változások új kockázatokat is jelenthetnek, ha azokat a bevezetés előtt nem vizsgálják át és validálják alaposan.

Ha a beszállítónál minőségi hibák lépnek fel, az azonnal befolyásolhatja a termék használhatóságát a vevői oldalon, hiszen a beszállítói szintű minőségi problémák, beleértve a gyártási szabványok változásait is, befolyásolhatják a végtermék minőségét [46]. A termék visszahívásának kockázatát a termék nem megfelelősége okozhatja. Visszahívásra lehet szükség, ha a termékek forgalomba hozatala után minőségi problémákat észlelnek, amelyek anyagi veszteségekhez és a márka károsodásához vezetnek.

A termelés minőségi kockázatainak mérséklése érdekében a szervezeteknek robusztus minőségirányítási rendszereket kell bevezetniük, rendszeres auditokat és vizsgálatokat kell végezniük, be kell fektetni az alkalmazottak képzésébe, és világos kommunikációs csa-

tornákat kell kialakítaniuk a beszállítókkal. A termelési folyamatok folyamatos nyomon követése és fejlesztése, valamint az ipari szabványok és előírások betartására való erős összpontosítás a hatékony minőségi kockázatkezelés alapvető elemei a termelésben.

Kockázatcsökkentés a pénzügy területén

A gyártóüzem pénzügyi részlege felelős az üzem működésének pénzügyi vonatkozásaiért, beleértve a költségvetést, a könyvelést, a pénzügyi beszámolást és a megfelelőséget. Különféle kockázatok befolyásolhatják a pénzügyi stabilitást és a pénzügyi részleg teljesítményét a termelőüzemen belül.

Számtalan költségvetési kockázat merülhet fel. Ezért a pontatlan költségvetés vagy a költségvetési korlátok be nem tartása pénzügyi stresszhez vezethet, és befolyásolhatja a gyártó üzem általános pénzügyi állapotát. Fennáll a költségtúllépés veszélye is. A termelési költségek váratlan növekedése [47], akár a nyersanyagárak ingadozása, akár a váratlan karbantartási költségek vagy más tényezők miatt, megterhelheti a pénzügyi erőforrásokat.

A cash flow-kezelési kockázatok során a rossz cash flow–kezelés likviditási problémákhoz vezethet, és megnehezítheti a rövid távú pénzügyi kötelezettségek teljesítését. Az árfolyamkockázatot több területen is kockázati tényezőként említették [48]. A nemzetközi kereskedelemben részt vevő gyártó üzemek az árfolyam–ingadozásokkal kapcsolatos kockázatokkal szembesülhetnek, amelyek befolyásolják az importált anyagok költségét vagy az exportált áruk versenyképességét.

A piaci kereslet ingadozása hatással lehet a bevételszerzésre, ami viszont hatással lehet a termelőüzem pénzügyi stabilitására. A hitel– és követeléskockázatok [49] azok a kockázatok, amikor a vevői fizetések késése vagy a behajthatatlan követelések növekedése befolyásolhatja az üzem pénzforgalmát és pénzügyi teljesítményét. Pénzügyi jelentési hibák akkor is előfordulhatnak, ha a pénzügyi jelentések pontatlanságai vagy hibái megfelelési problémákhoz, hatósági ellenőrzésekhez vezethetnek, és károsíthatják a vállalat hírnevét.

Kamatkockázat az instabil gazdaságú országokban fordulhat elő [50]. Ha a gyártóüzem hitelt vett fel, a kamatlábak változása befolyásolhatja az adósság költségeit és az általános pénzügyi kiadásokat, így a pénzügyi stabilitást. Megfelelőségi és szabályozási kockázatok alatt azt értjük, amikor a pénzügyi előírások és a beszámolási kötelezettségek be nem tartása bírságot és jogi következményeket von maga után.

A piaci ár volatilitása is kockázatot jelent. A késztermékek vagy nyersanyagok piaci árának ingadozása befolyásolhatja az üzem jövedelmezőségét és egyéb beszállítói kockázatokat [51]. A kis számú beszállítóra való túlzott támaszkodás olyan kockázatoknak teheti ki az üzemet, mint például az ellátási lánc megszakadása, áringadozások és minőségi problémák. Az autóiparban a vevő által jóváhagyott beszállítót általában helyettesítő alternatíva nélkül fogadják el.

A rossz befektetési döntések vagy a tőkeprojektek befektetésének megtérülésének nem megfelelő értékelése pénzügyi veszteségekhez vezethet [52]. Stratégiai kockázatok akkor fordulhatnak elő, ha a pénzügyi stratégia és az átfogó üzleti stratégia közötti összhang hiánya olyan pénzügyi döntéseket eredményezhet, amelyek nem kedveznek a gyártó üzem hosszú távú sikerének.

Az adószabályok be nem tartása pénzbírsággal és jogi következményekkel járhat. Bár ennek előfordulása nagyon ritka, egyfajta kockázatot is jelent. Sokkal gyakoribb a munkavállalói csalás és kötelességszegés kockázata. Az adózók megelégedettsége a kormány és

az adóhatóság által nyújtott szolgáltatásokkal az adószabályok fokozottabb betartásával függ össze [53]. A pénzügyi osztályon belüli csaló tevékenységek vagy helytelen magatartások pénzügyi veszteségeket és jó hírnév-károsodást okozhatnak.

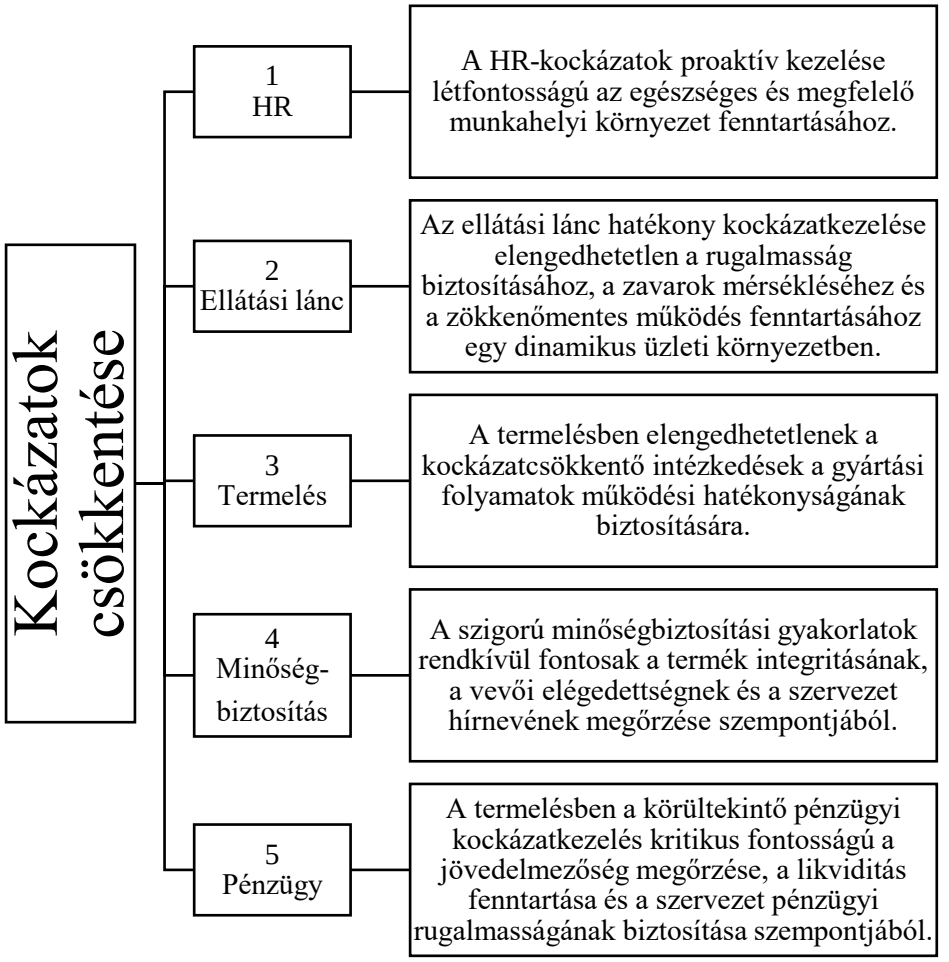
A gyártóüzemben a pénzügyi részleg kockázatainak csökkentése érdekében a szervezeteknek hatékony és eredményes pénzgazdálkodási gyakorlatot kell alkalmazniuk, rendszeres pénzügyi auditokat kell végezniük, tájékozódniuk kell a piaci trendekről, és diverzifikált beszállítói bázist kell fenntartaniuk. Ezenkívül a megfelelőségre való erős összpontosítás, a robusztus pénzügyi beszámolási rendszerek és a készenléti tervezés elengedhetetlen összetevői a hatékony kockázatkezelésnek a gyártóüzem pénzügyi részlegében.

KÖVETKEZTETÉSEK

Összefoglalva, az autóipar számos termelési kockázattal néz szembe, amelyek befolyásolják a hatékonyságot, a költséghatékonyságot és az általános sikert. A proaktív kockázatcsökkentési stratégiák azonban döntő szerepet játszanak a kihívások minimalizálásában és a gyártási folyamatok zavartalan működésének biztosításában. Az 1. ábra egy termelőüzem kockázatcsökkentését foglalja össze, bemutatva az öt leginkább érintett terület kockázatait.

A HR, a logisztika, a termelés, a minőség és a pénzügyek területén való eligazodás számtalan kockázat kezelésével jár, a tehetséggondozási kihívásoktól és az ellátási lánc zavaraitól a termelési hatékonyság hiányosságaiig, minőség-ellenőrzési problémákig és pénzügyi bizonytalanságokig. A hatékony kockázatcsökkentési stratégiák ezeken a területeken elengedhetetlenek ahhoz, hogy a szervezetek boldoguljanak a dinamikus üzleti környezetekkel szemben, biztosítva az optimális teljesítményt, megfelelőséget és a tartós sikert.

Az autóipar felismeri a proaktív kockázatkezelés fontosságát a termelés összetett kihívásaiban való eligazodásban. A technológiai fejlesztések felkarolásával, az ellátási láncok diverzifikálásával, az adatvezérelt tudás kihasználásával, az együttműködés elősegítésével, a szabályozási megfelelés biztosításával és a tehetségfejlesztésbe való befektetéssel a gyártók javíthatják a termelési kockázatok azonosítását és értékelését, valamint csökkenthetik képességeiket. Ahogy az ágazat folyamatosan fejlődik, a szilárd kockázatcsökkentő stratégiák iránti elkötelezettség elengedhetetlen lesz a tartós sikerhez és rugalmassághoz a folyamatosan változó globális környezetben.



1. ábra: Termelő üzem kockázatcsökkentése (a szerzők által készített)

FELHASZNÁLT IRODALOM

[1] W. L. Lin, „Corporate social responsibility and irresponsibility: Effects on supply chain performance in the automotive industry under environmental turbulence”, *J. Clean. Prod.*, köt. 428, o. 139033, nov. 2023, doi: 10.1016/j.jclepro.2023.139033.

[2] L. Varawala, M. R. Hesamzadeh, G. Dán, D. Bunn, és J. Rosellón, „A pricing mechanism to jointly mitigate market power and environmental externalities in electricity markets”, *Energy Econ.*, köt. 121, o. 106646, máj. 2023, doi: 10.1016/j.eneco.2023.106646.

[3] N. Piricz, „Management Challenges of Smart Grids”, in *Integration of Information Flow for Greening Supply Chain Management*, A. Kolinski, D. Dujak, és P. Golinska-Dawson, Szerk., in EcoProduction. , Cham: Springer International Publishing, 2020, o. 393–415. doi: 10.1007/978-3-030-24355-5_20.

[4] C. Rivera Domínguez, J. Eduardo Ramírez Guadian, J. Guerrero Lona, és J. Ivette Pozos Mares, „Hazard identification for risk assessment using the PRA technique in the

automotive industry", *Saf. Sci.*, köt. 160, o. 106041, ápr. 2023, doi: 10.1016/j.ssci.2022.106041.
[5] C. Cayrat és P. Boxall, „The roles of the HR function: A systematic review of tensions, continuity and change", *Hum. Resour. Manag. Rev.*, köt. 33, sz. 4, o. 100984, dec. 2023, doi: 10.1016/j.hrmr.2023.100984.
[6] M. Biggeri, L. Borsacchi, L. Braito, és A. Ferrannini, „Measuring the compliance of management system in manufacturing SMEs: An integrated model", *J. Clean. Prod.*, köt. 382, o. 135297, jan. 2023, doi: 10.1016/j.jclepro.2022.135297.
[7] J. Zuo, W. Zhang, M. Hu, X. Feng, és G. Zou, „Employee relations and stock price crash risk: Evidence from employee lawsuits", *Int. Rev. Financ. Anal.*, köt. 82, o. 102188, júl. 2022, doi: 10.1016/j.irfa.2022.102188.
[8] J. Liu, T. Wang, F. Yao, W. Pedrycz, Y. Song, és R. He, „Assessing growth potential of careers with occupational mobility network and ensemble framework", *Eng. Appl. Artif. Intell.*, köt. 127, o. 107306, jan. 2024, doi: 10.1016/j.engappai.2023.107306.
[9] Mészáros A. Á. és Tick A., „Az ipari kémkedéssel szembeni felkészültség vizsgálata a magyar szervezetek körében", *Biztonságtudományi Szle.*, köt. 3, sz. 4, Art. sz. 4, dec. 2021.
[10] C. M. Patterson, J. R. C. Nurse, és V. N. L. Franqueira, „Learning from cyber security incidents: A systematic review and future research agenda", *Comput. Secur.*, köt. 132, o. 103309, szept. 2023, doi: 10.1016/j.cose.2023.103309.
[11] Dér A., „A világ energiaellátása veszélyeinek meghatározása infokommunikációs stratégiák fogalmán és céljain keresztül", *Biztonságtudományi Szle.*, köt. 5, sz. 2, Art. sz. 2, jún. 2023.
[10] N. Piricz és B. Révész, „Lessons Learned from an Operational Smart Grid Through the Example of a Local Government in Hungary", *PÉNZÜGYI SZEMLE PUBLIC FINANCE Q. 1963-*, köt. 67, sz. 3, Art. sz. 3, 2022.
[13] Leisztner P., „A munkavédelmi képviselők szerepe a munkavédelmi feladatok ellátásában", *Biztonságtudományi Szle.*, köt. 5, sz. 2, Art. sz. 2, jún. 2023.
[14] D. Biermann-Teuscher, L. Thissen, K. Horstman, és A. Meershoek, „Safety: A collective and embedded competency. An ethnographic study of safety practices at an industrial workplace in the Netherlands", *J. Safety Res.*, nov. 2023, doi: 10.1016/j.jsr.2023.10.012.
[15] L. Molnár és Z. Tégla, „Logisztikai kihívások az autóiparban 2020-2023", *Acta Carolus Robertus*, köt. 13, sz. 2, o. 123–133, 2023.
[16] W. Zhou, H. Yang, Y. Dang, és B. Niu, „A novel mechanism in a dual-sourcing supply chain with supply disruption risk: The fraction-committed procurement contract", *Comput. Ind. Eng.*, köt. 186, o. 109712, dec. 2023, doi: 10.1016/j.cie.2023.109712.
[17] H. Bo, X. A. Chen, Q. Luo, és W. Wang, „Manufacturing rescheduling after crisis or disaster-caused supply chain disruption", *Comput. Oper. Res.*, köt. 157, o. 106266, szept. 2023, doi: 10.1016/j.cor.2023.106266.
[18] M. Liu, Z. Liu, F. Chu, F. Zheng, és C. Chu, „Integrated inventory management, supplier selection, disruption risk assessment problem under ripple effect", *IFAC-Pap.*, köt. 55, sz. 10, o. 3094–3099, jan. 2022, doi: 10.1016/j.ifacol.2022.10.204.

[19] T. Gao, J. Tian, C. Huang, H. Wu, X. Xu, és C. Liu, „The impact of new western land and sea corridor development on port deep hinterland transport service and route selection”, *Ocean Coast. Manag.*, köt. 247, o. 106910, jan. 2024, doi: 10.1016/j.ocecoaman.2023.106910.
[20] J. Rupp, N. Boysen, és D. Briskorn, „Optimizing consolidation processes in hubs: The hub-arrival-departure problem”, *Eur. J. Oper. Res.*, köt. 298, sz. 3, o. 1051–1066, máj. 2022, doi: 10.1016/j.ejor.2021.07.001.
[21] „Suez Canal Trade Disruptions 2024 | UPS Supply Chain Solutions - United States”. Elérés: 2024. február 4. [Online]. Elérhető: https://www.ups.com/us/en/supplychain/resources/news-and-market-updates/suez-canal-shipping-delays-2024.page
[22] S. To, „SAP BrandVoice: Suez Canal Crisis: Lessons Learned And How Tech Can Help”, Forbes. Elérés: 2024. február 4. [Online]. Elérhető: https://www.forbes.com/sites/sap/2024/01/22/suez-canal-crisis-lessons-learned-and-how-tech-can-help/
[23] G. Shen, L. Zhou, X. Xue, és Y. Zhou, „The risk impacts of global natural and technological disasters”, *Socioecon. Plann. Sci.*, köt. 88, o. 101653, aug. 2023, doi: 10.1016/j.seps.2023.101653.
[24] S. S. Padhi, S. Mukherjee, és T. C. Edwin Cheng, „Optimal investment decision for industry 4.0 under uncertainties of capability and competence building for managing supply chain risks”, *Int. J. Prod. Econ.*, köt. 267, o. 109067, jan. 2024, doi: 10.1016/j.ijpe.2023.109067.
[25] P. Chakrabarti és S. Sen, „Foreign currency borrowing and risk exposure of firms: An emerging market economy viewpoint”, *J. Policy Model.*, köt. 45, sz. 6, o. 1246–1261, nov. 2023, doi: 10.1016/j.jpolmod.2023.09.004.
[26] R. L. Rajani, G. S. Heggde, R. Kumar, és P. Chauhan, „Demand management strategies role in sustainability of service industry and impacts performance of company: Using SEM approach”, *J. Clean. Prod.*, köt. 369, o. 133311, okt. 2022, doi: 10.1016/j.jclepro.2022.133311.
[27] Q. Wang, H. Liu, F. Ore, L. Wang, J. B. Hauge, és S. Meijer, „Multi-actor perspectives on human robotic collaboration implementation in the heavy automotive manufacturing industry - A Swedish case study”, *Technol. Soc.*, köt. 72, o. 102165, febr. 2023, doi: 10.1016/j.techsoc.2022.102165.
[28] W. Qi, B. Li, Q. Liu, és J. Lv, „Low-skill lock-in? Financial resource mismatch and low-skilled labor demand”, *Finance Res. Lett.*, köt. 55, o. 104003, júl. 2023, doi: 10.1016/j.frl.2023.104003.
[29] X. Lai, Z. Chen, X. Wang, és C.-H. Chiu, „Risk propagation and mitigation mechanisms of disruption and trade risks for a global production network”, *Transp. Res. Part E Logist. Transp. Rev.*, köt. 170, o. 103013, febr. 2023, doi: 10.1016/j.tre.2022.103013.
[30] S. A. Babalola, D. Mishra, S. Dutta, és N. C. Murmu, „In-situ workpiece perception: A key to zero-defect manufacturing in Industry 4.0 compliant job shops”, *Comput. Ind.*, köt. 148, o. 103891, jún. 2023, doi: 10.1016/j.compind.2023.103891.
[31] V. S. Chinta, S. Kethi Reddi, és N. Yarramsetty, „Optimal feature selection on Serial Cascaded deep learning for predictive maintenance system in automotive industry with

fused optimization algorithm", *Adv. Eng. Inform.*, köt. 57, o. 102105, aug. 2023, doi: 10.1016/j.aei.2023.102105.
[32] Q. Wei, Y. Liu, Y. Dong, T. Li, és W. Li, „A digital twin framework for real-time ship routing considering decarbonization regulatory compliance", *Ocean Eng.*, köt. 278, o. 114407, jún. 2023, doi: 10.1016/j.oceaneng.2023.114407.
[33] E. Filippi, M. Bannò, és S. Trento, „Automation technologies and their impact on employment: A review, synthesis and future research agenda", *Technol. Forecast. Soc. Change*, köt. 191, o. 122448, jún. 2023, doi: 10.1016/j.techfore.2023.122448.
[34] V. Palea és C. Santhià, „The financial impact of carbon risk and mitigation strategies: Insights from the automotive industry", *J. Clean. Prod.*, köt. 344, o. 131001, ápr. 2022, doi: 10.1016/j.jclepro.2022.131001.
[35] L. Talens Peiró, N. Martin, G. Villalba Méndez, és C. Madrid-López, „Integration of raw materials indicators of energy technologies into energy system models", *Appl. Energy*, köt. 307, o. 118150, febr. 2022, doi: 10.1016/j.apenergy.2021.118150.
[36] „Japan's tsunami supply chain comeback". Elérés: 2024. február 4. [Online]. Elérhető: https://www.ft.com/content/c531d416-bc6b-11e0-acb6-00144feabdc0
[37] J. Zhou, Y. Liu, D. Liang, és M. Tang, „A new risk analysis approach to seek best production action during new product introduction", *Int. J. Prod. Econ.*, köt. 262, o. 108911, aug. 2023, doi: 10.1016/j.ijpe.2023.108911.
[38] J. Chen, P.-F. Hsieh, és K. Wang, „Cracking down on the infringement and counterfeiting: Intellectual property rights and corporate innovation in China", *Finance Res. Lett.*, köt. 55, o. 103846, júl. 2023, doi: 10.1016/j.frl.2023.103846.
[39] P. Della Corte, A. Jeanneret, és E. D. S. Patelli, „A credit-based theory of the currency risk premium", *J. Financ. Econ.*, köt. 149, sz. 3, o. 473–496, szept. 2023, doi: 10.1016/j.jfineco.2023.06.002.
[40] M. Mishra, S. K. Ghosh, B. Sarkar, M. Sarkar, és S. K. Hota, „Risk management for barter exchange policy under retail industry", *J. Retail. Consum. Serv.*, köt. 77, o. 103623, márc. 2024, doi: 10.1016/j.jretconser.2023.103623.
[41] Y. Shan, G. Zhang, Y. Shi, és H. Pang, „Synthesis and catalytic application of defective MOF materials", *Cell Rep. Phys. Sci.*, köt. 4, sz. 3, o. 101301, márc. 2023, doi: 10.1016/j.xcrp.2023.101301.
[42] K. Liu *és mtsai.*, „Risk identification and assessment methods of offshore platform equipment and operations", *Process Saf. Environ. Prot.*, köt. 177, o. 1415–1430, szept. 2023, doi: 10.1016/j.psep.2023.07.081.
[43] U. R. De Oliveira, L. Aparecida Neto, P. A. F. Abreu, és V. A. Fernandes, „Risk management applied to the reverse logistics of solid waste", *J. Clean. Prod.*, köt. 296, o. 126517, máj. 2021, doi: 10.1016/j.jclepro.2021.126517.
[44] X. Li és K.-M. Nam, „Environmental regulations as industrial policy: Vehicle emission standards and automotive industry performance", *Environ. Sci. Policy*, köt. 131, o. 68–83, máj. 2022, doi: 10.1016/j.envsci.2022.01.015.
[45] R. Li, N. Yang, H. Yi, és N. Jin, „The robustness of complex product development projects under design change risk propagation with gray attack information", *Reliab. Eng. Syst. Saf.*, köt. 235, o. 109248, júl. 2023, doi: 10.1016/j.ress.2023.109248.

[46] V. Azamfirei, A. Granlund, és Y. Lagrosen, „Lessons from adopting robotic in-line quality inspection in the Swedish manufacturing industry”, *Procedia Comput. Sci.*, köt. 217, o. 386–394, jan. 2023, doi: 10.1016/j.procs.2022.12.234.

[47] J.-P. Schöggl, R. J. Baumgartner, C. J. O’Reilly, H. Bouchouireb, és P. Göransson, „Barriers to sustainable and circular product design – A theoretical and empirical prioritisation in the European automotive industry”, *J. Clean. Prod.*, o. 140250, dec. 2023, doi: 10.1016/j.jclepro.2023.140250.

[48] A. H. Alami *és mtsai.*, „Additive manufacturing in the aerospace and automotive industries: Recent trends and role in achieving sustainable development goals”, *Ain Shams Eng. J.*, köt. 14, sz. 11, o. 102516, nov. 2023, doi: 10.1016/j.asej.2023.102516.

[49] L. Lind, M. Pirttilä, S. Viskari, F. Schupp, és T. Kärri, „Working capital management in the automotive industry: Financial value chain analysis”, *J. Purch. Supply Manag.*, köt. 18, sz. 2, o. 92–100, jún. 2012, doi: 10.1016/j.pursup.2012.04.003.

[50] C. Claußen és D. Platte, „Evaluating the validity of regulatory interest rate risk measures – a simulation approach”, *J. Bank. Finance*, köt. 154, o. 106933, szept. 2023, doi: 10.1016/j.jbankfin.2023.106933.

[51] K. E. Bartos, J. Schwarzkopf, M. Mueller, és C. Hofmann-Stoelting, „Explanatory factors for variation in supplier sustainability performance in the automotive sector – A quantitative analysis”, *Clean. Logist. Supply Chain*, köt. 5, o. 100068, dec. 2022, doi: 10.1016/j.clscn.2022.100068.

[52] R. Colombari *és mtsai.*, „The interplay between data-driven decision-making and digitalization: A firm-level survey of the Italian and U.S. automotive industries”, *Int. J. Prod. Econ.*, köt. 255, o. 108718, jan. 2023, doi: 10.1016/j.ijpe.2022.108718.

[53] A. Lutfi *és mtsai.*, „Enhancing VAT compliance in the retail industry: The role of socio-economic determinants and tax knowledge moderation”, *J. Open Innov. Technol. Mark. Complex.*, köt. 9, sz. 3, o. 100098, szept. 2023, doi: 10.1016/j.joitmc.2023.100098.

PHYSICAL PROTECTION CHARACTERISTICS OF CRITICAL INFRASTRUCTURES HUNGARY – THE ARMED SECURITY GUARD

A KRITIKUS INFRASTRUKTÚRÁK FIZIKAI VÉDELMI SAJÁTOSSÁGAI MAGYARORSZÁGON – A FEGYVERES BIZTONSÁGI ŐRSÉG

BORUZS Hunor [1]

Abstract

The protection of activities, facilities and supplies - also known as critical infrastructure elements or vital system elements - that are of paramount importance for the functioning of the state and the provision of services to the population, is ensured by the state through various organisations, which have a monopoly on the use of force. In Hungary, these organisations include the armed security guards operating under Act CLIX of 1997 on the Armed Security Guard, Nature Protection and Field Guard Service (hereinafter referred to as the "Armed Security Guard Act"). However, the concept of armed security guards in this context covers more than just security guards on duty with weapons: although the organisation does not belong to the law enforcement agencies and is civilian in nature, its powers within the premises are essentially the same as those of the police.

Keywords

police officer, armed security guard, security guard, physical protection, critical infrastructure

Absztrakt

Az állam működése, valamint a lakosság ellátása szempontjából kiemelten fontos tevékenységek, létesítmények, szállítmányok – más nevükön a kritikus infrastruktúra elemek, avagy a létfontosságú rendszerelemek – védelméről az állam az erőszak monopóliuma biztosításával különböző szervezetek által gondoskodik. Magyarországon ezen szervezetek közé tartoznak a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról szóló 1997. évi CLIX. törvény (a továbbiakban: Fbő tv.) alapján működő fegyveres biztonsági őrségek is. A fegyveres biztonsági őrség fogalma azonban itt többet takar a fegyverrel szolgálatot ellátó biztonsági őröknél, a szervezet ugyan nem tartozik a rendészeti szervekhez, jellege polgári, azonban a jogosultságaik az objektumon belül lényegében megegyeznek a rendőrökével.

Kulcsszavak

rendőr, fegyveres biztonsági őr, személy- és vagyonőr, fizikai biztonság, kritikus infrastruktúra

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

INTRODUCTION

Critical infrastructures are a network of interconnected, interacting, interactive and interdependent infrastructure elements, facilities, services, systems and processes that are considered vital to the functioning of the state, i.e., the population, economy and government, and have a substantive role in establishing and maintaining a socially desirable minimum level of legal certainty, public safety, national security, economic viability, public health and environmental condition. In the aftermath of the world-shaking attacks of 11 September 2001, critical infrastructure protection and its issues have become more prevalent in Europe similarly to many other parts of the world.

There is a myriad of solutions for the robust implementation of physical protection of critical infrastructure in Hungary and internationally. We regard the Hungarian model of armed security guarding as a Hungarian phenomenon, an organisation which is civilian in nature, yet with public authority.

CRITICAL INFRASTRUCTURES

In the European Union, the first Community legislation at the level of a directive is Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (hereinafter: ECI Directive), which was implemented in Hungary by Act CLXVI of 2012 on the Identification, Designation and Protection of Vital Systems and Facilities (hereinafter: Lrtv.). The purpose of the regulation is to identify and designate critical system elements and to ensure the establishment and operation of full protection. In addition to defining the basic concepts, the Act provides for and regulates the designation of national and European critical system elements, the obligation to prepare an operator's security plan, the designation of the security liaison officer, the rules on registration and control, and sanctions.

National Critical Infrastructure Designation in Hungary

The Lrtv lists in Annex 1 the relevant service sectors and subsectors, which are:

1. Energy
    - power system installations (excluding systems and components subject to the regulations on nuclear safety and radiation protection, physical protection and safeguards of nuclear power plants)
    - petroleum industry
    - natural gas industry
    - district heating
2. Transport
    - road transport
    - rail transport
    - air transport
    - water transport
    - logistics centres
3. Agricultural economy
    - agriculture

- food industry
- distribution networks

4. Health
    - active inpatient care and the services needed to run it
    - rescue management
    - health reserves and blood stocks
    - high security biological laboratories
    - pharmaceutical wholesale
5. Social security
    - IT systems and records for claiming social security benefits
6. Finance
    - infrastructures and systems for trading, payments, clearing and settlement of financial instruments
    - bank and credit institution security
    - cash supply
7. Info communication technologies
    - internet access service and internet infrastructure
    - electronic communications services, electronic communications net-works
    - broadcasting
    - postal services
    - meteorological infrastructure
    - government electronic information systems
8. Water
    - drinking water services
    - monitoring surface water and groundwater quality
    - sewage disposal and treatment
    - protecting aquifers
    - flood defences, dams
9. Defence
    - defence systems and installations
10. Public safety and security
    - law enforcement infrastructures

All operators in one of the listed sectors, regardless of the type of service they provide, are required to carry out an identification test. The assessment should include analysis and evaluation of the risks to the provision of the various services, the fulfilment of sectoral and horizontal criteria and the possibility of designation as a service provider. The relevant horizontal criteria are:

1. Economic impact criterion
2. Criteria for political impact
3. Social impact criterion
4. Environmental impact criterion
5. Losses criterion
6. Protection criterion

The identification report produced as a result of the investigation should include the outcome of the investigation and a proposal for designation as a national or European Critical System Element. The operator has 60 days from the date of provision of the service or entry into force of the law to do so.

The operator shall submit the completed identification report to the sectoral designating authority designated in the sectoral government decree within 8 days of its completion. The sectoral designating authority shall verify the compliance of the report with the requirements of the report by involving a competent authority in the designation procedure. If at least one sectoral criterion and at least one horizontal criterion are met, the sectoral designating authority shall designate the critical system element or service and order its registration and order its inclusion in the list of operators providing essential services if the requirements of Article 2/A (2) of the Lrtv. are met with regard to the system element operated by it. In addition, it provides for the obligation to draw up an operator security plan, the deadlines for its preparation and submission, and the employment of a security liaison officer.

The specialised authority (the central body of the professional disaster management bodies) is the body that issues opinions on the fulfilment of the horizontal criteria (National Tax and Customs Administration, the Office for the Protection of the Constitution, the Counter-Terrorism Centre, the Counter-Terrorism Information and Crime Analysis Centre, the National Directorate General for Aliens, the territorially competent government commissioner, the territorial environmental protection authority, the territorial water management and protection authority, the territorial body of the professional disaster management body).

Essential Service Providers are organisations or economic operators that provide an essential service to ensure the provision of vital social and/or economic processes and functions and that depend on electronic information systems for the provision of that service, and where a security incident affecting their service would cause a significant disruption to that service, and have been identified as an Essential Service Provider in the procedure for that purpose. The Directive has identified seven essential service sectors, namely:

1. Energy
2. Transport
3. Health care facilities
4. Digital infrastructure
5. Banking services
6. Financial market infrastructures
7. Drinking water supply and distribution

The Hungarian regulation on the designation of essential service providers is twofold, with one part being designated by the operators of the critical system element and the other part being designated by the National Security Service.

In Hungary, Act L of 2013 on the Electronic Information Security of State and Local Government Bodies regulates the information security framework of critical systems and facilities, which are supervised by the National Security Service, in addition to state and local government bodies.

The designated national critical system operator must arrange for the assignment or employment of a security liaison officer within 60 days of the designation decision becoming final, and must provide the details of the security liaison officer to the registering authority (BM OKF) within 60 days.

The operator of the designated national critical system element must prepare an operator security plan in accordance with the Lrtv. within the time limit set in the designation decision. The document must be submitted to the sectoral designating authority within the specified time limit, which, after checking the content and form requirements, sends it to the registering authority.

Every 5 years, the central body of the disaster management body carries out a complex audit of the designated national critical control element, which may include the sectoral designating authority, the specialised authority, the body involved in the designation procedure and the body entitled to carry out an on-site audit under the legislation.

The vision under the new CER Directive

Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisms, which entered into force on 1 January 2022, replaces the previous Council Directive 2008/114/EC. The new Directive brings a number of important changes to the regulation and protection of critical infrastructure in the EU.

The new directive starts by expanding the definition of critical infrastructure. In the 2008 directive, critical infrastructure referred only to facilities that provide essential services such as water, energy, food or transport. However, the new directive extends this concept to digital infrastructure such as data centres, information systems, telecommunications networks and internet services.

Another important change in the new directive is that the essential services defined in the previous directive are now extended to the category of "essential services". Essential services include essential services, but also other important services such as financial services, health services, distance learning and e-government.

The new directive also requires the organizations concerned to have a "resilience plan" to prepare for unexpected situations such as natural disasters, cyber attacks or even pandemics. The resilience plan should include activities to enable the organizations concerned to identify, prevent and manage such contingencies and to guarantee continuity in the provision of essential services.

The new directive also stresses the importance of cooperation between actors. Relevant organizations must work together with the competent authorities, as well as with industry partners and civil society organizations, to ensure the protection and continued operation of critical infrastructures. In particular, the Directive emphasises cross-border cooperation to enable the organizations concerned to prevent and manage potential cross-border threats.

The new Directive also requires relevant organizations to have the right staff, technology and processes in place to protect their infrastructure from cyber attacks and other threats. The directive also proposes the importance of standardization to facilitate industry partnerships and cross-border cooperation.

Overall, Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisations brings a number of important changes to the regulation and protection of critical infrastructure in the EU. The Directive aims to ensure that the organisations concerned are better prepared for unexpected situations and take appropriate measures to maintain critical services that are key to the lives of EU citizens and to economic development.

PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE

The importance, significance, purpose and function of a given infrastructure have a decisive impact on the level of security. The following factors should be taken into account when determining the level of security:

1. Physical characteristics of the property
    - size of the floor area
    - number of floors of buildings
    - length of boundary lines, protection
    - architectural solutions
    - different levels of protection zones
    - mechanical, electronic, life safety systems and regime control
2. Degree of vulnerability of the property to be protected
    - type of service
    - the degree of vulnerability of the service
3. Criminal contamination of the environment
4. Level of vulnerability of the safeguarded assets
    - property values
    - irreplaceable national values
    - confidential information, technologies
    - activities of major importance for the functioning of the State or the provision of services to the public
5. Some subjective characteristics of human resources
6. Disaster management assessment
7. Energy, communications, logistics security of supply

In Hungary, the live physical protection of critical infrastructure elements is not uniform, but involves private security services, the Hungarian Defence Forces, the Police and the Armed Security Guard, which is considered a hungaricum.

THE ARMED SECURITY GUARD

In Hungary, armed security guards shall be used to protect activities, facilities and cargoes that are of paramount importance for the operation of the State or the supply of the population, if the Hungarian Defence Forces and law enforcement agencies under this Act, the Parliamentary Guard providing security for Parliament or the National Tax and Customs Administration are not legally obliged to provide such protection, but the guarding is justified in the interests of public security or the protection of national property.

Definition of armed security guarding, relevant legislation

Armed security guards are defined in the Fbő tv. 3. According to the first paragraph of § 3 of the Armed Security Guard Act, it is *"a security organisation with specific guarding tasks, with service weapons and other coercive means, with special rights, whose members are employed by establishing or operating state, municipal or other institution, economic organisation, or are civil servants, employees of the national defence, or are employed by the law enforcement agency or are in the law enforcement administrative service of the agency"*.

To understand exactly where armed security guards fit into the system, we need to look at the police as a complex system. Law enforcement is part of the public administration, whose mission is to maintain internal order and public order and security, to protect the members of society and their fundamental values by preventing or stopping offences that violate or endanger them, including through the use of legitimate physical force. This is an extremely complex and multifaceted activity which cannot be expected to be carried out exclusively by a single public body, namely the police. Security can be achieved through social cooperation and collective work, in which, in addition to the police and the bodies responsible for law enforcement, local authorities, private security companies and civilian self-defence organisations also have an important role to play. This can also be described as a complementary policing system, in which the activities of state bodies are complemented, supported and assisted by market and civil organisations. These include the police, the penitentiary system, the professional civil protection services and the civilian national security services. The Parliamentary Guard and the National Tax and Customs Office are also law enforcement agencies. So-called complementary law enforcement bodies include organisations with specific law enforcement functions, in particular municipal law enforcement, voluntary associations for the prevention of crime, in particular the civil guard, and private security (protection of persons and property). [10]

Armed security guards, in the system we have examined, can be classified as complementary law enforcement agencies, and within that, as those performing specific law enforcement functions. Thus, today in Hungary, in accordance with the definitions of the legislation in force, armed security guards are responsible for a huge share of the protection of activities, facilities, cargoes and national assets of irreplaceable value, i.e., critical infrastructure elements, which are of paramount importance for the functioning of the state and the supply of the population.

Field of application

Armed security guards shall protect the critical infrastructure elements mentioned above if the protection is not required by law to be provided by the Hungarian Defence Forces, law enforcement agencies under the Act on the Status of Members of the Government and State Secretaries, the Parliamentary Guard providing security for Parliament, or the National Tax and Customs Administration, but is justified in the interests of public security or the protection of national property.

So especially:

1. a facility important for the security of the State or for national defence;
2. an airport with international passenger or freight traffic;

3. activities related to the use, production, storage, distribution, transport of explosive, flammable, toxic material, or that of being hazardous to health or the environment, which could cause a disaster, as well as nuclear and other radioactive material, nuclear installations as defined by law;
4. elements of the infrastructure and utilities system that provide the basic needs of the population;
5. a national, cultural asset of major importance;
6. the flagship facility of the postal service, the central facility for public service, radio and television, and telecommunications systems.

Professional supervision

In Hungary, the police headquarters of the counties (capitals) and the police headquarters operate as organs of the competent police headquarters, with independent duties and powers - on the basis of the Government Decree 329/2007 (XII. 13.) on the organs of the Police and the duties and powers of the Police. The National Police Headquarters (hereinafter referred to as ORFK) is the central management body of the police headquarters and the bodies of the general police body established to perform certain tasks. Within its administrative competence, the ORFK ensures the conduct of the administrative authority procedures assigned to it, performs official, registration and control tasks, including:

- performs official duties relating to the establishment, operation and termination of the armed security guard, as well as the ordering of armed security guards and the authorisation of the armed security guard to be armed with firearms, ammunition and other coercive means,
- authorises the armed security guards to be supplied with firearms, ammunition and other coercive means,
- performs the tasks of the authority defined for armed security guards operating in several counties or nationally and within the organisation of the penitentiary organisation and the bodies under its control, and supervises the activities of these armed security guards,
- supervises and monitors the activities of the police headquarters of the county (capital) and the Airport Police Directorate in relation to armed security guards,
- carry out official tasks not assigned to another body,
- at the second instance, hear appeals against first instance decisions of local bodies under Article 10/A of the Act on the General Administrative Procedure on the basis of complaints under Article 10/A of the Act on the General Administrative Procedure, and in these cases act as a supervisory body under the Act on the General Administrative Procedure,
- in the first instance, adjudicate on a complaint within the competence of the police pursuant to Section 10/A of the Police Act
- verify the implementation of the Decision by means of official controls;
- issue, revoke, temporarily withdraw and register the official service card of an armed security guard at the expense of the debtor or the organisation operating the FSA;
- approves by decision the watch instructions and guard instructions of the FOPC;

- monitors the provision of services by the GSA in the framework of an official control;
- order an enhanced duty, alert;
- checks the information needed to assess the suitability of the armed security guard;
- investigate the use of coercive measures and measures restricting the personal liberty of the DPO from a legal and professional point of view;
- may, during a special legal period, request the Minister for Police to take over the command of the FPS from the police;
- supervises, monitors and exercises professional supervision over the training, education and further training activities of the JIT, and conducts the examinations of the JIT;
- issue the service badge of the FDPIC at the expense of the debtor or the organisation operating the FDPIC.

There may be more specific cases where a patrol is not created by a police body, but by organisations within their own organisation with the right to create a patrol. They can be established by the Minister responsible for defence in relation to the installations of the Hungarian Defence Forces requiring increased protection and the installations of the Military National Security Service, as well as in relation to the installations of a company under the ownership of the Minister responsible for defence. By the Minister responsible for the management of civil intelligence activities, in relation to the facilities of the Information Office. By the Minister responsible for the management of the civil national security services, in respect of the installations of the civil national security services under his control. In the cases listed here, professional supervision and official authority are exercised by the ministers responsible for the areas concerned.

Forms of service, hierarchy

The service can be divided into hierarchical ranks, according to the hierarchical order typical of military organisations, i.e., superiors and subordinates. A superior is a person who, on the basis of a guard order or a guard instruction, directs a subordinate, even temporarily, and has the right to give instructions. The superior officer shall be responsible for supervising the execution of the instructions. A subordinate is a person who is assigned to a superior officer, whether permanently or temporarily, and is required to obey his orders. The organisation shall be headed by the commander of the guard, who shall have authority over the whole guard. Depending on the number of guards, additional deputy sergeant-major posts may be created. The daily rotation is managed by the sergeant-major and in his absence, for example during rest periods, he is relieved by the deputy sergeant-major. Guard patrols may perform the duties of posted guard, patrol, escort, or guard escort.

Clothing, badges

Armed security guards shall be provided with uniforms and service insignia, which shall be different from the uniforms of the Hungarian Defence Forces, central state administration bodies, law enforcement bodies under the Act on the Status of Members of the Government and State Secretaries, the uniform of the Parliamentary Guard providing security for Parliament, and the uniform of the professional staff of the National Tax and Customs Administration.

The rules for the wearing, supply and replacement of uniforms are usually set by employers according to their financial means. The uniform to be introduced must be subject to an opinion of the competent supervisory body. The uniforms issued are the property of the employer. The uniform shall remain in the possession of the Controller until the termination of employment and it shall be his duty and obligation to keep it in safe custody, use it for its intended purpose and preserve it. The uniform may be worn only in the performance of his duties or for the purpose of travelling to or from work, and may not be worn at any other time. No alteration other than to fit the body is permitted. The clothing shall bear the employer's name, insignia, rank, name badge and shall be clearly visible. [11]

Rights of action, use of coercive measures

An armed security guard is a person authorised to carry a weapon on duty, performing public and law enforcement duties. Armed security guards are equipped with the following means of coercion:

- Chemical device;
- Police baton;
- Handcuffs;
- Service dog (optional);
- Marksman's rifle;
- A firearm that can be fired in bursts on special order.

An armed security guard is entitled and obliged to order a person who violates or endangers security to stop his/her activity and check his/her identity, to detain a person who actively resists his/her action or is caught in the act of committing a crime or an offence against property until the police arrive, and to take from the person stopped, detained or arrested the object or instrument of the crime or the means of attack, and to search his/her clothing and luggage for this purpose. The use of means of coercion becomes justified when the person subject to the measure does not comply with the request or does not cease his or her activities which are prejudicial or dangerous. The armed security guard is then entitled to use coercive means to stop the person, subject to strict compliance with the requirement of proportionality and the conditions of use laid down by law. The latter means that the person concerned must be warned in advance of the use of force, if the circumstances of the case so permit, and that, if it is used, the use of force must be avoided, in particular the infliction of injury or the taking of human life. The person injured during the action must be assisted as soon as possible and, if necessary, the armed security guard must ensure that the injured person is attended by a doctor. In the event of the use of a firearm, the use shall be preceded by a call to obey the security guard's order, the use of other means of coercion, a warning that a firearm is to be used, a warning shot. However, where, in the circumstances of the case, there is no time for preventive measures and the delay results in the attack directly endangering the protected establishment, property or activity, preventive measures may be partially or totally waived. On the basis of proportionality, the armed security guard may use physical force to compel the person subject to the measure to act or to cease acting, or may use a service dog with or without a lead and with a muzzle. He may use handcuffs to prevent the escape of a restrained person or, when carrying out a guard or escort duty, to prevent a person whose personal liberty is restricted from escaping or self-harming. He may

use a chemical or electric shock device, a police baton or an unleashed service dog on a lead to prevent assault or to break resistance to the measure. The most serious means of coercion, i.e., firearms (and muzzled and unleashed service dogs), may be used by an armed security guard in the event of an armed or armed attack on an activity, establishment or transport of vital importance for the functioning of the State or the provision of services to the public.

Training, examinations

In Hungary, an armed security guard may be a Hungarian citizen or a person with the right of free movement and residence under a separate law, who has reached the age of eighteen, is able to carry a weapon and has the qualifications required for the position. A criminal record is an exclusion criterion. In the case of both existing and trainee armed security guards, the professional examination must be taken before a professional examination board made up of representatives of the police headquarters supervising the guard and of the organisation responsible or of the organisation operating the guard. Every two years, the theoretical and practical competence of armed security guards shall be verified by means of a professional examination before the aforementioned examination board. The knowledge assessment is composed of two major modules, theory and practice, for the armed security guards operating in Hungary. However, in the case of armed security guards guarding nuclear and other radioactive material, nuclear installations, a physical fitness assessment shall also be carried out, as provided by law. The theoretical part of the test covers legal and professional knowledge, while the practical part covers self-defence and shooting skills. A regulation regulates the structure of the questions and topics of the theoretical examination and the tasks to be carried out during the practical part. The examination of shooting skills must be carried out annually by the professional commission, on the basis of the criteria of the legislation on professional examinations. In order for armed security guards to be able to carry out their duties with excellence, it is necessary that, in addition to the above-mentioned official training and examinations, they should be continuously upgraded and receive special training in the management of large-scale incidents. These are essential if armed security guards are to have the theoretical and practical knowledge they need, together with the ability to respond to extraordinary and unusual events, so that they can act lawfully and professionally during their period of service, if necessary.

SUMMARY

In summary, it is clear how important the role of the armed security guard is in the Hungarian critical infrastructure protection system. The organisation is unique in that it is not a law enforcement agency, it is civilian in nature, but the state provides it with the legitimate use of force that results from its monopoly on the use of force through legislation. [12] The law enforcement challenges of our time make it imperative to place a high priority on the protection of our national vital systemic elements. Current EU efforts can provide a solution to strengthen the regulatory framework, but the degree of physical security remains a matter for national states. The Hungarian model of armed security guarding can serve as a model at international level, as it can guarantee a significantly higher level of security than private security services, without tying up the capacities of law enforcement agencies and the armed forces.

REFERENCES

[1] Act CLIX of 1997 on the Armed Security Guard, Nature Conservation and Field Guard Service
[2] Act XLIII of 2010 on Central State Administration Bodies and the Status of Members of the Government and State Secretaries
[3] Act CLXVI of 2012 on the Identification, Designation and Protection of Vital Systems and Facilities
[4] Act L of 2013 on the Electronic Information Security of State and Local Government Bodies
[5] 24/1997 (III. 26.) BM Decree on the scope of facilities of priority for the operation of the state and the supply of the population
[6] 27/1998. (VI. 10.) BM Decree on the Rules of Operation and Service of the Armed Security Guard
[7] 70/2012 (XII. 14.) BM Decree on the detailed rules for the clothing of persons performing law enforcement duties and armed security guards
[8] Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[9] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisms
[10] László Christián: *Law enforcement agencies*, Internet Encyclopaedia of Law, 2018
[11] László Christián, Zsolt Lippai: *The regulation of personal and property protection activities*, Ludovika University Publishing House, 2022
[12] Hunor Boruzs: Theoretical protection capabilities of the police officer, the armed security guard and the security guard, *Safety and Security Sciences Review*, vol. III., no. 2., pp. 105-113., 2021

ATTACK TRENDS AGAINST CRITICAL INFORMATION INFRASTRUCTURE SYSTEMS

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA RENDSZEREI ELLEN INTÉZETT TÁMADÁSI TRENDEK

DÉR AttilaTibor [1] BUSA Attila József[2]

Abstract

Based on the experience of the past few years, it is safe to say that attacks against critical infrastructures are an increasing percentage of the attackers' target. Attackers are increasingly focusing on developing and upgrading the toolkits used to prepare these attacks. Critical object defences need to be equipped with a similar intensity against external threats. As a consequence, one of the most important starting points is to provide critical infrastructure protection managers with an adequate picture of attack trends. This information can then be used to decide in which direction to organise and innovate individual defence systems and where to concentrate and divert resources. In this article, we briefly explain the background of cyber threats, some possible alternatives to supply chain attacks, and finally analyse the ENISA report and make suggestions for a more effective and modernised method of defence.

Keywords

Strategy, cybersecurity, Information security, legal regulation, critical infrastructure.

Absztrakt

Az elmúlt évek tapasztalatai alapján biztosan kimondható, hogy a támadók célkeresztjében egyre nagyobb százalékában vannak jelen a kritikus infrastruktúrák elleni támadások. A támadók egyre nagyobb figyelmet szentelnek, ezen támadások előkészítéséhez használt eszközparkok fejlesztésére és korszerűsítésére. A kritikus objektumok védelmeit is hasonló intenzitással kell felvértezni a külső fenyegetésekkel szemben. Ennek következtében az egyik leglényeges kiindulási pont, hogy a támadási trendekről megfelelő képet kapjanak a kritikus infrastruktúrák védelmi vezetői. Ezen információk alapján lehet, majd eldönteni melyik irányban kell szervezni, illetve fejleszteni az egyes védelmi rendszereket, hová kell csoportosítani, illetve elvonni erőforrásokat. Ebben a cikkben a röviden kifejtjük kiberfenyegetések hátterét, ellátási lánc ellen irányuló támadások néhány lehetséges alternatíváját. végül elemezzük az ENISA jelentését és javaslatot teszünk egy hatékonyabb és korszerűbb védekezési módszerekre.

Kulcsszavak

Stratégia, kiberbiztonság, információbiztonság, jogi szabályozás, kritikus infrastruktúra.

[1] der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] busa.attila@phd.uni-obuda.hu | ORCID: 0009-0009-6167-2154 | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Napjainkban az információs rendszerek főként a kritikus infrastruktúrák védelme egyre jobban felértékelődik gazdasági és nemzetbiztonsági érdekek összefonódása következtében. Az egész világon fontos kiberbiztonsági stratégia a kritikus infrastruktúrák védelme és a már bekövetkezett támadások enyhítésének segítése. Erre a nemzetállamok külön figyelmet fordítanak jogszabályi szinteken és egyéb szabványosítások és iránymutatások terén. Európában a hálózati és információs rendszerek biztonsága NIS 2 (Network and Information Systems Directive) direktívában már jól tükröződnek ezek a törekvések, hogy egy egységes zászló alatt kell felvonultatni a kibervédelmet érintő főbb stratégiai kérdéseket, hogy majd később nemzetállamok szintjén ne legyenek nagy eltérések a különféle nézetek és elképzelések között. Több szervezetet is alapított erre az Unió, hogy a tagállamokat egy mederbe terelje és ez által egy egységes erős védelmet alakítson ki. Az egyik ilyen szervezet az Európai Unión belül az ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában.

KIBERTÁMADÁSOK ÁLTALÁNOSSÁGBAN

Ahhoz, hogy megértsük a kibertámadások trendjeit, fontos tisztázni néhány alapvető kibervédelmi fogalmi rendszert. A kiberfenyegetések hátterében rengeteg féle okot találhatunk a szakirodalomban. Az akarat lenne a legkézenfekvő közhelye ennek a gondolatkörnek, de nyilvánvaló nem elégséges feltétele egy támadás kivitelezéséhez. Így kell a szándékhoz megfelelő motiváció is, amely későbbiekben lesz kifejtve bővebben a tanulmányban, de annyit „elárulhatok", hogy nem mindegy, hogy megkora nyeresége, illetve haszna lesz ebből a támadónak, mint anyagi és mint szakmai téren. Tovább folytatva általánosságban a támadás feltételrendszerét, minél összetettebb egy kibertérben bekövetkezett behatolás, annál több szaktudásra és időre van szükség. A szaktudás külön nem ecsetelném, viszont az ehhez hozzácsapott évek alatt felhalmozott szakmaspecifikus gyakorlatot már igen, ahol az elkövetők akár tesztkörnyezetben vagy éles helyzetekben már bizonyították szakmai rátermettségüket. A szakmai fortélyok illetve trükkök elengedhetetlen feltételei, hogy valaki éles környezetben egy sikeres támadást hajtson végre egy kiszemelt létesítmény ellen. Meg kell még említeni az anyagi és a támadást segítő eszközök forrásait, amelyek nem az utolsó szempontok a fent nevesített szándék tettleges formába öntésére. Sőt az egyes szerzők által emlegetett különféle fenyegetési formákra is nagymértékben hatással vannak, mint kiberterrorizmus, kiberbűnözés, kiberkémkedés stb.

Ha a szaktudást és a mögötte megbúvó erőforrásokat vesszem alapul, akkor a következő képpen osztályozhatok: A legalsó kategóriába vannak, akiknek nincs képességük, hogy saját támadási eljárást dolgozzanak ki és csak kész termékből dolgoznak, nyomot hagynak és csak egyszerűbb sérülékenységeket használnak ki. Középen helyezkednek el az úgymond erős szaktudással, de kevés erőforrással rendelkező támadók, akik elsősorban becsvágyból illetve szakmai tudásukból fakadó kíváncsiságból elégítik ki ezen hajlamukat. A tevékenységük irányulhat a rendszerek hiányosságainak felderítésére, a hiányosság javításának kikényszerítésére, de irányulhat a támadott rendszer kompromittálására is. Egy adott célcsoportra kiélezett informatikai támadások, ahol inkább ideológiai háttér a legfőbb

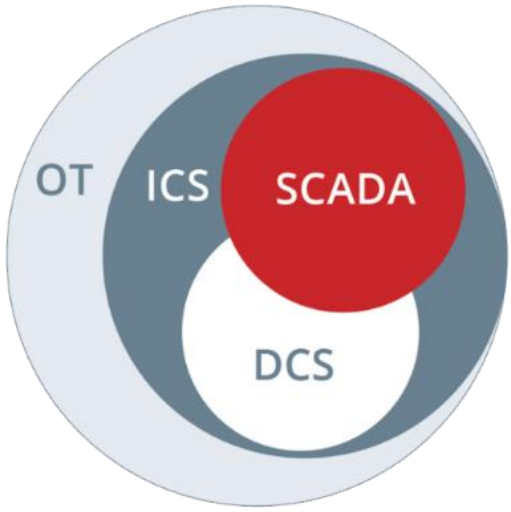
motiváció. A tagok szimpátia alapján alkotnak egy közösséget egy szervezet zászlója alatt, a legfőbb mozgatórugó nem a rombolás, hanem a figyelemfelhívás. A másik csoportosulás, ahol a tagok csak haszonszerzés reményében csatlakoznak egy bűnözői szervezethez. Itt van lehetőség drága eszközök használatára, káros programok elkészítésére, illetve megvételére. Így ezen a szinten már meg van a lehetősége az úgynevezett APT (Advanced Persistent Threat): jellegű támadási megoldásokra is. Az APT olyan informatikai adatszerzésre, illetve irányuló módszer, ahol távolról kiadott irányításnak megfelelően különféle kódok és parancsok folyamatosan és észrevétlenül fejtik ki hatásukat. Végül ennek a csoportosításnak a csúcsa, ahol az állam is valamilyen szinten közreműködik, illetve teljes mértékben szerepet vállal egy kibertámadási forgatókönyvben. Rengeteg anyagi és emberi erőforrás áll rendelkezésre, sok az ismert faktor főként saját ország határain belül.

Az elérni kívánt cél elérése szempontjából is megkülönbözhetünk támadásokat úgy, mint: Sérülés, szivárgás, megtagadás. Továbbá lehetséges még az információs rendszer működésének teljes vagy részleges működésének irányítása a fenyegető általi kompromittálása is.

Ezeknél a módszereknél jellemző veszélyeztetési formula, ahol az agresszor a rendszer vagy annak egyes elemeit a rendszer módosítása nélkül, külső úgynevezett szolgáltatásmegtagadással járó támadást (Denial of Service vagy DoS) vagy elosztott szolgáltatásmegtagadással járó támadást (Distributed Denial of Service vagy DDoS) hajt végre. Ezen támadások jellemzően rövid ideig tartanak, és intenzitásuk nagy mértékben függ a támadás végrehajtójától.[1]

OT SECURITY SZEREPE A KRITIKUS INFRASTRUKTÚRÁKNÁL

Az üzemeltetési technológia (OT) olyan hardver és szoftver, amely az ipari berendezések, eszközök, folyamatok és események közvetlen felügyelete és/vagy ellenőrzése révén változást észlel vagy okoz. Az OT-n belül megjelennek az ipari vezérlőrendszerek (ICS) és ezen belül a SCADA és DCS rendszerek (1. ábra: Az üzemeltetési technológiák felépítése1. ábra).



1. ábra: Az üzemeltetési technológiák felépítése

Az "OT security" az "Operational Technology security" rövidítése, és olyan intézkedéseket és technológiákat foglal magában, amelyeket az ipari technológiák védelmére terveztek. Az üzemeltetési technológia biztonság tehát a fizikai eszközök, folyamatok és események megfigyelésében és/vagy ellenőrzésében részt vevő személyek, eszközök és információk védelmére használt gyakorlatok és technológiák összessége. Ez a terület különösen fontos a kritikus infrastruktúrákban, ahol az ilyen típusú technológiák irányítják és felügyelik az energiahálózatokat, vízkezelő rendszereket, közlekedési rendszereket és egyéb kulcsfontosságú infrastruktúrákat.

Az OT security tehát azokat a védelmi intézkedéseket jelenti, amelyek a kritikus infrastruktúrákat üzemeltető rendszerek, eszközök és folyamatok biztonságát szolgálják. Ez magában foglalhatja a következőket:

Fizikai biztonság: Az OT rendszerek és eszközök fizikai hozzáférésének korlátozása és védelme.

Hálózatbiztonság: A hálózatok védelme, beleértve az adatforgalom titkosítását, tűzfalak alkalmazását és más hálózati biztonsági intézkedéseket.

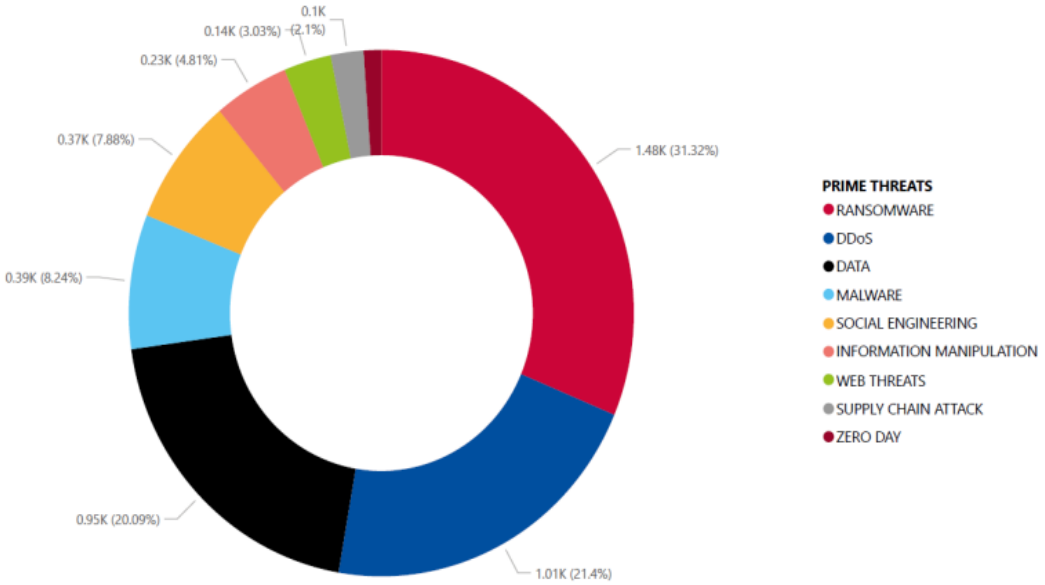
Rendszerbiztonság: A számítógépes rendszerek védelme, beleértve a frissítések rendszeres telepítését, a jogosultságkezelést és a sebezhetőségek elleni védelmi intézkedéseket.

Adatbiztonság: Az adatok védelme, különös tekintettel az érzékeny információkra, például az üzemeltetési adatokra és vezérlőrendszer-információkra.

Incidenskezelés: Az esetleges biztonsági incidensek és támadások kezelése, beleértve az azonnali választ és a rendszer helyreállítását.

A kritikus infrastruktúrák terén az OT security kiemelten fontos, mivel az ilyen típusú rendszerek sérülése vagy megbénulása jelentős károkat okozhat az egész társadalomban. Az energiaellátás, vízellátás, közlekedés és más kritikus szolgáltatások fenntartása érdekében elengedhetetlen a megfelelő OT security intézkedések alkalmazása.

Az OT rendszerek sérülékenysége igen magasnak mondható, hiszen egy gyártósort csupán 10-20 évente cserélnek le és a működtető szoftverek, operációs rendszerek is rengeteg sérülékenységet hordoznak magukban életkoruknál fogva.[4] Így a fent kifejtett okok miatt a kritikus infrastruktúrák és az OT rendszerek kiemelkedő célpontnak számítanak a kibertámadások terén.



2. ábra: 2022 június és 2023 július között véghez vitt kibertámadások csoportosítása a kritikus infrastruktúrák ellen [4]

ELLÁTÁSI LÁNC ELLEN IRÁNYULÓ TÁMADÁSOK

Az ellátási lánc közvetlenül nem jelenik meg a kritikus infrastruktúrák felsorolásánál, ha szigorúan értelmezzük a 2012. évi CLXVI. törvényt. Azonban mindenhol megjelenhet, mint kritikus infrastruktúrát kiszolgáló rendszerelem, hiszen a rendelkezésre állás kiemelkedően fontos ezeknél a szervezeteknél, mivel számos gazdasági, társadalmi és egyéb terület működését meghatározó elemeket foglal magában.

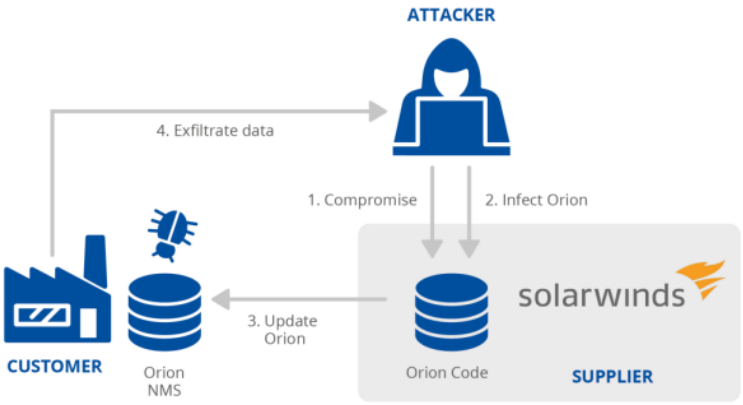
Az ellátási lánc elleni támadás a szervezetek és beszállítóik közötti kapcsolatot veszi célba. Egy támadás akkor tekinthető ellátási lánc komponenssel rendelkezőnek, ha legalább két támadás kombinációjából áll. Ahhoz, hogy egy támadás ellátási láncot érintő támadásnak minősüljön, a szállítónak és a vevőnek egyaránt célpontnak kell lennie. A SolarWinds volt az egyik első ilyen jellegű támadás, amely megmutatta az ellátási láncot érintő támadások potenciális hatását.

SolarWinds

SolarWinds Orion Platform ellen irányult támadás, egy sikeres kiberbiztonsági incidens volr 2020 decemberében. Ezt a támadást "SolarWinds-hack" vagy "Sunburst" néven ismerik.

A támadók a SolarWinds Orion Platformba bejutva manipulálták az egyik szoftverfrissítést, amelyet a SolarWinds ügyfelek automatikus frissítési rendszere használt.

Az ártalmas szoftver egy backdoor-t nyitott meg a rendszereken, amelyen keresztül a támadók további tevékenységeket folytathattak a célpontok munkaállomásán (3. ábra).



3. ábra: A SolarWinds támadási mechanizmusa

A támadók és információkat gyűjtöttek, illetve hozzáférést szereztek a célcsoportok hálózati rendszereihez.

A SolarWinds-hack jelentőségét az adja, hogy a támadók képesek voltak olyan rendszerekbe és hálózatokba bejutni, amelyek kulcsszerepet játszanak az államigazgatásban és a vállalati szektorban. A kibertámadás súlyossága és összetettsége miatt jelentős figyelmet kapott a kiberbiztonsági szakértők, a kormányok és a vállalatok részéről. A támadás forrása hivatalosan Oroszországot hozta összefüggésbe a csoporttal, amelyet kiberbiztonsági közösségek APT29 vagy Cozy Bear néven ismernek. [6]

Az eset megmutatta, hogy mennyire fontos az informatikai rendszerek és szoftverek biztonsága, és kihangsúlyozta a kritikus infrastruktúrák és az üzleti szektor védelmének jelentőségét a kibertámadások ellen.

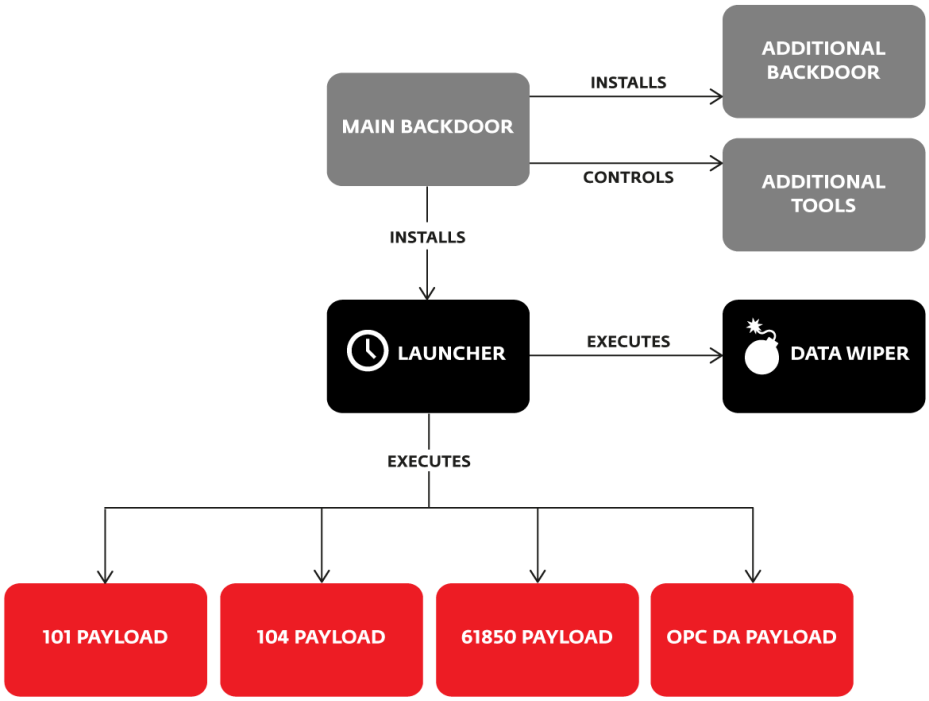
Industroyer

A vírus képes közvetlenül irányítani az elektromos alállomások kapcsolóit és megszakítóit. Ezek a kapcsolók és megszakítók az analóg kapcsolók digitális megfelelői. Így a potenciális hatás az áramelosztás egyszerű kikapcsolásától kezdve a tényleges meghibásodásokon át a berendezések súlyosabb károsodásáig terjedhet.

Helyi proxyval hitelesíti magát a belső hálózaton keresztül a backdoor telepítése előtt. A hitelesítés után HTTP-csatornát nyit a külső a C2 szerver felé.

A későbbi kommunikáció ezt követően a belső proxyn zajlik. Létrehoz egy fertőzött fájlt a helyi rendszeren (melyen keresztül életben tartja a kapcsolatot), amely egy futó szerviz szolgáltatáshoz kapcsolódik. A megfertőzött szolgáltatás folyamatosan nyitva tartja a backdoor-t, úgy, hogy előre meghatározott időközönként újranyitja a kapcsolatot a támadó szerver felé, így a rosszindulatú program továbbra is fut az újraindítások után is. [6]

Az Industroyer rendkívül testreszabható malware. Bár univerzális, mivel bármely ipari vezérlőrendszer megtámadására használható, amely a célzott kommunikációs protokollok némelyikét használja, az elemzett minták egyes összetevőit úgy tervezték, hogy bizonyos hardvereket célozzanak meg.



4. ábra: Az Industroyer támadási mechanizmusa [6]

Industroyer 2

A beavatkozást 2022.04.08-ra tervezték, de a jelek arra utalnak, hogy a támadást legalább két héttel előtte előkészítették.

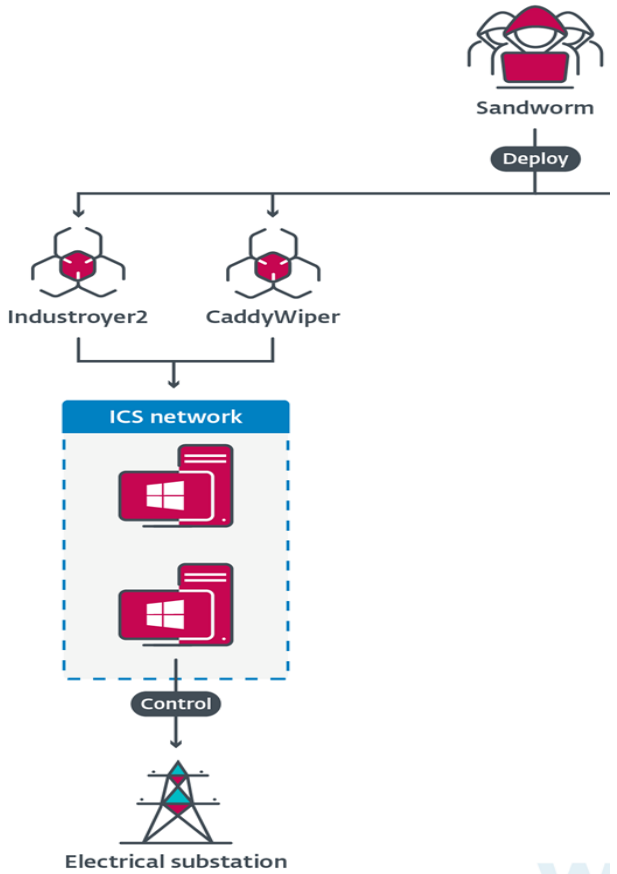
A támadásban ICS-képes rosszindulatú szoftvereket és Windows, Linux és Solaris operációs rendszerekhez alkalmazható lemeztörlőket használtak. Nagy valószínűséggel a támadók az Industroyer rosszindulatú szoftver új verzióját használták, amelyet 2016-ban az ukrajnai áramkimaradáshoz használtak.

Az Industroyer2 mellett a Sandworm több pusztító kártevő családot is használt, köztük a CaddyWiper-t. A CaddyWiper-t először 2022.03.14-én fedezték fel, amikor egy ukrán bank ellen használták. A CaddyWiper egy változatát 2022.04.08 14:58-án ismét felhasználták a korábban említett ukrán energiaszolgáltató ellen.

Az Industroyer2-t egyetlen Windows futtatható fájlként telepítették, amelynek neve 108_100.exe, és egy ütemezett feladat segítségével 2022.04.08-án 16:10:00 UTC-kor futtatta le. A PE időbélyege szerint 2022.03.23-án állították össze, ami arra utal, hogy a támadók több mint két hétig tervezték a támadást.

Az Industroyer2 nagymértékben konfigurálható. Részletes konfigurációt tartalmaz a testében, amely a rosszindulatú programok műveleteit vezérli. Ez eltér az Industroyer-től, amely a konfigurációt egy különálló .INI fájlban tárolja. A rosszindulatú szoftver megszüntet egy legitim folyamatot, amelyet a szokásos napi műveletek során használnak. Ráadásul átnevezi ezt az alkalmazást úgy, hogy a fájlnévhez .MZ-t ad hozzá. Ezt azért teszi, hogy megakadályozza a valódi folyamat automatikus újraindulását. Ez a komponens képes bizonyos ICS-rendszereket vezérelni az áramellátás leállítása érdekében. [8]

A CaddyWiper egy loader segítségével a Hex-Rays IDA Pro szoftver egyik legális komponensének, konkrétan a távoli IDA debugger szerver win32_remote.exe fájljának javított változatának álcázták. A patch-elt bináris kód egy fájlból tölti be a titkosított shellcode-ot, amely a CaddyWiper kissé módosított változata. Ez törli a meghajtó partícióinak kiterjesztett információit: a Master boot record (MBR) vagy a GUID Partition Table (GPT). Ezáltal a gép indíthatatlanná válik. A megtámadott energiavállalat hálózatán további, Linux és Solaris rendszert futtató, pusztító hatású kártevőket is találtak. A támadásnak két fő összetevője van: egy féreg és egy wiper.



5. ábra: Az Industroyer 2 és a CaddyWiper közös használata [8]

HATÁSVIZSGÁLAT

Az ENISA fenyegetettségi térképében szerepelnek a kritikus infrastruktúrák ellen intézett kibertámadások hatása. Mivel a kibertámadások hatásával kapcsolatos információk gyakran nem állnak rendelkezésre vagy nem hozzák nyilvánosságra, az eseményt követő hatás meghatározása és értékelése olyan szintű feltételezéssel jár, amelyben bizonyos fokú szubjektivitás nem kerülhető el. Ez önmagában is érvként szolgál az EU-ban az incidensek jelentési folyamatának javítása mellett, amely szempont a NIS2-irányelvben is megjelenik, és az ENISA az elkövetkező években is folytatja erőfeszítéseit.

Az ETL-jelentés keretében az alábbi hatástípusok figyelhetők meg:

- A digitális hatás a sérült vagy nem elérhető rendszerekre, sérült adatfájlokra vagy adatok kiszivárgására, vagy valamilyen bejelentett rosszindulatú behatolásra vonatkozik.
- A gazdasági hatás a közvetlen pénzügyi veszteségre, a nemzetbiztonságot érő károkra utal, amelyek fontos anyagok elvesztését vagy váltságdíj követelését eredményezheti.
- A társadalmi hatás a közvéleményre gyakorolt bármilyen hatásra vagy olyan széles körű zavarra utal, amelynek a társadalomra lehet következménye (pl. egy ország nemzeti egészségügyi rendszerét megzavaró események, bármely adat kiszivárgása a lakosság személyi azonosítóira, társadalombiztosítási azonosítókra vonatkozó adatok kiszivárgása stb.).
- A hírnévre gyakorolt hatás a negatív nyilvánosság vagy a közvélemény negatív megítélésének lehetőségére utal.
- A fizikai hatás az alkalmazottak, ügyfelek vagy betegek sérülésére vagy károsodására utal.
- A pszichológiai hatás okozhat megtévesztést, kellemetlenséget, frusztrációt, aggodalmat vagy szorongást. [3]

MOTIVÁCIÓ

Az ellenség és a kiberbiztonsági incidens vagy célzott támadás mögött álló motiváció megértése azért fontos, mert így meghatározható, hogy az ellenfél mire törekszik. Az indítékok ismerete segíthet a szervezeteknek meghatározni és prioritásként kezelni, hogy mit és hogyan kell védeni. Emellett képet ad a támadók szándékairól, és segít a szervezeteknek abban, hogy védelmi erőfeszítéseiket az adott eszközzel kapcsolatos legvalószínűbb támadási forgatókönyvre összpontosítsák.

A motiváció öt különböző fajtáját határozták meg:

- Pénzügyi haszon: bármilyen pénzügyekkel kapcsolatos csalás (amelyet többnyire kiberbűnözői csoportok hajtanak végre).
- Kémkedés: információk megszerzése érzékeny adatokról, minősített adatokról (többnyire államilag támogatott csoportok hajtják végre).
- Megzavarás: bármilyen geopolitikai céllal végrehajtott bomlasztó akció (többnyire államilag támogatott csoportok hajtják végre).
- Rombolás: minden olyan romboló akció, amelynek visszafordíthatatlan következményei lehetnek.
- Ideológiai: minden olyan akció, amely mögött ideológia áll (például hacktivizmus).[3]

TÁMADÁSOK ELEMZÉSE

Fontos felismerés, hogy egyes kibertámadó csoportok némi állami segítséggel törvényes eszközöket vetnek be, hogy meghosszabbítsák a kiberkémkedési műveleteiket. Céljuk, hogy minél tovább elkerüljék a felderítést, és elfedjék tevékenységüket azáltal, hogy a

legtöbb rendszerből széles körben elérhető szoftvereket használnak, ami megnehezíti a védők számára az azonosításukat. A geopolitika továbbra is nagy hatással van a kiberműveletekre. Számos fenyegető szereplő tovább fejlesztette az úgynevezett As-a-Service programjait. Nemcsak a új taktikákat és módszereket használnak a célpontokhoz való behatoláshoz, hanem a nyomásgyakorlás alternatív megközelítéseit is egyre jobban finomítják, amellyel zsarolják az áldozatokat, mindezt tiltott vállalkozásaik előmozdítása mellett.

Az egyik legnagyobb malware fenyegetés még mindig az információlopók, mint például az Agent Tesla, a Redline Stealer és a FormoBook. Folyamatosan csökken a klaszszikus mobil kártevők száma, viszont az adware-ek továbbra is megmaradtak ebben az évben is, mint a mobil eszközökre leselkedő legelterjedtebb fenyegetés. Sajnos a kémprogramok előretörése folytatódni fog a következő években is egyre jobban felhasználva a mesterséges intelligenciát.

Az adathalászat ismét a reneszánszát éli a legújabb elemzések szerint, ahol a social engineering új modellje adja az alapot. Ennek a modellnek a lényege áldozatokat nem csak a fizikai világban hanem a virtuális térben is megtéveszthetik. Az üzleti e-mailek kompromittálása (BEC, VEC) továbbra is a támadók egyik kedvenc eszköze a megszerzésre, amely valószínűsíthető a közeljövőben is hasonlóképpen lesz.

A Microsoft makróktól az ISO , Onenote és LNK fájlok felé való elmozdulás folytatódik, az ISO , Onenote és LNK fájlok használata felé. Az adatok kompromittáltsága 2023-ban nőtt. 2021-ig növekedett az adatveszélyeztetések száma, és bár ez a tendencia 2022-ben viszonylag stabil maradt, 2023-ban ismét növekedni kezdett.Megugrott a kiberbiztonsági fenyegetettségre hatást gyakorló AI Chatbotok száma. A bomlasztó hatás és a generatív mesterséges intelligencia chatbotok, például az OpenAI ChatGPT exponenciális elterjedése,

A DDoS-támadások egyre nagyobbak és összetettebbek, a mobilhálózatok és az IoT felé mozdulnak el, és kontextusban használják, hogy egy konfliktus keretében további eszközök támogatására használják őket. Az internet leállása minden idők legmagasabb szintjén van. Az internet elérhetőségét fenyegető fenyegetések lendületben maradnak, különösen a covid utáni korszakban, mivel az emberi tevékenységek és a társadalom egyre inkább az internetre támaszkodik. Az "olcsó hamisítványok" és a mesterséges intelligenciával támogatott információmanipuláció továbbra is aggodalomra ad okot. Az elmúlt hónapokban a mesterséges intelligencia információmanipulációra való felhasználásáról szóló vita felerősödött mind az Unión belül, mind azon kívül. A fenyegető csoportok egyre nagyobb érdeklődést mutatnak az ellátási láncot érő támadások iránt, és egyre nagyobb képességet mutatnak az alábbiakra azáltal, hogy az alkalmazottakat használják fel belépési pontként.

Nagy kihatással járó események ebben az évben is csak kis mértékben emelkedtek. A minősített bizalmi szolgáltatások bejelentése is növekedett az elmúlt évek statisztikájához képest az összes incidens 75%-ra volt hatással. A nem minősített bizalmi szolgáltatások viszont közel sem ennyire egyértelműek számadatok tekintetében, mivel az adatot szolgáltatóknál általában, olyan automatizmusok vannak beépítve a rendszerben amelyek torzítják a kevésbé fontos adatok megérkezését a központi elemző rendszerek felé. A jelentett incidensekkel kapcsolatos pontos és teljes információ biztosítása elengedhetetlen a megfelelő elemzéshez és nyomon követési intézkedésekhez. Sajnos az ENISA jelentése szerint legalább 10% a bejelentett incidenseknek nem tartalmaz további feldolgozható információs

adattartalmat, amelyet adatelemzés céljára fel lehetne használni. A rosszindulatú tevékenységek kezelésére vonatkozó korai figyelmeztetések nagymértékben segíthetnek a különböző piaci szegmenseknek, amellyel csökkenteni lehet az incidensek hatását. Itt lehetne megemlíteni a kritikus infrastruktúrák közötti, egymástól való kölcsönös tanulást is, amelynek során jelentősen lehetne mérsékelni a potenciális kibertámadási veszélyeket. [3] a webhelytanúsítványok (TLS), amelyek az online/internetes biztonság alapvető elemei. Világszerte a webhelyek körülbelül 80%-a használ webtanúsítványt.

VÉDELMI INTÉZKEDÉSEK

Egy általános szervezet infokommunikációs felépítése általában minimum két, jól elkülöníthető szektorra bontható. Ezen szektorokhoz javaslok néhány egyszerű védelmi megoldást az alábbiakban.

1. szektor: Azok a szerverek, amik az internetről láthatóak.

Az egyes szerverek egy alhálózatban vannak és kommunikálnak egymással. A bejutás többnyire egy létező rendszersérülékenység segítségével történik.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- hálózati szegmentálás (nincs új a nap alatt);
- hardveres illetve szoftveres biztonsági megoldások (IDS, IPS, Firewall);
- ellenőrzött operációs rendszer frissítések alkalmazása;
- képzett személyzet (ahol nem üzemeltetés a cél!!!).

2. szektor: Felhasználói szféra vagy üzemi terület

Általában külön alhálózatot képeznek a szerver szekcióval. A bejutás többnyire phising kampánnyal kezdődik. Ebben az esetben a támadónak mindenképpen el kell érnie, hogy a felhasználó hibázzon.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- „erős jelszó” használata;
- kiberbiztonsági tudatosító oktatások megtartása (védekezni kell a social engineering ellen).

A felhasználókkal szemben elkövetett csalások jelentős kockázatot jelentenek az egyének személyes adataira és pénzügyi biztonságára, és az ilyen incidensek megelőzése és kezelése kulcsfontosságú a kiberbiztonsági stratégiákban.

ÖSSZEFOGLALÁS

A kibervédelem kritikus infrastruktúrák esetében kiemelkedően fontos, mivel ezek az intézmények és rendszerek olyan alapvető szolgáltatásokat nyújtanak, amelyek elengedhetetlenek a társadalom és a gazdaság működéséhez. Ilyen infrastruktúrákhoz tartoznak például az energiaszolgáltatások, víz- és csatornahálózatok, közlekedési rendszerek, egészségügyi intézmények, pénzügyi szervezetek, és más olyan létesítmények, amelyek kulcsfontosságúak a mindennapi életünkben.

A kibertámadások súlyos következményekkel járhatnak, nem csak az adott intézményre vagy szolgáltatásra, hanem az egész társadalomra nézve. A támadók célja lehet a szolgáltatások megbénítása, az adatok manipulálása, vagy akár a fizikai rendszerek károsítása is. Ezért a kibervédelem célja a biztonsági rések folyamatos monitorozása, az azokból adódó veszélyek azonosítása és azok elleni hatékony védekezés.

Az Industroyer típusú támadások tanulságos példák lehetnek a kritikus infrastruktúrák védelmének szempontjából. Az Industroyer egy kifinomult kártevő, amely képes irányítani és manipulálni az ipari vezérlőrendszereket, például az elektromos hálózatokat. Ezek a támadások rávilágítottak arra, hogy az ipari rendszerek sebezhetőségei jelentős veszélyt jelenthetnek, és hogy a támadók milyen mértékben tudnak kihasználni az ellátási láncokban rejlő gyenge pontokat. Az ilyen típusú támadásokból levonható tanulságok segíthetnek az ipari szektor és más kritikus infrastruktúrák védelmi stratégiáinak fejlesztésében, a biztonsági intézkedések javításában és az esetleges támadások elleni hatékony védekezés kidolgozásában.

A legfontosabb javaslat, hogy az üzemi területen is fel kellene váltania a „safety” nézőpontot, az informatikában alkalmazott „security” gondolkodásmódra. Ez azt jelenti, hogy be kell látni, hogy nem csupán a bitonságos rendelkezésreállásra van szükség az ipari területeken, hanem a tényleges információbiztonsága.

FELHASZNÁLT IRODALOM

[1] Sági G., „Informatikai rendszerek támadási folyamata.” *Műszaki Katonai Közlöny,* 27 évfolyam, 3. szám, pp. 212-223., 2017.

[2] Almási L., Balog P., Berkecz G., Busa A., Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K., *Honvédelmi alapismeretek tankönyv*. Zrínyi Kiadó, Budapest, 2023.

[3] ENISA Threat Landscape 2023 [online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (letöltve: 2023.11.20.)

[4] Kiberbűnözők célpontja lett az energiaszektor [online]. Elérhető: https://greendex.hu/kiberbunozok-celpontja-lett-az-energiaszektor/ (letöltve: 2023.11.18.)

[5] ENISA Threat Landscape for Supply Chain Attacks [online]. Elérhető: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (letöltve: 2023.11.18.)

[6] CyberArk Blog Team: The Anatomy of the SolarWinds Attack Chain [online]. Elérhető: https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain (letöltve: 2023.11.20.)

[7] Industroyer: Biggest threat to industrial control systems since Stuxnet [online]. Elérhető: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (letöltve: 2023.11.18.)

[8] MalPedia for win.industroyer [online]. Elérhető: https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer (letöltve: 2023.10.18.)

[9] How Kaspersky Industrial CyberSecurity deals with an APT based on Industroyer malware [online]. Elérhető: https://www.kaspersky.com/enterprise-security/mitre/industroyer (letöltve: 2023.11.07.)

SECURE DATA UTILIZATION FROM PHOTOVOLTAIC SYSTEMS FOR OPTIMIZATION PURPOSES

BIZTONSÁGOS ADATKEZELÉS NAPELEMES RENDSZEREK OPTIMALIZÁLÁSÁHOZ

ČOVIĆ Zlatko[1] – RAJNAI Zoltán[2] – FÜRSTNER Igor[3]

Abstract

As the global push for more sustainable energy sources gains momentum, solar energy adoption is becoming increasingly significant. This research deals with the complex challenges that a special category of producers of electric energy from solar power, an individual producer - consumer encounters. More specifically, the research focuses on electric energy production-distribution-consumption data extraction, independently from the available data recorded and stored by the installed photovoltaic systems, and the suppliers of electric energy. The independent data extraction enables safe long-term data storage, and a possibility to perform different calculations enabling the optimization of the elements of the photovoltaic systems regarding their structure and capacity. The initial part of the research offers an overview of independent data extraction technology. Subsequently, a case study involving a producer-consumer household compares collected data with the photovoltaic system's output.

Keywords

Photovoltaic Solar Energy System, Information Security, Individual Producer – Consumer, Data Extraction, REST API

Absztrakt

Napjainkban világszerte növekszik a fenntarthatóbb energiaforrások alkalmazása, ezért a napenergia hasznosítása egyre fontosabbá válik. A kutatás a napenergiából elektromos energiát termelő, ún. termelő-fogyasztó esetében jelentkező összetett kihívásait vizsgálja, konkrétan, az elektromos energia termelés-felhasználás adatainak kinyerésére összpontosít, függetlenül az adatoktól, amelyeket a napelemes rendszerek, valamint a szolgáltatók rögzítenek és tárolnak. A független adatkinyerés lehetővé teszi a biztonságos hosszútávú adattárolást, és lehetőséget nyújt különböző számítások végrehajtására, amelyek optimalizálják a napelemes rendszerek elemeit és kapacitását. A kutatás bevezető része áttekintést nyújt a független adatkinyerés technológiájáról. Ezt követően egy esettanulmány kerül bemutatásra, ahol egy termelő-fogyasztó háztartás esetében a függetlenül kinyert adatok összehasonlításra kerülnek a napelemes rendszer által bemutatott és használható adataival szemben.

Kulcsszavak

Napelemes Rendszer, Információ Biztonság, Egyéni Termelő – Fogyasztó, Adatkinyerés, REST API

[1] zlatko.covic@uni-obuda.hu | ORCID: 0000-0002-1769-1990| University professor, researcher, Óbuda University Doctoral School on Safety and Security Sciences | egyetemi oktató, kutató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

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

[3] furstner.igor@bgk.uni-obuda.hu | ORCID: 0000-0002-5688-7443 | Associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi docens, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

Solar energy has raised considerable attention as a renewable and sustainable form of electricity, not just within industrial facilities like electric energy production, but also among individual households. With advancements in solar technologies and growing environmental concerns, numerous studies have delt with the feasibility, advantages, and obstacles linked to adopting solar energy at the household level.

Researchers have pointed out that solar energy systems can yield long-term cost savings in comparison to traditional electricity sources, by lowering energy costs, and offering returns on investment over time [1, 2]. Additionally, solar energy adoption contributes to the reduction of greenhouse gas emissions and dependence on non-renewable energy sources, promoting sustainability [3, 4].

Also, recent advancements in solar energy system technologies have significantly improved the efficiency and effectiveness of residential solar systems. The development of high-performance solar panels, advanced tracking systems, and energy storage solutions, enhance the overall performance of individual household solar systems [5]. These advancements have increased the feasibility and attractiveness of solar energy adoption in individual households [6].

The economic feasibility of solar energy adoption in individual households has been extensively studied too. Research suggests that the cost-effectiveness of solar systems is influenced by factors such as government incentives, the availability of net metering programs, and the cost of alternative electricity sources [7, 8, 9, 10, 11]. Studies have also emphasized the importance of accurately assessing the financial benefits and payback periods associated with solar energy systems [12, 13]. Optimization of solar systems and the use of information and communication technologies (ICT) in the process is also an issue that has been delt with in literature [14, 15].

The environmental benefits of solar energy adoption in individual households are well-documented as well. Solar energy systems generate clean and renewable energy, reducing carbon emissions and mitigating climate change [16, 17]. Additionally, the use of solar energy in individual households can contribute to the overall sustainability of the electricity grid by reducing peak demand and promoting decentralized power generation [18].

Despite the numerous advantages of using solar energy in individual households, several challenges and barriers must also be addressed. Researchers have highlighted issues such as system intermittency, limited rooftop space, high upfront costs, and complex installation processes as potential obstacles to widespread adoption [19, 20, 21]. Additionally, policy and regulatory frameworks, grid integration challenges, and public perception can affect the rate of solar energy adoption [22].

This points towards the presented research, which aims at providing valuable insights into the technology of independent electric energy production-distribution-consumption data extraction in the case of individual producers – consumers. This would enable for the safe and secure data storage with no dependency on the installed photovoltaic systems (PVS), and the supplier of electric energy. Moreover, this would assure the possibility of performing different calculations enabling the optimization of the elements of the PVS regarding their structure and capacity.

We are witnessing that nowadays web information systems are most developed as integrated web systems composed of several different components. These systems typically

consist of: a multi-platform web application (front-end part serving as a presentation platform), web application and/or services (back-end part for performing all necessary operations crucial for the system's functioning, administrative section), a mobile application (with capabilities either different or similar to the web application on the front-end but designed for intuitive use on mobile devices), and REST or RESTful API services for data exchange between components of the integrated web system. There are systems that retrieve data from other services via API endpoints, process it, and store it in their own databases. By using this data, they create API endpoints that can be public or require some form of authentication. These newly created API endpoints can then be used in other systems, which will utilize the obtained data in applications tailored to new requirements.

To maintain consistent communication across various devices, components, and platforms, it's essential to format the data using a standardized data format, like JSON (JavaScript Object Notation) or XML (Extensible Markup Language). Researchers compared both standards and provides an in-depth analysis of their performance. The results of each test were analysed and discussed. Overall, JSON outperformed XML in terms of data size and web API response time for all operations, except deletion. In some cases, JSON was 30 to 40% faster than XML, particularly with a growing number of records [23].

JSON format can be quickly parsed and generated by programming languages. Most programming languages provide built-in support or libraries for working with JSON, but the performance of JSON parsers varies with their implementation. In [24] performance analysis of JSON parsers in the native environment of 5 different programming languages has been conducted in terms of parsing speed and resource consumption.

The server can authenticate each client through cookies or session on the HTTP protocol using REST API. Nonetheless, there is a vulnerability that makes it easy for a hacker to take the identification information, such as tapping the broadcast packets or employing a fake proxy or other tool for this purpose. In research [25], a new mechanism called disposable token is proposed, which is based on token authentication of RESTful API on the HTTP protocol. The client is requested to store the public and private token-pair computed by the server as part of this mechanism.

In the following paragraphs, the proposed ICT technologies for data extraction will be presented, followed by a case study showing the extracted data compared with the data from the installed PVS regarding the energy production, direct consumption, distributed energy towards the grid, as well as taken energy from the grid. Following this, a short discussion and conclusions will be presented.

Data extraction

The photovoltaic system has its own web panel where, through logging in with valid credentials, current data for the installed system can be viewed. The web panel is used for data visualization, and data can be filtered based on certain criteria. To use the data from the PVS for optimization calculations, it is necessary to extract them from the system by applying ICT (Information and Communication Technology) technologies. It can be done with various technologies.

In our case, the extraction of data was done using the PHP programming language, version 8, with the JSON Machine class. PHP (Hypertext Preprocessor) is a server-side scripting language designed for web development to create dynamic and interactive web

pages. PHP 8 introduced several features and improvements aimed at enhancing speed and execution performance. It includes a JIT compiler, which stands for Just-In-Time compilation. This feature can improve the performance of certain types of applications by dynamically translating PHP bytecode into machine code at runtime, potentially resulting in faster execution.

JSON Machine is a parser based on generators designed for handling JSON streams or documents that may be unpredictably long. It is efficient, user-friendly, and offers fast processing capabilities. The extracted data is stored in the MySQL relational database.

The creation of HTTP requests was done using the cURL (Client URL) library. In PHP, cURL is a library and command-line tool used for making HTTP requests, interacting with various protocols, and retrieving or sending data to remote servers. It provides a versatile set of functions that allow developers to work with URLs, handle cookies, set various options for HTTP requests, and perform actions like GET, POST, PUT, or DELETE. cURL is commonly used for tasks such as fetching API data, making HTTP requests, and interacting with web services.

Case study

The case study presented is based on a producer – consumer household that produces electric energy by using a PVS with a total string capacity of 12kWp (32 modules – Mono-crystalline – CHSM60M-HC (BF) 166), with a 10KW inverter (SUN2000-10KTL-M1) and with no storage.

For the case study, the following data was extracted:

- Produced electric power from PVS (PEPPVS) [kW],
- Totally consumed electric power (TCEP) [kW],
- Directly consumed electric power from PVS (DCEPPVS) [kW],
- Electric power transferred to the grid from PVS (EPTGPVS) [kW],
- Electric power transferred from the grid for consumption (EPTGC) [kW].

Based on the extracted data, the following data was calculated:

- Produced electric energy from PVS (PEEPVS) [kW/h],
- Totally consumed electric energy (TCEE) [kW/h],
- Directly consumed electric energy from PVS (DCEPPVS) [kW/h],
- Electric energy transferred to the grid from PVS (EETGPVS) [kWh],
- Electric energy transferred from the grid for consumption (EETGC) [kWh].

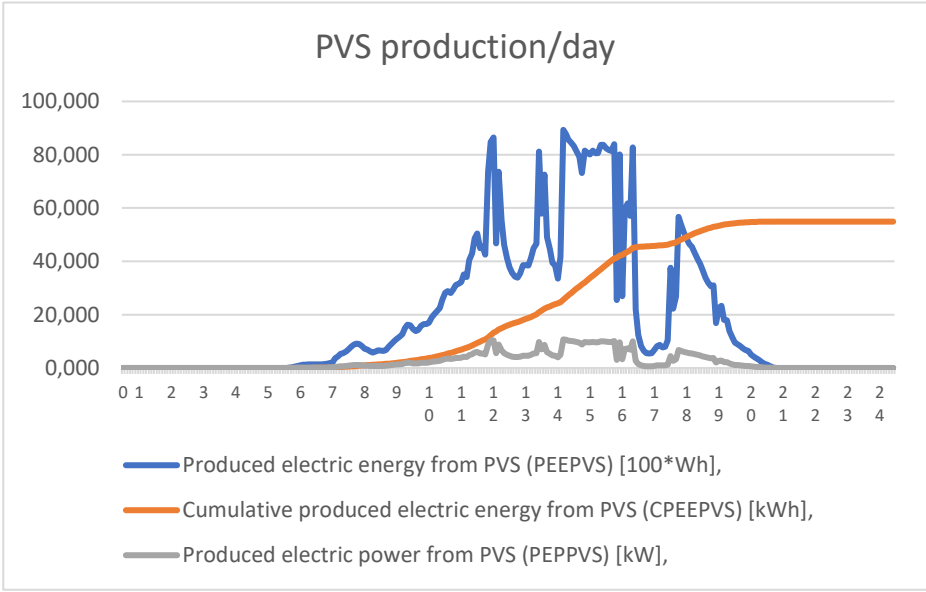
Also, the cumulative values of the energy amounts were calculated as well:

- Cumulative produced electric energy from PVS (CPEEPVS) [kW/h],
- Cumulative totally consumed electric energy (CTCEE) [kW/h],
- Cumulative directly consumed electric energy from PVS (CDCEPPVS) [kW/h],
- Cumulative electric energy transferred to the grid from PVS (CEETGPVS) [kWh],
- Cumulative electric energy transferred from the grid for consumption (CEETGC) [kWh].

The data was automatically extracted indirectly from the data provided by the installed PVS. The used time step was 5 minutes. For the study, the data was extracted for 12 months, however due to the extensive amount of information, only part of the data for one day, namely for May 27, 2023, is presented in the paper.

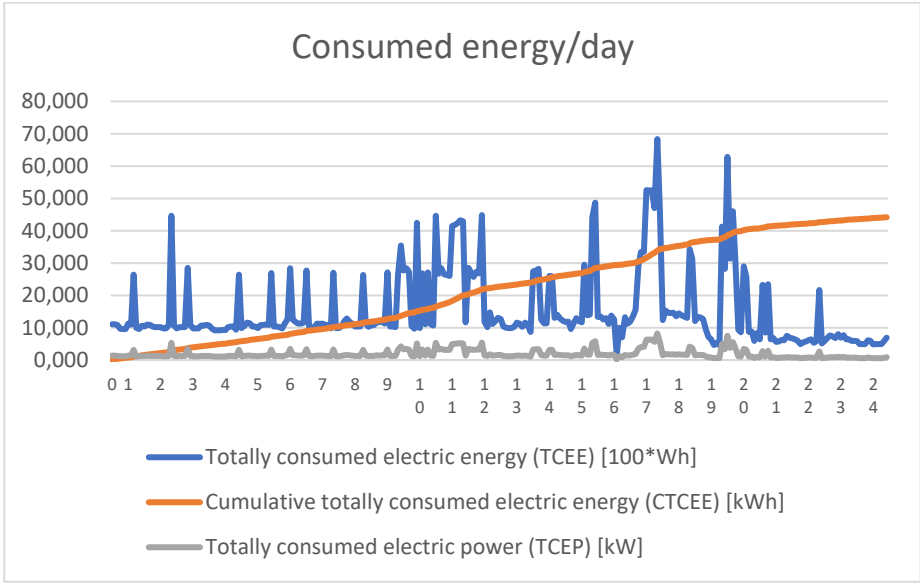
In the following figures, the extracted and calculated values are presented.

In Figure 1, the PEPPVS, PEEPVS and CPEEPVS are presented.



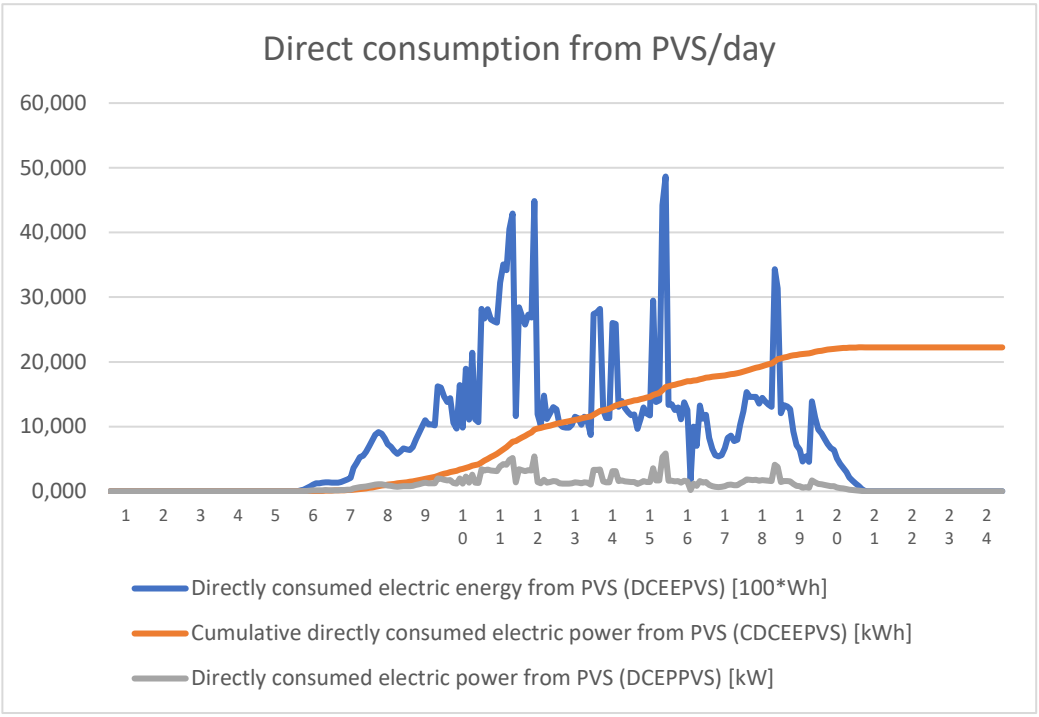
1. Figure: PVS production for one day (May 27, 2023)

In Figure 2, the TCEP, TCEE and CTCEE are presented.



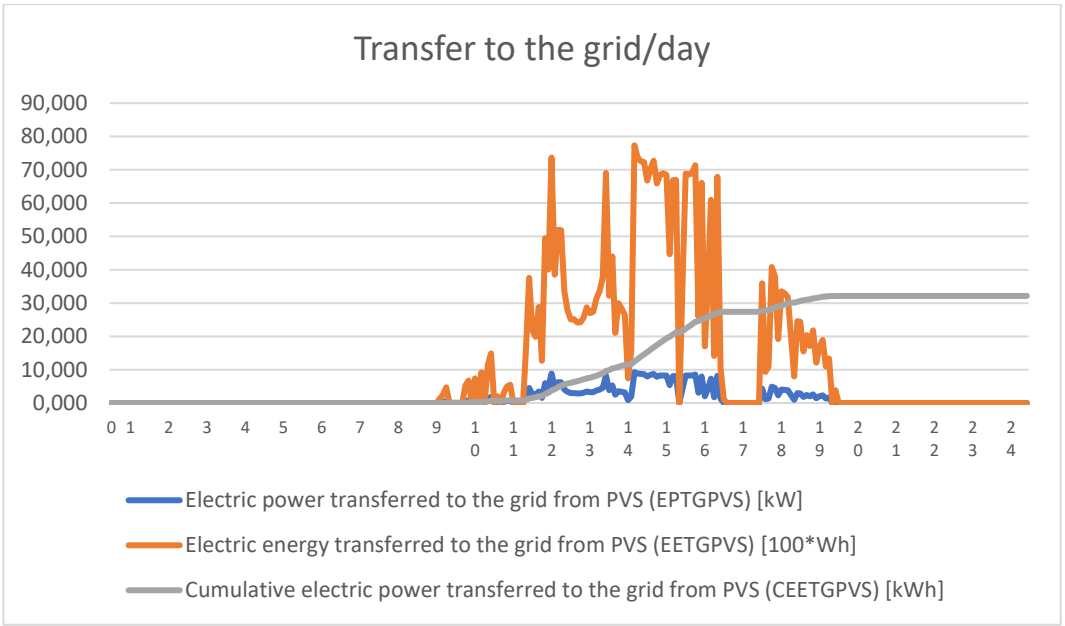
2. Figure: Total energy consumption for one day (May 27, 2023)

In Figure 3, DCEPPVS, DCEEPVS and CDCEEPVS are presented.



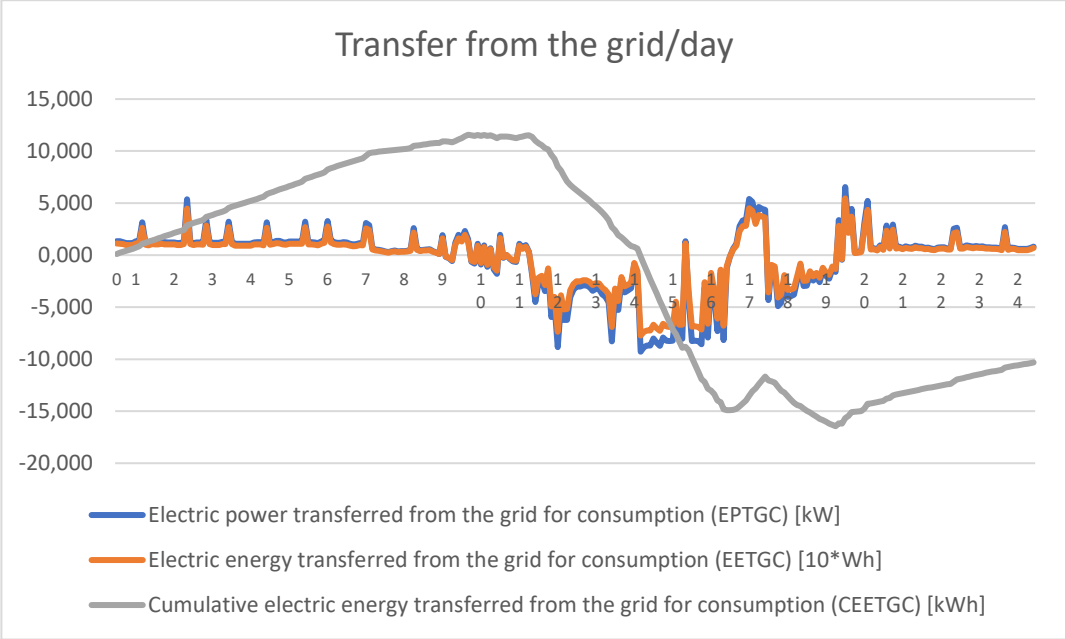
3. Figure: Direct consumption from PVS for one day (May 27, 2023)

In Figure 4, EPTGPVS, EETGPVS and CEETGPVS are presented.



4. Figure: Energy transfer from PVS to grid for one day (May 27, 2023)

In Figure 5, EPTGC, EETGC and CEETGC are presented.

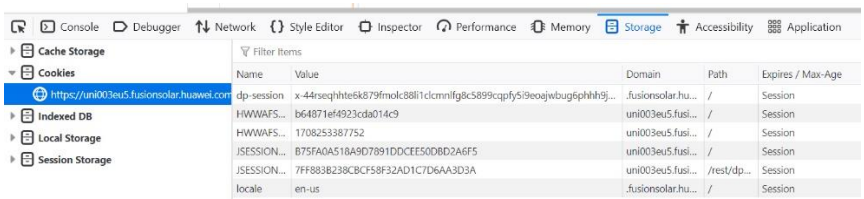


5. Figure: Energy transfer from grid to consumer for one day (May 27, 2023)

It can be noted that there are positive and negative values in Figure 5. Positive values refer to the situation when the total consumption is higher than the production from the PVS, while negative values refer to the situation when the total consumption is lower than the production from the PVS, and then the excess energy from the PVS is distributed to the grid.

Discussion

The data provided by the installed system to the user interface is formatted in JSON format and accessible through REST API endpoints. Access to this data is not public and requires a valid user to be logged into the system. To retrieve and store this data in another database, it was necessary to determine the authentication method. For the analysis of HTTP headers, Web Developer Tools were used, which exist in all modern web browsers. These tools offer multiple options, with Network and Storage being the most used. Through the Network option, information about HTTP requests and responses can be determined. Key information includes the URL of the request, parameters sent with the request, request body, HTTP headers, as well as the method and type of request. After receiving the response, an analysis was conducted on the parameters obtained in the response: HTTP headers and cookies. A detailed analysis of the response through the Storage option provided insight into cookies related to the site's operation and session cookies created after successful login to the system.

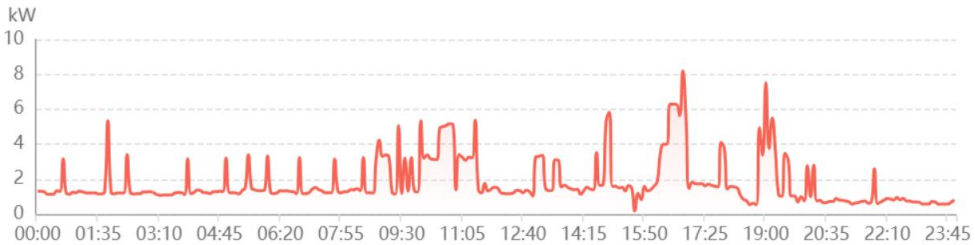


6. Figure: Web Developer Tools – Storage tab

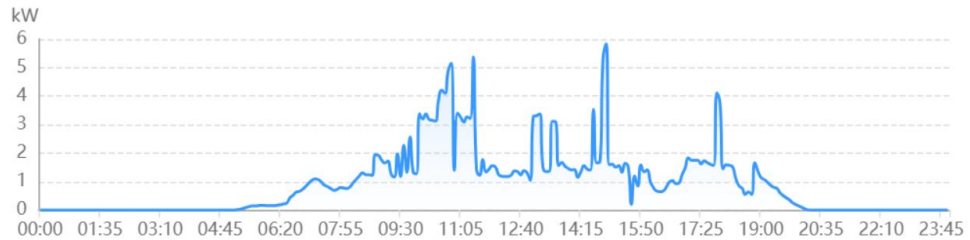
To verify the availability of API endpoints, requests were tested by sending data from HTTP headers and cookies. Postman and ReqBin tools were used for testing purposes. After successful tests and data retrieval, a program code was created to automatically send requests for a specific date. The program code utilized the cURL library. The desired data, obtained in JSON format, was parsed, and stored in a database. Retrieving data for the specified date was possible because the request included not only valid data from HTTP headers and cookies but also a parameter for the required date.

To be able to reflect on the data obtained and calculated, it is necessary to present the data available directly from the PVS. There is a possibility to present a certain type and amount of data, namely the PEPPVS (Fig. 7), TCEP (Fig. 8), and DCEPPVS (Fig. 9).

7. Figure: PVS production power for one day (May 27, 2023)



8. Figure: Total consumption power for one day (May 27, 2023)



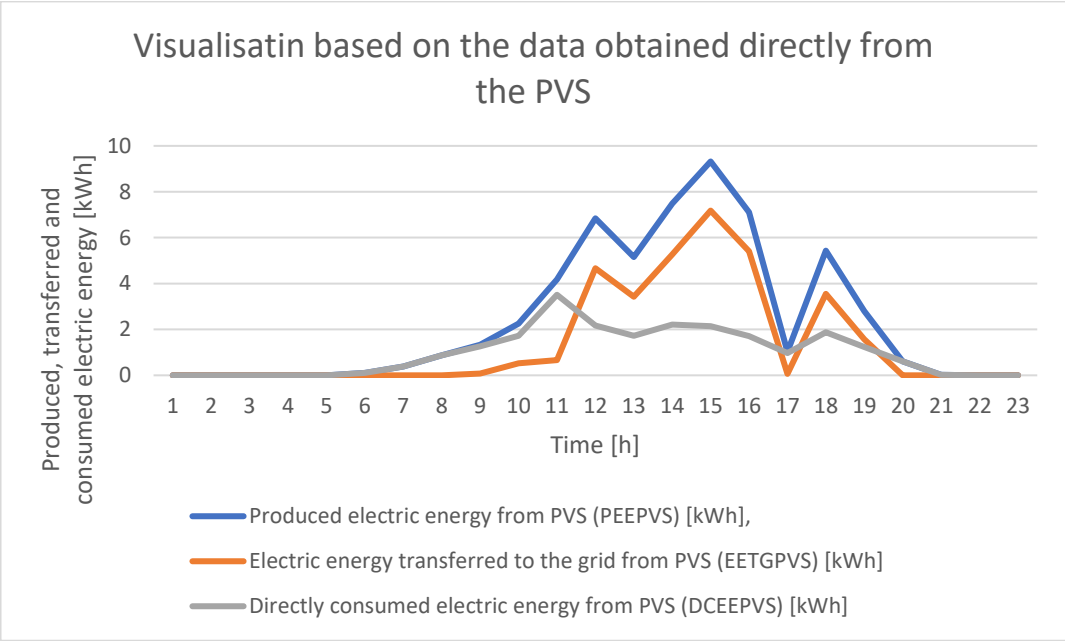
9. Figure: Direct consumption power from PVS for one day (May 27, 2023)

If the data presented in Fig. 1, Fig. 2, and Fig. 3 are compared to those presented in Fig. 7, Fig. 8, and Fig. 9, it can be concluded that the data patterns are similar. However, the data obtained directly from the PVS can only be used for visualization purposes. There is a possibility to obtain data from the PVS, but this possibility is rather limited. The data can be obtained only for whole hours, and for PEEPVS, EETGPVS, and DCEEPVS. This is presented in Table 1, while the visualization is presented in Fig. 10.

Time [h]	**Produces electric energy from PVS (PEEPVS) [kWh]**	**Electric energy transferred to the grid from PVS (EETGPVS) [kWh]**	**Directly consumed electric energy from OVS (DCEEPVS) [kWh]**
0	0	0	0
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0.1	0	0.1
6	0.39	0	0.39
7	0.88	0	0.88
8	1.34	0.08	1.26
9	2.25	0.52	1.73
10	4.18	0.67	3.51
11	6.84	4.67	2.17
12	5.15	3.42	1.73
13	7.48	5.27	2.21
14	9.32	7.18	2.14
15	7.11	5.4	1.71
16	1.03	0.06	0.97
17	5.43	3.55	1.88
18	2.8	1.57	1.23
19	0.61	0	0.61
20	0.02	0	0.02

21	0	0	0
22	0	0	0
23	0	0	0

1. Table: Data obtainable directly from the PVS



10. Figure: Data visualization based on the data obtained from the PVS

By comparing the data presented in Fig. 1, Fig. 3, and Fig.4 with the data presented in Fig. 10, one can conclude that there are significant differences in the presented data.

CONCLUSIONS

This research on the possibilities of independent data extraction for a PVS in individual households demonstrates the potential for significant benefits in terms of cost savings, environmental impact, and sustainability, based on calculations that could be made by using the extracted data. The presented case study provides valuable insights into the performance of the extracted data and the data from the installed PVS.

Thanks to the analysis of the HTTP communication between the web panel and the PVS, and the retrieval of necessary data for sending valid requests, independent data extraction for the entire year for the installed system has been carried out. ReqBin and Postman tools were used for testing purposes, and the actual extraction program code was implemented using the PHP 8 programming language, along with the JSON Machine and cURL libraries.

The results of the case study show that there are similarities in the visualization of the data obtained indirectly from the PVS, and those visualized by the PVS, but this is limited to visualization purposes only. The data obtained directly from the PVS is rather limited, both in quantity and type of data, and therefore cannot be used for meaningful calculations.

Based on the presented results, it can be concluded that there is a necessity to obtain the data indirectly if one wants to use the data for optimization purposes. This also points towards future research that will use the data for making decisions regarding further development of PVS-s in the case of producers – consumers.

One of the plans is to, after completing the information system for calculating data obtained through independent data extraction from the PVS system, create API endpoints that would be protected by disposable tokens. These API endpoints would be utilized by a mobile application designed to facilitate the viewing of obtained data and calculations in a simple and intuitive manner.

REFERENCES

[1] Santiago, I., Lopez-Rodriguez, M.A., Trillo-Montero, D., Torriti, J.and Moreno-Munoz, A., "Activities related with electricity consumption in the Spanish residential sector: Variations between days of the week, Autonomous Communities and size of towns," *Energy and Buildings*, vol. 79, pp. 84-97, 2014, doi: 0.1016/j.enbuild.2014.04.055.

[2] Qin, X., Xu, B., Lestas, I., Guo, Y. and Sun, H., "The role of electricity market design for energy storage in cost-efficient decarbonization," *Joule*, Vol. 7, no.6, pp: 1227-1240, Jun. 2023, doi: 10.1016/j.joule.2023.05.014.

[3] Chang, Y., Wei, Y., Zhang, J., Xu, X., Zhang, L. and Zhao, Y., "Mitigating the greenhouse gas emissions from urban roadway lighting in China via energy-efficient luminaire adoption and renewable energy utilization," *Resources, Conservation and Recycling*, vol. 164, 2021, Art. no.105197, doi: 10.1016/j.resconrec.2020.105197.

[4] Shahsavari, A. and Akbari, M., "Potential of solar energy in developing countries for reducing energy-related emissions," *Renewable and Sustainable Energy Reviews*, vol. 90, pp: 275-291, Jul. 2018, doi: 10.1016/j.rser.2018.03.065.

[5] Mârza, C., Moldovan, R., Corsiuc, G. and Chisăliță, G., "Improving the energy performance of a household using solar energy: A case study," *Energies*, vol. 16, no. 18, 2023, Art. no. 6423, doi: 10.3390/en16186423.

[6] Schulte, E., Scheller, F., Sloot, D. and Bruckner, T., "A meta-analysis of residential PV adoption: The important role of perceived benefits, intentions and antecedents in solar energy acceptance," *Energy Research & Social Science*, vol. 84, Feb. 2022, Art. no.102339, doi: 10.1016/j.erss.2021.102339.

[7] O'Shaughnessy, E., "Rooftop solar incentives remain effective for low- and moderate-income adoption," *Energy Policy*, vol.163, Apr. 2022, Art. no.112881, doi: 10.1016/j.enpol.2022.112881.

[8] Eslami, M. and Nahani, P., "How policies affect the cost-effectiveness of residential renewable energy in Iran: A techno-economic analysis for optimization," *Utilities Policy*, vol. 72, Oct. 2021, Art. no. 101254, doi: 10.1016/j.jup.2021.101254.

[9] Poponi, D., Basosi, R. and Kurdgelashvili, L., "Subsidisation cost analysis of renewable energy deployment: A case study on the Italian feed-in tariff programme for photovoltaics," *Energy Policy,* vol. 154, Jul. 2021, Art. no. 112297, doi: 10.1016/j.enpol.2021.112297.
[10] Xin-gang, Z., Yi, Z., Hui, W. and Zhen, W., "How can the cost and effectiveness of renewable portfolio standards be coordinated? Incentive mechanism design from the coevolution perspective," *Renewable and Sustainable Energy Reviews*, vol. 158, Apr. 2022, Art. no. 112096, doi: 10.1016/j.rser.2022.112096.
[11] Jia, X., Du, H., Zou, H. and He, G., "Assessing the effectiveness of China's net-metering subsidies for household distributed photovoltaic systems," *Journal of Cleaner Production,* vol. 262, Jul. 2020, Art. no. 121161, doi: 10.1016/j.jclepro.2020.121161.
[12] Delapedra-Silva, V., Ferreira, P., Cunha, J. and Kimura, H., "Methods for financial assessment of renewable energy projects: A review," *Processes*, vol. 10, no.2, Jan. 2022, Art. no.184, doi: 10.3390/pr10020184.
[13] Cui, Y., Zhu, J., Meng, F., Zoras, S., McKechnie, J. and Chu, J., "Energy assessment and economic sensitivity analysis of a grid-connected photovoltaic system," *Renewable Energy*, vol. 150, pp: 101-115, May 2020, doi: 10.1016/j.renene.2019.12.127.
[14] Al-Shahri, O.A., Ismail, F.B., Hannan, M.A., Hossain, M.S.L., Al-Shetwi, A.Q., Begum, M.A., Al-Muhsen, N.F.O. and Soujeri, E., "Solar photovoltaic energy optimization methods, challenges and issues: A comprehensive review," *Journal of Cleaner Production*, vol. 284, Feb. 2021, Art. no. 123456, doi: 10.1016/j.jclepro.2020.125465.
[15] Bastida, L., Cohen, J.J., Kollmann, A., Moya, A. and Reichl J., "Exploring the role of ICT on household behavioural energy efficiency to mitigate global warming," *Renewable and Sustainable Energy Reviews*, vol. 103, pp: 455-462, Apr. 2019, doi: 10.1016/j.rser.2019.01.004.
[16] Rabaia, M.K.H., Abdelkareem, M.A., Sayed, E.T., Elsaid, K., Chae, K.J., Wilberforce, T. and Olabi, A.G., "Environmental impacts of solar energy systems: A review," *Science of The Total Environment*, vol. 754, Feb. 2021, Art. no. 141989, doi: 10.1016/j.scitotenv.2020.141989.
[17] Chen, X.H., Tee, K., Elnahass, M. and Ahmed, R., "Assessing the environmental impacts of renewable energy sources: A case study on air pollution and carbon emissions in China," *Journal of Environmental Management*, vol. 345, 2023, Art. no.118525, doi: 10.1016/j.jenvman.2023.118525.
[18] Strielkowski, W., Civín, L., Tarkhanova, E., Tvaronavičienė, M. and Petrenko, Y., "Renewable energy in the sustainable development of electrical power sector: A review," *Energies*, vol. 14, no.24, Dec. 2021, Art. no. 8240, doi: 10.3390/en14248240.
[19] Bakht, M.P., Salam, Z., Gul, M., Anjum, W., Kamaruddin, M.A., Khan, N. and Bukar, A.L., "The potential role of hybrid renewable energy system for grid intermittency problem: A techno-economic optimisation and comparative analysis," *Sustainability*, vol. 14, no.21, Oct. 2022, Art. no.14045, doi: 10.3390/su142114045.
[20] Zander, K.K., "Unrealised opportunities for residential solar panels in Australia," *Energy Policy*, vol. 142, Jul. 2020, Art. no. 111508, doi: 10.1016/j.enpol.2020.111508.
[21] Adenle, A.A., "Assessment of solar energy technologies in Africa - opportunities and challenges in meeting the 2030 agenda and sustainable development goals," *Energy Policy,* vol. 137, Feb. 2020, Art. no. 111180, doi: 10.1016/j.enpol.2019.111180.

[22] Lazdins, R., Mutule, A. and Zalostiba, D., "PV energy communities—Challenges and barriers from a consumer perspective: A literature review," *Energies*, vol. 14, no. 16, 2021, Art.no. 4873, doi: 10.3390/en14164873.

[23] Breje, A.R., Gyorodi, R., Győrödi, C., Zmaranda, D. and Pecherle, G., "Comparative study of data sending methods for XML and JSON models," *International Journal of Advanced Computer Science and Applications,* vol. 9, no. 12, pp. 198-204, 2018. doi:10.14569/ijacsa.2018.091229.

[24] H. K. Dhalla, "A Performance Analysis of Native JSON Parsers in Java, Python, MS.NET Core, JavaScript, and PHP," in *Proc. 2020 16th International Conference on Network and Service Management (CNSM)*, Izmir, Turkey, 2020, pp. 1-5, doi: 10.23919/CNSM50824.2020.9269101.

[25] X.-W. Huang, C.-Y. Hsieh, and C. H. Cheng, "A token-based user authentication mechanism for data exchange in restful API," in *Proc. 18th International Conference on Network-Based Information Systems*, Taipei, Taiwan, 2015, pp. 601-606, doi:10.1109/nbis.2015.89.

DATA EXTRACTION DURING CBRN CRIME SCENE INVESTIGATION

ADATKINYERÉS CBRN KÖRNYEZETBEN

Dr. KAKUJA Izabella[1]

Abstract

Nowadays, it is not a curiosity that a crime scene is contaminated with various hazardous, noxious or CBRN materials. Consequently, the traces, lesions and personal effects left behind by the perpetrator at the scene will also be contaminated. To counter this, the collection of these traces, whether traditional or digital, is necessary. In the event that no CBRN contamination is found at the scene, it is possible to involve persons with specific expertise and to carry out laboratory tests on uncontaminated digital media. However, in the case of digital media contaminated with CBRN material, this is not an option. First the media must be cleaned, but then the problem arises that in the process the traditional traces and residues of the material can be damaged and destroyed. This meant that a method had to be developed whereby both traditional traces and digital data could be retained.

Keywords

CBRN contaminated crime scene, conventional and digital evidences, data extraction, chain of custody.

Absztrakt

Napjainkban nem kuriózum, hogy a bűnügyi helyszín, különböző veszélyes-, káros- vagy CBRN anyaggal szennyezett. Következésképp a helyszínen az elkövető által hátrahagyott nyomok, elváltozások, személyes tárgyak is szennyezettek lesznek/lehetnek. Mindezek ellenére ezen nyomok, legyenek azok hagyományos vagy digitális nyomok begyűjtésére szükség van. Abban az esetben, ha nem jelentkezik CBRN szennyezés a helyszínen, akkor lehetőség van speciális szakértelemmel rendelkező személyek bevonására, illetve a nem szennyezett digitális adathordozók laboratóriumi vizsgálatára. Abban az esetben azonban, mikor a digitális adathordozók CBRN anyaggal szennyezettek ez nem elérhető lehetőség. Először az adathordozókat meg kell tisztítani, azonban ekkor jelentkezik az a probléma, hogy eközben a hagyományos nyomok, anyagmaradványok sérülhetnek, megsemmisülhetnek. Vagyis szükség volt/van egy olyan módszer kialakítására, melynél a hagyományos nyomok és a digitális adatok is egyaránt megtarthatók.

Kulcsszavak

CBRN anyaggal szennyezett helyszín, hagyományos és digitális bizonyíték, adatkinyerés, felügyeleti lánc.

[1] kakujai@nni.police.hu | ORCID: 0000-0003-1324-033X | PhD student, University of Public Service, Military Engineering Doctoral School | PhD hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

INTRODUCTION

First, it is useful to clarify what the popularly known term "crime scene investigation" actually means in reality, far from the world of CSI (crime scene investigation) films. The concept of crime scene investigation itself can be interpreted in two ways: broadly and narrowly. In the narrow sense, it is exclusively a technical and tactical criminal investigation activity, carried out in practice, which serves and/or provides the investigation and evidence in criminal or administrative proceedings by searching for and recording traces and material remains on the spot.[1] While in a broader sense, and in addition to the above activities, it also includes the on-site activities of forensic experts (e.g. forensic, criminalistics), the criminalistics specialisation of canine forensics, and other criminal investigation activities (e.g. forensic traps), and by extension, education.[2]

Accordingly, it is advisable to carry out an on-site inspection where there is something to look for, i.e. where there are traces of evidence and material remains of a crime.[3] It is of particular importance all over the world as it supports both detection and evidence. To achieve its purpose, it requires forensic investigators who are always impartial, who do not look for patterns, but who systematically search the scene. They are aware that a negative trace is a trace.[4] That is, what is not there but should be there, or what is not there but was there. It often says more than the clue that is there.[5] So forensic investigation achieves its maximum objective when we have a highly qualified, impartial team of experts, a well-equipped technical equipment and a well-defined set of procedures defined by legislation and professional codes.

From all this, we can see that the collection of traces and material remains is the task of the crime scene investigation, whether traditional or digital traces. But it is important to give these words substance. Traces, lesions and material remains that are closely related to the so-called classical forensic areas of expertise (trace, weapon, fingerprint, handwriting) can be considered as traditional evidence, since they were created specifically for the purpose of forensic investigation.[6]

Social, scientific and technological changes in recent decades have brought with them the concept of the digital footprint. Social digitalisation as a process has had a significant impact on forensic activities, and it has become necessary to reform previously established procedures and ways of thinking. The use of IT experts for on-site inspections and the provision of equipment for investigating authorities to record and store digital traces have become justified.[7] Electronic evidence, like evidence obtained from digital devices or cyberspace, carries with it its variability and manipulability. For this reason, they are subject to special requirements in order to be admissible in court. I would like to note that the location of the data that can be used as evidence is of particular importance. This data may be stored on a phone, computer, printer or even in a car, smart device (fridge, fridge-freezer, vacuum cleaner, etc.) or the data may be stored only in the cloud.[8] [9] As you can see, digital traces and electronic data are extremely diverse and their storage locations do not always require a physical medium. In my presentation I will focus exclusively on data extraction from physical media.

In this spirit, therefore, "Evidence is only that which is credible and serves to establish the facts to be proved." [10]

The third set of concepts that we need to clarify is the acronym CBRN and their context in the crime scene. Nowadays, the acronyms ABV (Atomic, Biological, Chemical)

and CBRN (Chemical, Biological, Radiological and Nuclear) are used as synonyms for each other. Unlike the military term, CBRN refers to all hazards associated with chemical, biological, radiological and nuclear materials. It is understood that my presentation will only deal with CBRN materials that are out of control, i.e. where a criminal offence is involved. Because only there does the forensic investigation make sense. CBRN hazards pose serious health risks. It is therefore clear that they must be protected against. According to military rules, this is done in 3 steps. This is because ABV [16] protection is a complex system based on three pillars to protect personnel and technical equipment against any ABV attack. The elements of this three pillar system are avoidance, protection and relief.[11]

The concept described above is linked to policing by the nowadays intensified international terrorism and the intertwined CBRN terrorism as a possible instrument of asymmetric warfare. The arsenal and expertise of terrorist organisations is growing. Terrorist organisations and individual terrorists can threaten and achieve their goals by using radiological, toxic and infectious agents. These tools are therefore no longer just weapons of the regular army, but can also be used by extremist groups outside a war situation, even within a country.[12] In other words, the prevention, suppression, detection and proof of such acts, together with the criminal claim of the state, form the basis of police action. As we have already clarified in the concept of the on-site visit, in such cases it is necessary to gather as much evidence as possible, as this can determine the direction of the investigation and can also function as a decision support.

Once these basic concepts have been clarified, it will be clear to everyone that this is not a simple procedure, but a complex task requiring the involvement of a number of different disciplines.

INVESTIGATION, EVIDENCE COLLECTION

The presence of a CBRN element on the site makes the procedural act extremely difficult, since it is not enough to comply with legislation, professional rules and ISO standards, but all this has to be done under time pressure, in heavy protective clothing, with extra security rules and constant communication.

Preparation is also a complex process for this type of site. I will not go into this in my presentation - due to time constraints.

After the preparations, a primary reconnaissance is essential. This activity covers risk assessment, planning of the work and background measurement, followed by a surface contamination investigation (detection of possible spills, contamination), identification, marking and disposal of hot spots (e.g. elevated radiation levels indicating the presence of radiological material, or hot spots).

This is followed by the professional collection of the detected materials using forceps and manipulators. During collection, the safety rules and the ABV protocol must be followed to the maximum extent possible, and care must be taken to avoid contamination (cross-contamination). This is important for two reasons. Firstly, the contamination should not be taken off-site, i.e. no new contaminated area should be created. Secondly, do not contaminate yourself or the crime scene. This can be achieved by always having a "clean" technician on site and having him/her provide the crime bags for the crime scenes and/or by changing gloves between each sample collection. Avoiding cross-contamination is also important for the integration of crime signals. A continuous video and photographic record of

the crime scene shall be made beforehand and during the procedure, including the activities of the forensic technicians, as the procedure itself shall comply with the requirements of the MSZ EN ISO 21043 series of standards, Parts 1 and 2.[17]

All material leaving the scene, including collected crime scene evidence and any equipment used for searching or recording, as well as any instruments or equipment used to detect the material, must be re-measured in the clear zone. They must also be decontaminated (cleaned) there.

After CBRN materials have been collected, repeat measurements should be taken at the site to see if there is any contamination remaining at the site. If not, the site can be handed over to the forensic team and the level of personal protective equipment can be reduced. In the event that contamination remains at the site, the site should be processed under expert guidance. The primary step in this process is to prepare a "TRIAGE" of the crime scene to be collected. The priority here is always to collect first those that can be easily destroyed and that directly point to the perpetrator. Then digital evidence and traditional evidence whose degradation is not immediate. As regards digital evidence, I will only discuss those on physical storage. The treatment of collected digital evidence is identical to the treatment of traditional evidence, as it is subject to the same legislation.

In the case where the digital storage devices are not contaminated with CBRN material, then everything goes its own way, since it is a crime scene from a criminal inspection. Data recovery can begin in the clear zone. If it is not possible or necessary to use other technologies, the data or data storage devices can be removed from the site for further analysis. This means that evidence collection and data extraction and analysis can take place at the same time and in parallel at the site visit. However, in cases where the data storage device is contaminated with CBRN material, the possibilities are limited, as there is no possibility to analyse the data content in a conventional way. We can only start the investigation if we can protect the technical staff, the bystanders, the experts and the site from contamination. In such cases, the data recovery can be carried out by placing the data storage devices issued from the site in glove bags at the same time as the on-site inspection, so that the data recovery officer can work in safe conditions and start the necessary investigations at the same time.(e.g. data recovery can start at the same time as the DNA residue capture - in the case of a telephone device - using UFED technology[18]. However, this procedure implies that the person performing the data collection must also learn at least at a basic level and adhere to the ABV protocol, i.e. wear the specified personal protective equipment in the specified manner and for the required time while performing his or her task. This implies that the data recovery expert should be prepared, if only minimally, for such situations, should be familiar with the protocols, should learn to wear the required personal protective equipment and should be able to perform a high quality job in doing so. He/she must learn the discharge procedures and be able to apply them at a skill level.

The question arises, why is this important?

Well, because traditional crime-signal capture, digital data extraction and CBRN material characterisation are done simultaneously, while still on site, and the immediate secure transmission of the resulting data significantly increases law enforcement competence. There is no doubt that this capability is extremely important in the event of a terrorist incident. If we are able to send video footage of the scene in real time to the command post,

transmit the photographs via a data link as soon as the photograph is taken, then through coordinated action, partner agencies, other experts, law enforcement agencies, even in other countries, can receive a live picture (on an encrypted channel) in real time, thus assisting the team working in the investigation zone or passing the information to the appropriate agency.[13] Also unique to the Hungarian method is the ability of forensic staff to instantly deliver a scaled photograph of traditional crime scenes to forensic institutions, where data processing can begin during the crime scene, so there is no time delay, while the chain of custody of evidence continues.

Figure 1: Safe extraction of radioactively contaminated mobile phone data using a UFED tool, while also capturing DNA residue (Photo: D. Calma UN IAEA)

CONCLUSIONS

The risks posed by CBRN hazards are ever-present in today's world, and therefore the maintenance and development of CBRN detection capabilities remains justified.[14] Education and training of specialist personnel is also important. However, there is a lack of training in this area, as it is not included in the training of forensic technicians. To overcome this, it is proposed to prepare an educational theme specifically for those working in this field, and later to provide theoretical and practical training along this theme.

A crime scene investigation is essential, but CBRN materials complicate the process, as in addition to forensic staff, the presence of people with specific expertise is required who need to know the basics of site inspection. Currently this is also a gap, so the proposal is similar to those mentioned earlier. In other words, the CBRN expert should be familiarised with the basics of the site investigation and the techniques of investigation and

detection, in order to enable the two disciplines to work together as effectively as possible during the procedure.

In addition, if digital evidence is to be extracted, the expert needs to be exposed to both areas, and there is a gap in this area. Proposal follows on from the above. There is a need to ensure interoperability between the knowledge materials of the different disciplines and to ensure knowledge transfer.

In addition to all this, we must not forget to acquire the right equipment and to keep improving it. And the tools must be adapted to the specificities of the field inspection.

At the same time, the coordinated, high quality execution of these activities can result in a powerful unit capable of maximum data collection and analysis in a short time and, when transmitted, can result in a fast, effective law enforcement.

However, one possible direction is to train crime scene technicians to be able to perform such tasks at a basic level. In this case, however, it will still be necessary to involve an expert to analyse the data, i.e. although data analysis and inspection will be carried out in parallel, the on-site data analysis will still require the expert to be familiar with the ABV protocol.

SUMMARY IN NUTSHELL

To summarise the above ideas, in today's digital world, law enforcement agencies cannot afford to ignore electronic data on storage media and in cyberspace. The European Commission's Digital Single Market Strategy for 2015 also argues that the internet and digital technologies are transforming our world.[15] This is precisely why digital data and its carriers cannot be ignored during a site visit, as there is often more data in virtual space than in reality. If all this can be used as evidence in subsequent proceedings, law enforcement agencies can work more effectively.

Data collection may be necessary in all cases, even if the environment is contaminated with CBRN material. So you have to be prepared for this. Partly by education, partly by ensuring knowledge transfer. On the other hand, in the case of a real site, it is necessary to be able to concentrate the technical equipment, the specialised staff with the appropriate knowledge in one place, and to be able to coordinate both the activities and the use of the equipment in the case of several subtasks requiring specialised knowledge. This is the key to efficiency.The sooner and more efficiently coordination can be achieved, the faster and more effective law enforcement will be.

BIBLIOGRAPHY

[1] Csaba Fenyvesi: *The forensic characteristics of the on-site inspection*. PTE ÁJK Pécs, 2009 p. 1.

[2] Gergely Gárdonyi: *CSI Hungary - Facts and Perspectives in Hungarian Crime Scene Investigation* In: Gyula Gaál-Holtán Hautzinger (eds.) Studies from the scientific conference "QUO VADIS police protection? QU QU QU QUO QUO QUALITY QUESTIONS", Pécs, 2010, 104-110 p. [Pécs Border Guard Scientific Publications XI.]

[3] András Benkő - András Huszár - István Szilvásy. In Zoltán Hautzinger (ed.): *Studies on the scientific conference "Border Guard on the Path of Quality*". Hungarian Military

Science Society Border Guard Section Pécs Section, Pécs, 2005, pp. 255-256 [Pécs Border Guard Scientific Publications IV.]
[4] János Dobos: *Negative conditions on the ground*. Internal Affairs Review, 1964/1, pp. 54-59.
[5] Csaba Fenyvesi: *Criminal chess game in the mirror of criminological principles* Internal Affairs Review 2016/11. number, pp. 40-57.
[6] Gabriella Kármán, *The Criminalistics Expert Evidence - The Building Blocks of Credibility* Institute of Criminology, Budapest, 2019, 137 p.
[7] Zoltán Mráz: *The importance of digital evidence tools in the investigation of crimes against property* Internal Affairs Review, Budapest, 2018, 7-8, p.
[8] Zoltán Kovács: *The potential applicability of cloud-based IT systems in law enforcement agencies*- Military Engineer, Volume VI, Issue 4, December 2011, page 177, source: http://hadmernok.hu/2011_4_kovacsz.pdf, downloaded: 2023.09.01.
[9] Gyaraki Eszter Réka: *Problems of computer crime investigation*, PhD thesis, Pécs, 2018, 69. pp.
[10] Vilmos Garamvölgyi - László Viski (eds.): *Kriminalisztika*. Ministry of Interior, Department of Studies and Methodology, Budapest, 1961, p. 688.
[11] Juhász László: *Nuclear, Biological and Chemical (ABV) Reconnaissance, Leadership and Management and Organization*, https://docplayer.hu/24496254-Az-atom-biologiai-es-vegyi-abv-felderites.html downloaded: 10.09.2023.
[12] T. Berek - R. Pellérdi: *Responding to CBRN challenges in the EU* 2011. Bolyai Szemle, Vol. XX, No. 2, http://portal.zmne.hu/download/bjkmk/bsz/bszemle2011/2/Berek_Pellerdi.pdf
[13] Izabella Kakuja: *Unique Hungarian method in radiological crime scene managent*, Budapest, 2022, Military Technology, LVI. year - 2022/5, 58-62
[14] László Juhász: *Nuclear, biological and chemical (ABV) detection* https://docplayer.hu/24496254-Az-atom-biologiai-es-vegyi-abv-felderites.html downloaded: 10.09.2023.
[15] Béla Simon: *Digital challenges facing law enforcement Hungarian Policing* 2017/5. 83-103
[16] The abbreviation ABV is used in MH documents according to the 2009 Uniform Guidance of the MH Standing Working Group on Chemical Defence of the Armed Forces Section
[17] MSZ EN ISO 21043 Forensic science. Part 1: Terminology and definitions Part 2: Searching for, documenting, collecting, transporting and storing evidences (Author)
[18] A UFED (Universal Forensic Extraction Device) is a device for extracting and decrypting information from almost all phones on the market, even those with lock protection. It can be used to retrieve call logs, even for deleted SIM cards, phone numbers, images, videos, audio files, or even graphical geographic labels. (Author)

DEVELOPMENT OF A VIRTUAL TECHNIQUE AIDED, CONTROLLED TEST ENVIRONMENT ON PROVING GROUND FOR ASSESSMENT OF ADVANCED DRIVING FUNCTIONS

VIRTUÁLIS MÓDSZEREKKEL TÁMOGATOTT KONTROLÁLT TESZTKÖRNYEZET KIALAKÍTÁSA TESZTPÁLYÁN FEJLETT VEZETÉSI FUNKCIÓK VIZSGÁLATÁRA

TÓTH Bálint[1] – SZALAY Zsolt[2]

Abstract

Testing advanced driving functions in a highly realistic and repeatable way is one of the biggest challenges of today's automotive research, development and validation process. Although the role of the computer simulations is increasing in the development phase, it is still necessary to test the vehicles on real proving grounds with physically existing target objects. Therefore, finding the balance between the virtual and real test methods is a key task. In this paper, we present the Scenario-in-the-Loop (SciL) concept which uses similar closed-loop testing methodology compared to the widely used SiL, HiL, or ViL approaches. The core component is the control software which controls virtual and real disturbances and adapt the scenario based on the continuously changing input parameters of the tested vehicle and the proving ground infrastructure in real-time.

Keywords

Scenario-in-the-Loop, proving ground, simulation, vehicle testing

Absztrakt

Napjaink egyik legnagyobb járműipari kutatás-fejlesztési és validációs kihívása a fejlett vezetési funkciók megismételhető, és realisztikus módon történő tesztelése. Habár a fejlesztési fázisban a számítógépes szimulációk szerepe megnövekedett, de továbbra is szükséges a járművek próbapályán történő tesztelése valós tesztobjektumok használatával. A valós és virtuális tesztelési módszerek közötti egyensúly megtalálása kulcsfeladat. Ebben a munkában bemutatásra kerül a Scenairo-in-the-Loop (SciL) koncepció, amely a széleskörben használt SiL, HiL vagy ViL eljárásokhoz hasonló zárthurkú tesztelési módszer. A koncepció fő komponense az a vezérlőszoftver, amely a valós és virtuális zavarások vezérlését és a tesztszcenárió adaptálását végzi a tesztelt járműből és az infrastruktúrából származó bementi paraméterek alapján valós időben.

Kulcsszavak

tesztpálya, szimuláció, járműtesztelés, Scenraio-in-the-Loop

[1] tothb.0920@edu.bme.hu | ORCID: 0000-0003-1688-9089 | PhD student, Department of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics | PhD hallgató, Budapesti Műszaki és Gazdaságtudományi Egyetem, Közlekedésmérnöki és Járműmérnöki Kar, Gépjárműtechnológia Tanszék

[2] szalay.zsolt@kjk.bme.hu | ORCID: 0000-0002-6172-5772 | Head of Department, Department of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics | Tanszékvezető, Budapesti Műszaki és Gazdaságtudományi Egyetem, Közlekedésmérnöki és Járműmérnöki Kar, Gépjárműtechnológia Tanszék

BEVEZETÉS

Reagálva a növekvő társadalmi igényekre a biztonságosabb és hatékonyabb közlekedés biztosítására az autóipari fejlesztések is jelentős mértékben felgyorsultak az elmúlt évtizedben, amely egyúttal további kihívásokat generált a járművek jóváhagyási és tesztelési területén is. [1] A legújabb fejlesztések, mint például a fejlett vezetés támogató rendszerek, azaz az ADAS (Advanced Driver Assistance Systems), vagy az autonóm járművek olyan további előnyöket is ígérnek, mint a zéró lokális emisszió, a szélesebb társdalami rétegek számára elérhető mobilitás. Azonban az ilyen funkciókkal szerelt járműveknek, különösen az önvezető autóknak, sokkal komplexebb közúti szituációkban kell tudni helytállni, amely szituációk modellezéséhez új tesztelési eljárások kifejlesztésére van szükség. [2] Az autonóm járművek teszteléséhez nem használhatók teljes mértékben a jellemzően az ADAS funkciók tesztelésére kifejlesztett eljárások, ugyanis az ilyen típusú járművek viselkedése változhat a különböző forgalmi szituációk és körülmények függvényében, továbbá közel végtelen számú ilyen szituáció és tesztelés céljából levezetendő kilométer vizionálható, amelyeket természetesen szinte lehetetlen a hagyományos vizsgálati módszerekkel lefedni. [3][4] Ugyan az egyre szélesebb körben elterjedt közúti teszteléssel, jelentős mennyiségű hasznos adat gyűjthető, azonban az ilyen eljárásokkal nem biztosítható a megfelelő megismételhetőség, amely a jóváhagyási és homologációs eljárások egyik kulcs eleme, továbbá az ilyen módszerek biztonsági kockázatot is hordoznak magukban a közúti közlekedés más résztvevői számára. [5] Ebből kifolyólag a zárt tesztpályán történő tesztelés továbbra is fontos részét képezi a járművek validációs folyamatainak. [6]

Jelen munka az úgynevezett Scenario-in-the-Loop (SciL) koncepciót hivatott bemutatni, amely a széleskörben használt Software-in-the-Loop (SiL), Hardware-in-the-Loop (HiL) vagy Vehicle-in-the-Loop (ViL) eljárásokhoz hasonló zárthurkú tesztelési módszer. A következő, második fejezet egy áttekintést nyújt a járműipari fejlesztések céljaik szerinti csoportjairól, valamint néhány jellemző példát mutat be a már alkalmazott fejlett tesztelési eljárásokról. Ezt követően a harmadik főfejezetben bemutatásra kerül maga a SciL koncepció, továbbá annak főbb előnyei is ismertetésre kerülnek a jelenleg használt eljárásokkal szemben a negyedik fejezetben.

JÁRMŰTESZTELÉSI ELJÁRÁSOK

Az alábbi fejezetben elsőként bemutatásra kerülnek a jaműiparban végzett tesztelési eljárások céljai azok főbb jellemzőinek ismertetésével, majd néhány olyan fejlett vizsgálati módszert mutatunk be, amelyek feltárt hiányosságainak orvoslására a SciL koncepció alkalmazása megfelelő alternatívát kínálhat.

A járműipari tesztelés főbb céljai

A járműipari tesztelési eljárásokat céljuk szerint, követve a termékfejlesztés folyamatát, három főbb csoportba lehet sorolni. Ezek az alábbiak:

- Fejlesztési célú tesztelés
- Típusjóváhagyás, előírások által szabályozott tesztelés
- Fogyasztói tesztek

A fejlesztési célú tesztelés jellemzően a korábban a szoftverfejlesztésben már elterjedt V-modell szerint történik, amely során már a tervezés korai szakaszában elkezdődik a

tesztelés és validálás, ezzel kiszűrhetők olyan hibák, melyek a tervezés fázis során tovább gyűrűzve csak nagy költség ráfordítással lennének korrigálhatók. A V-modell alkalmazása során a tesztelés végig követi a termék fejlesztését. A modul teszteléstől az integráción keresztül egészen a komplett rendszerig szinte minden szinten tesztet végzünk biztosítva, hogy a végtermékbe kerülő eszköz a lehető legkevesebb hibát hordozza magában. Ez abból a szempontból is kedvező, hogy így nem kell minden módosítást a konkrét járművön kipróbálni, ezáltal megspórolhatók például a tesztpályákon folytatott vizsgálatok költségei is. [7]

A fejlesztési tesztek során továbbá nagy mértékben használhatók szimulációk szinte a fejlesztés minden szintjén, amelyekkel jelentős költség- és időmegtakarítás érhető el. A járműipari validáció tesztek során kiemelt szerepe van az úgynevezett hurokban történő tesztelésnek, vagy más néven az „in-the-loop" típusú szimulációs módszereknek, amelyek jellemzően nyílt és zárt hurkú tesztelési eljárásokra oszthatók. Előbbiek esetén a vizsgálat tárgyát képező elem adott bemeneti adatokra történő válaszát vizsgáljuk és nem foglalkozunk az adott elem egész szimulációs rendszerre gyakorolt hatásával, míg utóbbi esetén lényeges, a rendszer reakciója a tesztelt elem által adott válaszra, amely által a bementi adatok is megváltozhatnak ezzel újabb válaszokra késztetve a tesztelt elemet. Ez az elem lehet egy egész alrendszer, de egy kisebb alegység, például egy elektronikai vezérlőegység, de akár egy szoftver vagy egy rendszer modell is, amelyekhez még nem tartozik később beépítésre kerülő konkrét hardver. Ezek alapján ilyen eljárások a teljesség igénye nélkül például az úgynevezett Model-in-the-Loop (MiL), a bevezetésben már említett SiL, és a már valós idejű tesztelés miatt nagyobb költségráfordítású HiL tesztelés. [8] Ilyen zárthurkú tesztelési eljárás a szintén említett ViL, amelynek során az egész jármű kerül a szimulációs hurokba tesztelés céljával, illetve ezen alapulva ide sorolható a jelen munkában ismertetett SciL koncepció is, amely a következő főfejezetben kerül részletesebb bemutatásra.

A típusjóváhagyás során jellemzően teljes járműveket, vagy nagyobb jármű alrendszereket, illetve bizonyos esetekben beépítésre kerülő alkatrészek megfelelőségét vizsgálják nemzetközi előírások alapján. Ezek általában konkrét megfelelési értékeket, úgynevezett „pass-fail" kritériumokat fogalmaznak meg, amelyek alapján egyértelműen eldönthető, hogy az adott jármű megfelel-e az adott előírásokban foglalt, főként műszaki követelményeknek. Emiatt az ilyen tesztek jellemzően nem nyújtanak teljekörű képet egy adott rendszer részletesebb teljesítményéről. A típusjóváhagyás során általában valós tesztek kerülnek elvégzésre, legtöbb esetben próbapályán. Az utóbbi időben azonban mind az EU, mind pedig az ENSZ munkacsoportjai elkezdték vizsgálni a szimulációk, virtuális módszerek és fejlett tesztelési eljárások típusjóváhagyási folyamataiban történő alkalmazhatóságának lehetőségeit és elkezdődött az ehhez kapcsolódó feltétel rendszerek kidolgozása. [9][10] Ugyan már találunk olyan ENSZ előírást, amely során szimulációs mérések eredményei is felhasználhatók, de a nagyobb volumenben történő alkalmazásuk a következő évtizedben megszülető előírásoktól várható. [11]

A fogyasztói tesztek során a típusjóváhagyással ellentétben már jellemzően az adott jármű vagy funkció teljesítmény mutatóinak vizsgálatára fókuszálnak. Ilyen teszteket jellemzően az úgynevezett „New Car Assessment Program" azaz az NCAP tesztek keretében vizsgálnak. Az egyik legismertebb és legrészletesebb protokollokkal rendelkező ilyen szervezet az Európában tevékenykedő EuroNCAP. A tesztek során az adott funkciókat sokkal több lépcsőben, mélyebb analízisnek vetik alá, majd az eredményeket a korábban töréstesztekből ismert öt csillaggal jelölt skálán értékelik. Ma már az öt csillagból három kapható a

passzív biztonsági rendszerekre, viszont a fennmaradót kettőt a megfelelően teljesítő ADAS funkciókkal érdemelhetik ki a gyártók. [10]

Fejlett járműtesztelési eljárások

Az elmúlt néhány évben egyre több olyan fejlett tesztelési megoldást dolgoztak ki, amelyek nagy mértékben támaszkodnak különböző szimulációs eljárásokra. Ezek nagy része a ViL metódust alkalmazza, amelynek során az egész jármű kerül tesztelésre. A ViL eljárásoknak azonban különböző implementációi léteznek. Az egyik fő jellemző, amely szerint szeparálni lehet ezeket, hogy a vizsgálat során a tesztobjektum statikus vagy mozgó jármű. Előbbi esetén gyakran úgynevezett Vehicle-Hardware-in-the-loop (VeHiL) módszerről is beszélhetünk, hiszen a jármű akár egy nagy komplex hardverként is értelmezhető. Ilyen eljárások során a járművet gyakran fékpadra, teszik és a szimuláció alapján a körülötte lévő objektumokból származó szimuláció által generált adatokat részben vagy egészben közvetlenül a jármű döntéshozó rétegében juttatják be megkerülve annak szenzorrétegét. [13] Bizonyos esetekben természetesen lehetőség van a szenzorok vizsgálatára is, például a kamerák számára kivetíthetők a különböző közlekedési szituációk, de még a radarok és a LiDAR (Light Detection and Ranging) szenzorok számára is létezik olyan célobjektum generáló megoldás, amely képes elnyelni a jármű ilyen szenzorai által kibocsátott hullámokat és a szimulációban történtek alapján a megfelelő reflexiókat biztosítani. [14]

A klasszikus ViL eljárás során a tesztelt jármű, azaz VUT-vel (Vehicle Under Test) ténylegesen közlekedik a tesztelés közben. Ilyenkor jellemzően a VUT egy olyan biztonságos környezetben halad, ahol azon kívül nem található más olyan objektum, amellyel összeütközhet. [15] Ilyen környezetek jellemzően a járműipari próbapályák dinamikai felületeti. A teszt során a járműben található az szimulációs számítógép, amely a jármű szenzorinak adatokat szolgáltat a szimulációban zajló forgalmi szituációk alapján. A jármű valós mozgása a szimulációba általában valamilyen nagypontosságú helymeghatározó és inerciamérő berendezés, az INS (Inertial Navigation System) által szolgáltatott adatokon alapul, így a szimulációban közlekedő digitális iker pontosan ugyanúgy viselkedik, mint a valós jármű. A jármű mozgása alapján a közlekedési szituációk szereplői reagálnak a tesztelt járműre, amely így a szimulációból érkező generált adatok alapján különböző beavatkozásokat, például vészfékmanővert végezhet úgy, hogy a jármű teljes dinamikai jellemzői vizsgálhatóak maradnak anélkül, hogy valós ütközésveszély állna fenn. Az ilyen klasszikusnak nevezhető ViL szimulációk alapvetően a járművezetők szokásainak és a vezetés támogató rendszerek együttműködésének kiértékelésére lettek kifejlesztve. [16] A jelen munkában bemutatott SciL koncepció architektúrája nagyban támaszkodik a klasszikus ViL eljárás modelljére.

A ViL eljárások azonban rendelkeznek bizonyos korlátokkal. Ilyen például, hogy sok esetben nem lehet a már említett összes szenzort tesztelni azok megkerülése nélkül, továbbá amennyiben a statikus ViL megoldások kerülnek alkalmazásra, akkor nem nyerhetünk megfelelő kinematikai és dinamikai információkat a járműből.

További fejlett eljárásoknak tekinthetők az úgynevezett „mixed reality” eljárások, amelyekben a virtuális és valós elemeket ötvözik akár valós időben is. Ilyen tesztelés során lehetőség van például térben szeparált szereplőket a virtuális térben közösen tesztelni. Például egy gyalogos mozoghat egy laborkörnyezetben, ahol a mozgását pontosan rögzítik, majd ez alapján, egy a tesztpályán közlekedő jármű számára juttatják el gyalogosról alkotott

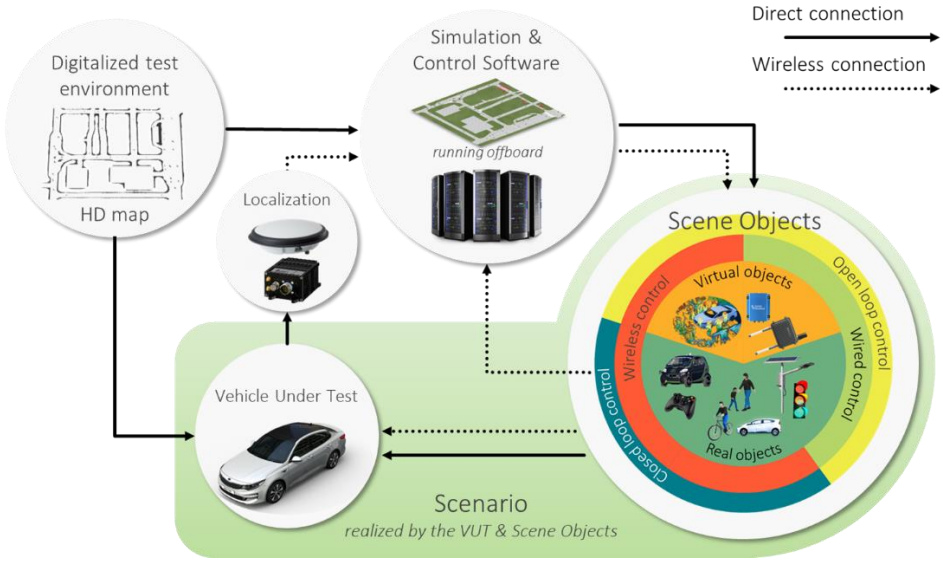
akár nyers szenzoradatot a digitális iker környezet alkalmazásával annak érdekében, hogy még realisztikusabb kihívás elé állítsák a járművet a valós ütközés veszélyének kizárásával.

A SCENARIO-IN-THE-LOOP KONCEPCIÓ

A SciL koncepció a ViL szimuláción alapuló főként tesztpályákon alkalmazható zárt hurkú tesztelési eljárás, amely egyik fő célja az önvezető járművek biztonságos környezetben, megismételhető módon történő tesztelése. [18] Az alábbiakban bemutatásra kerül a SciL működési modellje, illetve a ki és bemeneti oldali elemei, valamint azok rendszerezési lehetőségei.

A SciL működési modellje, architektúrája

Ahogy az már korábban említésre került, a SciL koncepció architektúrája nagyban támaszkodik az előző fejezetben bemutatott ViL működési modelljére, valamint sajátosságaira. Az 1. Ábra a SciL architektúráját szemlélteti. [19] A SciL esetén is a VUT nem statikus, hanem egy tesztkörnyezetben mozog, azonban ez a tesztkörnyezet már valósághű kialakítású környezet kell legyent, például városi tesztkörnyezet, országút vagy autópálya. Ez a környezet a statikus elemeken kívül, – mint amilyen maga az úthálózat felfestésekkel, a szegélyek, járdák, járdaszigetek vagy utcai bútorok –, további objektumokat, például mozgó forgalmi szereplőket is tartalmazhat.



1. Ábra: A Scenario-in-the-Loop koncepció architektúrája, forrás: [19]

A rendszer központi eleme a szimulációs és kontrol szoftver (*Simulation & Control Software*), amelynek egyik bementi eleme a valós tesztkörnyezet pontos virtuális modellje (*Digitalized test environment*), hiszen fontos, hogy a szoftverben lezajló szimulációk összerendelhetők legyenek a valóságban megtalálható infrastruktúrával. Ez a virtuális modell ideális esetben a VUT navigációs rendszerébe is betöltésre kerül például valamilyen nagyfelbontású térkép (*HD map*) formájába, hogy az autó is ismerje az általa bejárható környezetet. A tesztelés során legoptimálisabb esetben a tesztelt járművet egy „black box” jellegű

elemnek tekinthetjük, amely belső jellemzőibe, – beleértve a benne működő vezérlési algoritmusokat is –, nem kell belelátnunk, csupán csak a tesztpályán történő viselkedését kell független módszerekkel megfigyelni, regisztrálni. A jármű mozgása szintén egy bemeneti elemet jelent a központi szoftver számára, amely a jármű lokalizációs adatai (*Localization*) alapján jeleníti meg annak virtuális mását, úgynevezett digitális ikrét a szimulációban, majd ezek alapján futtatja a különböző tesztesetek, azaz a szcenáriókat. A kimeneti oldalon fellelhető zavarások (*Scene Objects*) vezérlését szintén ez a központi szoftver látja el a benne futó szimulációk alapján. Ezek a zavarások így hatással tudnak lenni a VUT viselkedésére, ezzel gyakorlatilag zárva a SciL zárthurkú modelljét. A VUT és a zavarások együttesen folyamatos teszteseteket hoznak létre vagy definiálják újra azokat, ezzel lényegében a folyamat központi elemévé téve magát a szcenáriót (*Scenario*). Ebből jött létre a Scenario-in-the-Loop elnevezés. A klasszikus ViL megoldással ellentétben a szimulációs és kontrol szoftver már nem a járműben helyezkedik el, hanem egy irányító központban található. Ennek legfőbb oka, hogy a feladat ellátásához nagyobb számítási kapacitású számítógépekre lehet szükség, amelyek méretükből kifolyólag nem minden esetben helyezhetők el a VUT fedélzetén. Ezért a központi szoftver a zavaró célú objektumokkal és a tesztel jármű lokalizációját végző rendszerrel rádiókommunikációs kapcsolaton kommunikál, amellyel szemben szigorú hatótávolsági és késedelmi követelmények támaszthatók.

A SciL bemeneti oldali elemei

A SciL koncepciónak két fő bemente van, ebből az egyik maga a fizikai tesztkörnyezet, valamint annak virtuális modellje, a másik pedig maga a VUT, pontosabban annak mozgása, viselkedése.

A fizikai környezet tulajdonságai általában a tesztek során nem változnak, így az ebből származó adatok statikusnak tekinthetők. Ezek a környezetek jellemzően komplexebb úthálózatokat és olyan további elhelyezett objektumokat tartalmaznak, amelyek jól közelítik a valós közúti viszonyokat. Ilyen valósághű tesztkörnyezet például a Zalaegerszegen létesített ZalaZONE Járműipari Tesztpálya „Smart City" elnevezésű városi tesztkörnyezete, autópályája és országúti tesztkörnyezete is. [20] Az ezeken alapuló virtuális környezettel szemben azonban már számos kritérium támasztható, – mint például annak logikai kialakítása, geometriai helyessége, felbontása vagy a magassági jellemzői –, amelyek mind befolyásolhatják a tesztelt jármű digitális reprezentációjának viselkedését. [21] Továbbá a virtuális környezetben lehetőség van különböző dinamikusan változó paraméterek alkalmazására is, mint például az időjárási vagy fényviszonyok. Fontos megjegyezni, hogy a virtuális környezetek teljeskörű leírására még nem létezik uniformizált megoldás, azonban számos standard, és leíró módszert dolgoztak ki erre a célra. Ilyenek például az OpenDIRVE® és OpenCRG® standardok, amelyek az úthálózatok logikai és geometriai, valamint felületi és magassági jellemzőit írják le. [22] Virtuális környezetek különböző módokon hozhatók létre, például megépíthetők a különböző járműipari szoftverek virtuális környezetmodellező programjaival, de annak érdekében, hogy a lehető legnagyobb egyezőség álljon fenn a virtuális és valós tesztkörnyezet között, érdemes például a valós környezet lézerszkennelésén alapuló pontfelhőkből előállítani azokat. [23]

A bemenő adatok további forrásai a tesztelt jármű vagy járművek, azok vontatmányai, illetve a tesztben résztvevő többi zavaró célú mozgó objektum lokalizációs informá-

ció. Ezek már előállíthatók akár külső szenzorok, pl. kamerák és LiDAR-rok detekciói alapján is. [24] Jellemzően napjainkban inkább még mindig az autóiparban elterjedt, járműbe szerelhető nagypontosságú lokalizáció egységeket alkalmazzák erre a célra. Az ilyen lokalizációs eszköz célszerűen valamilyen INS (Inertial Navigation Unit), amely két fő egység, egy DGNSS (Differential Global Navigation Satellite System) és egy IMU (Inertial Measurement Unit) kombinációjából áll. A kettő együttes használatával érhető el az a megfelelő pontosság, amely a szimulációhoz is szükséges. Az IMU általában tartalmaz mindhárom tengely irányába egy lineáris gyorsulásmérőt, illetve egy rotációs elven működő mérőegységet, amelyek segítségével a mérés során a mozgás minden szabadsági foka lefedhető. Az INS eszköz esetén előnyös, ha olyan DGNSS alegységet tartalmaz, amelynek kettő antennája van, ezáltal képes a jármű irányát is mérni. A jobb, akár 1 cm-es pontosság elérése érdekében a DGNSS differenciális korrekciót használ, amely egy tesztelési helyszínre kitelepített bázisállomáshoz viszonyított lokalizációs adatokkal korrigálja a hagyományos műholdas rendszerből származókat. A korrekciós jel azonban érkezhet más forrásból is, például celluláris hálózaton keresztül.

A tesztelt jármű esetén fontos megemlíteni, hogy amennyiben a SAE (Society of Automotive Engineers) által definiált jármű automatizáltságot leíró szinteken 3 vagy magasabb szintű járműről van szó, akkor elégséges lehet a fentebb említett INS egység beszerelése. Amennyiben viszont a jármű nem képes teljesen autonóm vezetésre, azaz 2 SAE szintű vagy az alatti, akkor szükség lehet egy kormány és pedálrobotokból álló úgynevezett Driverless Test System (DTS) beszerelésére, amely képes vezetni a kontrolszoftver által meghatározott módon a járművet. [25] Ez azonban inkább ADAS funkciók tesztelésénél jellemzőbb.

A SciL kimeneti oldali elemei és csoportosítási módjaik

A SciL kimeneti oldalán található elemek, vagy úgynevezett zavarások öt főbb típusba sorolhatók:

- VUT szenzor „spoofing”
- V2X kommunikációs „spoofing”
- Mozgó célobjektumok
- Kontrolált mozgású valós járművek
- Infrastruktúra elemek

A VUT szenzor „spoofing” lényegében a VUT szenzorrétegének megkerülésével operáló megoldás, amely során a szimulációs és kontrol szoftverből jövő virtuális információk közvetlenül a jármű döntéshozó rétegébe kerülnek bejuttatásra, ezáltal mintegy becsapva a járművet, amelyet ezzel lehet különböző interakciókra késztetni a virtuális szereplőkkel. Ez a megoldás hasonlít a ViL esetén alkalmazott módszerre, azonban ebben az esetben az információ a központi számítógépen futó szimulációból származik, és onnan kell rádiókommunikációs megoldás alkalmazásával eljuttatni a VUT fedélzetére. A megoldás előnye, hogy veszélyes, nehezen kivitelezhető forgalmi szituációkon alapuló szcenáriók is tesztelhetők a segítségével, biztonságosabbá és költséghatékonyabbá téve a vizsgálatokat. Például lehetőség van ily módon forgalmi dugók, nagy járművek, például vonat vagy villamos szcenáriókban történő szerepeltetésére.

A V2X kommunikációs „spoofing” szintén a jármű kvázi becsapásán alapul, viszont jelen esetben a szimulált információ érkezhet a valós V2X kommunikációs hálózaton

keresztül szabványos üzenetek formájába, amely nem igényel semmilyen szenzor megkerülést a VUT oldaláról. Az eljárás lényege, hogy a zavarás nem feltétlenül létezik a valóságban, de mégis szabványos információ küldhető a létezéséről, amely bizonyos reakciókat válthat ki a VUT-ből. Például, ha a jármű olyan információt kap a V2X hálózaton keresztül, hogy az eredetileg választott útszakaszon forgalmi dugó alakult ki, dönthet úgy, hogy másik útvonalat választ. Hasonlóan egy nem belátható kereszteződést óvatosabban közelít meg, ha arról kap információ, hogy más járművek érkezhetnek a többi irányból. Mind a V2X, mind pedig a VUT szenzor „spoofing" lehetőséget nyújthat a jármű kiberbiztonsági képességeinek, aspektusainak vizsgálatára is.

A zavaró célú mozgó célobjektumok két csoportra oszthatók. Az egyik csoportot a járművek, a másikat pedig a sérülékeny úthasználókat reprezentáló úgynevezett VRU (Vulnerable Road User) dummy-k alkotják. Ezeket az objektumokat jellemzően platformok hordozzák, amelyeknek attól függően, hogy például járművet vagy gyalogost hordoznak másmás mérettel és végsebességgel kell rendelkezniük, de alapvető tulajdonságaikban jellemzően megegyeznek. Ilyen tulajdonságok például, hogy a platformoknak ki kell bírniuk egy elütés esetén azt, ha áthajtanak rajtuk úgy, hogy nem okoznak sérülést a tesztelt járműben sem. Fontos a megfelelő rendelkezésreállás, ezért kellően jó akkumulátor idővel kell rendelkezniük. Ahhoz, hogy az érzékelés szempontjából is megfelelők legyenek a platformoknak kis radarkeresztmetszettel kell rendelkeznie, így nem zavarják meg a jármű szenzorait. A platformoknak továbbá szintén tartalmazniuk kell INS egységet azért, hogy egyrészt a mozgásukat a szimulációs szoftver is tudja követni, illetve a szoftver által végrehajtandó parancsokhoz az eszköz saját maga is a lokalizációs információit tudja visszacsatolásként felhasználni. Ez tehát rádiókommunikációs aspektusból is fontos, hiszen a szoftver és a platformok közötti két irányú adatkapcsolatot kell létesíteni, ahol szoftver irányába történő visszajelzésnél esetén fontos a kis késedelem. A platformokon túl az általuk hordozott dummy-knak is vannak közös tulajdonságaik. Például megfelelő radarreflexiójú anyagból kell készíteni őket, továbbá előnyös, ha elütésük esetén nem sérülnek jelentősen, hanem például olyan darabokra hullanak szét, amelyeket viszonylag rövid idő alatt egy újabb teszthez össze lehet építeni. Az VRU-k esetén fontos lehet, ha belülről fűthetők, hiszen így akár infrakamerás rendszerek is tesztelhetők velük. Sétáló gyalogos bábuk esetén fontos a lábak mozgása, amely kiegészíthető a karok és a fej mozgásával, biciklis bábuk esetén pedig ilyen meghatározó a kerekek és a pedálozó láb mozgása is. A kerekek forgása motorbiciklis dummy-k esetén is fontos lehet, csakúgy, mint a rajtuk különböző testhelyzetben elhelyezett bábuk alkalmazása. Az emberi dummy-k mellett használhatunk még több különböző méretű állatot megformáló dummy-t is.

A mozgó célobjektumok mellett használhatunk még valós járműveket is, amelyek mozgását valamilyen módon kontrolálni kell a központi szoftverből. Ezek a valós járművek vagy DTS vagy akár a saját aktuátoraik segítségével is vezethetők, és jellemzően kevésbé biztonságkritikus szcenáriókban és szerepekben használatosak.

Kimenő oldali szereplőként még az olyan infrastrukturális elemeket említhetjük, mint a különböző forgalom irányító lámpák és aktív dinamikus forgalom korlátozó jelek, valamint a szenzorok zavarására alkalmas esőztető berendezés és különböző megvilágítások.

A kimeneti oldali elemek, zavarások háromféleképpen kategorizálhatók (1. Ábra):

- Valós vagy virtuális objektum
- Vezetéknélküli vagy vezetékes vezérlés
- Zárt vagy nyílt hurkú szabályozás

A valós objektumok közé tartoznak a mozgó objektumok, valós járművek és infrastrukturális elemek, tehát minden, amelynek van valós reprezentációja. A virtuális elemek és V2X információk csak a szimulációban léteznek és jellemzően „spoofing" technológiával jutnak el a VUT-be.

A vezetéknélküli vezérlésű eszközök jellemzően a mozgó objektumok és járművek, valamint azok a virtuális információk, amelyeket közvetlenük a VUT döntéshozó rétegébe kell bejuttatni a központi szoftverből. Az infrastrukturális elemek és a V2X hálózat jeladói azonban közvetlenül vezetéken csatlakozhatnak a központi szoftvert futtató szerverekhez így azok esetén nincs szükség vezetéknélküli kapcsolatra.

Azok az eszközök, amelyeknek módosítani kell a viselkedését a VUT mozgás alapján, zárt hurkú szabályozásúnak tekinthetők. Ezek közé tartoznak a mozgó objektumok és valós járművek, hiszen ezek esetén a kontrol szoftvernek tudnia kell, hogy hogyan és hol mozognak a tesztpályán a szcenárió közben. A többi típusú zavarás esetén jellemzően elég csak elküldeni a megfelelő vezérlési információt.

A SCENARIO-IN-THE-LOOP ALKALMAZÁSÁNAK FŐBB JELLEMZŐI

Az előzőekben bemutatottak alapján látható, hogy a SciL alkalmazásának számos előnye van a klasszikus ViL eljárásokkal szemben, azonban a SciL koncepció alkalmazásának is vannak bizonyos korlátjai. Az alábbi két alfejezetben ezek a főbb előnyök és limitációk kerülnek részletesebben bemutatásra.

A SciL felhasználásának előnyei

A SciL alkalmazásának egyik meghatározó jellemzője, hogy lehetőséget biztosít sokkal realisztikusabb tesztek elvégzésére, amely nagy előnyt jelent az autonóm járművek tesztelésében. Ugyanis a jelenleg főként ADAS funkciók tesztelésére használt tesztesetek nem használhatók fel teljes mértékben erre a célra, mivel az autonóm járművek esetében nem biztosítható minden esetben, hogy a jármű teljesítse a tesztesetek bementi kritériumait, ezzel érvénytelen teszt futásokat létrehozva, ezáltal a tesztek kiértékelése sem végezhető el a megszokott módszerekkel. A realisztikus környezetben végzett tesztek is jobban illeszkednek az autonóm járművekhez szemben az ADAS funkciók steril környezetben végzett tesztjeivel.

További előny, hogy a központi szimulációs kontroll szoftvernek köszönhetően a tesztesetek lefutása sokkal flexibilisebben kivitelezhető, ugyanis a szoftver képes az önvezető jármű viselkedéséhez igazítani a különböző zavarások mozgását, aktivációját, ezáltal folyamatos, jól időzített kihívás elé állítva a járművet. Ebből kifolyólag az előző pontban említettnek megfelelően a tesztelt járműnek nem kell szigorúan követni a tesztesetek érvényességi kritériumait, hiszen azokat a szoftver minden esetben a jármű viselkedéséhez igazítja. Ettől függetlenül a koncepció alkalmas lehet ADAS funkciók vizsgálatára is, ebben az esetben azonban a flexibilitásra kevésbé van szükség, valamint a realisztikus környezet megléte sem feltétlenül szükséges.

Ellentétben a közúton végzett teszteléssel, a SciL koncepció lehetőséget biztosít a reprodukálható tesztelésre is, amely fontos kritérium a jóváhagyási validációs folyamatokban. Még akkor is, ha a tesztesetek bementi feltételei változnak a jármű viselkedése alapján, de az általuk reprezentált forgalmi szituációk ugyanazon kihívások elé állítják a tesztelt járműveket.

A koncepció egy további előnye, hogy nem csak teljes járműrendszerek vagy funkciók tesztelésére nyújt lehetőséget, hanem segítségével akár egyéb mobilitással és közlekedési infrastruktúrával összefüggő, azokba integrálható eszközök tesztelését is elvégezhetjük. Például lehetőség van kommunikációs eszközök tesztelésére, mint például a különböző V2X eszközök, de akár okos forgalomirányítási megoldások, és egyéb ITS (Intelligent Transportation Systems) applikációk is megvizsgálhatók a segítségével. Ilyen esetben az önvezető járművek is válhatnak zavaró célú objektummá a tesztelt eszköz szemszögéből.

Egy további előny, hogy a központi szoftver szimulációs része jól felhasználható a valós mérésekből történő teszteset absztrakcióra, valamint ezen alapulva további szcenáriók generálhatók a szimulációkra jellemző előnyök felhasználásával.

A SciL alkalmazásának korlátjai

A SciL kritikusabb elemei közé sorolható a zárthurkú tesztelésben megjelenő kommunikációs és számítási késedelem kérdése. Annak érdekében, hogy a teszteszközök aktiválási kritériumainak flexibilitását fenn lehessen tartani, szükség van a mozgó objektumok, központi szoftverrel történő kis késedelmű, de mégis nagy hatótávú rádiókommunikációs összeköttetésére, beleértve mind a tesztelt járművet, mind pedig annak viselkedését befolyásoló zavarásokat. Ehhez hozzáadódhat még a szimuláció újra definiálásának számítási ideje, ezzel pedig a virtuális környezet és a valóság között olyan eltolódás jöhet létre, amely veszélyezteti a zavarások megfelelő időzítését, illetve a szcenáriók reprodukálhatóságát. Már léteznek olyan megoldások, amelyek akár mindösszesen 10-20 ms késedelmet ígérnek, de a tesztesetben résztvevő szereplők potenciális nagy száma miatt, valamint az esetleges infrastruktúra okozta interferenciák további rizikófaktorként jelennek meg.

Ahogy az korábban már bemutatásra került, a SciL lehetőséget biztosít a ViL eljárásoknál megismert virtuális zavarásokkal történő még komplexebb szcenáriók létrehozására. Azonban ehhez fel kell adni a tesztelt járműtől való teljes függetlenséget, és meg kell kerülni a jármű szenzorendszerét. Viszont erre csak akkor van lehetőség, ha a jármű gyártó megadja a hozzáférést a jármű megfelelő alrendszereihez, hogy a virtuális információ bejuttatható legyen. Továbbá a labor környezettel ellentétben a különböző szintű szenzor szimulációk elvégzése próbapályán további kihívást jelent. Szükség lehet nagy számítási képességű eszközök beszerelése, amelyek megfelelően aktiválhatók a központi szoftverből, vagy szélessávú rádiókommunikáció kapcsolatra, a nagy mennyiségű adat központi számítási egységekből történő továbbítására.

A folyamatos valós időben történő teszteset kontrolláláshoz speciális szoftverekre is szükség van, amelyek jelenleg nem érhetők el a SciL központi szoftverének minden igényét kielégítő módon kereskedelemi forgalomban, így azokat le kell fejleszteni. Ehhez érdemes lehet összekapcsolt szimulációs megoldásokat, úgynevezett „co-simulation” technológiákat alkalmazni, amelyre azonban már találhatunk ígéretes példákat a gyakorlatban. [26] A megfelelő működéshez azonban szükség van a különböző hardverek és a szoftverek közötti interfészek létrehozására is, amely szintén további kihívásokat tartogat.

ÖSSZEFOGLALÁS

A SciL koncepció egy olyan újszerű tesztelési koncepció, amely lehetőséget biztosít az önvezető járművek reprodukálható módon, biztonságos környezetben történő tesztelésére. A SciL központi szoftvere képes kontrolálni a teszteléshez használt valós objektumokat, de ezen felül virtuális zavarások segítségével is képes kihívások elé állítani a tesztelt járművet. A koncepció előnye, hogy realisztikus tesztkörnyezetet biztosít, amelyben a futtatott szcenáriókat képes flexibilisen a VUT mozgásához igazítani, ezáltal fenntartva a megismételhetőséget, valamint felhasználható különböző ITS eszközök tesztelésére és újabb szcenáriók létrehozására is. Fontos azonban megjegyezni, hogy a munkában bemutatott komplex SciL koncepció még nem került teljesen megvalósításra, de már léteznek kutatások és megoldások, amelyek a koncepció alapján kerültek realizálásra. [27] A SciL vizsgálata és teljeskörű létrehozása így további kutatási feladatoknak adhat teret.

ALKALMAZOTT RÖVIDÍTÉSEK

ADAS	Advanced Driver Assistance Systems
DGNSS	Differential Global Navigation Satellite System
DTS	Driverless Test System
EuroNCAP	European New Car Assessment Programme
HiL	Hardware-in-the-Loop
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
ITS	Intelligent Transportation Systems
LiDAR	Light Detection and Ranging
MiL	Model-in-the-Loop
SAE	Society of Automotive Engineers
SciL	Scenario-in-the-Loop
SiL	Software-in-the-Loop
ViL	Vehicle-in-the-Loop
VRU	Vulnerable Road User
VUT	Vehicle Under Test
V2X	Vehicle-to-everything communication

FELHASZNÁLT IRODALOM

[1] P. Koopman and M. Wagner, “Challenges in Autonomous Vehicle Testing and Validation,” *SAE Int. J. Trans. Safety*, vol. 4, no. 1, pp. 15–24, Apr. 2016, doi: 10.4271/2016-01-0128.

[2] L. Chen et al., “Milestones in Autonomous Driving and Intelligent Vehicles: Survey of Surveys,” *IEEE Trans. Intell. Veh.*, vol. 8, no. 2, pp. 1046–1056, Feb. 2023, doi: 10.1109/TIV.2022.3223131.

[3] D. Zhao *et al.*, “Accelerated Evaluation of Automated Vehicles Safety in Lane-Change Scenarios Based on Importance Sampling Techniques,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 595–607, Mar. 2017, doi: 10.1109/TITS.2016.2582208.

[4] M. D. Vaio, P. Falcone, R. Hult, A. Petrillo, A. Salvi, and S. Santini, "Design and Experimental Validation of a Distributed Interaction Protocol for Connected Autonomous Vehicles at a Road Intersection," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9451–9465, Oct. 2019, doi: 10.1109/TVT.2019.2933690.

[5] C. Nowakowski, S. E. Shladover, and C.-Y. Chan, "Determining the Readiness of Automated Driving Systems for Public Operation: Development of Behavioral Competency Requirements," *Transportation Research Record*, vol. 2559, no. 1, pp. 65–72, Jan. 2016, doi: 10.3141/2559-08.

[6] N. Katzorke, M. Moosmann, R. Imdahl, and H. Lasi, "A Method to Assess and Compare Proving Grounds in the Context of Automated Driving Systems," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, Sep. 2020, pp. 1–6. doi: 10.1109/ITSC45102.2020.9294310.

[7] B. Liu, H. Zhang, and S. Zhu, "An Incremental V-Model Process for Automotive Development," in *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*, Dec. 2016, pp. 225–232. doi: 10.1109/APSEC.2016.040.

[8] N. Hansen, N. Wiechowski, A. Kugler, S. Kowalewski, T. Rambow, and R. Busch, *Model-in-the-Loop and Software-in-the-Loop Testing of Closed-Loop Automotive Software with Arttest*. Gesellschaft für Informatik, Bonn, 2017. Accessed: Jan. 02, 2024. [Online]. Available: https://dl.gi.de/items/bab4a8a8-6908-4534-92f0-2e6bbed1892f

[9] Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down Rules for the Application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles (Text with EEA Relevance). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1426 (accessed on 4 April 2023).

[10] UNECE: New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS). 2022. Available online: https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-58.pdf

[11] UNECE 1958 Agreement: Addendum 139–Regulation No. 140: Uniform Provisions Concerning the Approval of Passenger Cars with Regard to Electronic Stability Control (ESC) Systems. 2017. Available online:
https://unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2017/R140e.pdf

[12] EuroNCAP ASSESSMENT PROTOCOL – OVERALL RATING, Version 9.1.1 2021. Available online: https://cdn.euroncap.com/media/67890/euro-ncap-assessment-protocol-overall-rating-v911.pdf

[13] R. Donà, S. Vass, K. Mattas, M. C. Galassi, and B. Ciuffo, "Virtual Testing in Automated Driving Systems Certification. A Longitudinal Dynamics Validation Example," *IEEE Access*, vol. 10, pp. 47661–47672, 2022, doi: 10.1109/ACCESS.2022.3171180.

[14] A. Diewald *et al.*, "Radar Target Simulation for Vehicle-in-the-Loop Testing," *Vehicles*, vol. 3, no. 2, Art. no. 2, Jun. 2021, doi: 10.3390/vehicles3020016.

[15] S. A. Fayazi, A. Vahidi, and A. Luckow, "A Vehicle-in-the-Loop (VIL) verification of an all-autonomous intersection control scheme," *Transportation Research Part C: Emerging Technologies*, vol. 107, pp. 193–210, Oct. 2019, doi: 10.1016/j.trc.2019.07.027.

[16] T. Bock, „Vehicle in the Loop–Test und Simulationsumgebung für Fahrerassistenzsysteme” in *Audi Dissertationsreihe*, Vieweg: Göttingen, Germany, 2008; Volume 10.
[17] M. F. Drechsler, J. Peintner, F. Reway, G. Seifert, A. Riener, and W. Huber, “MiRE, A Mixed Reality Environment for Testing of Automated Driving Functions,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3443–3456, Apr. 2022, doi: 10.1109/TVT.2022.3160353.
[18] H. Németh, A. Háry, Z. Szalay, V. Tihanyi, and B. Tóth, “Proving Ground Test Scenarios in Mixed Virtual and Real Environment for Highly Automated Driving,” in *Mobilität in Zeiten der Veränderung : Technische und betriebswirtschaftliche Aspekte*, H. Proff, Ed., Wiesbaden: Springer Fachmedien, 2019, pp. 199–210. doi: 10.1007/978-3-658-26107-8_15.
[19] Z. Szalay, “Next Generation X-in-the-Loop Validation Methodology for Automated Vehicle Systems,” *IEEE Access*, vol. 9, pp. 35616–35632, 2021, doi: 10.1109/ACCESS.2021.3061732.
[20] Z. Szalay, Z. Hamar, and Á. Nyerges, “Novel design concept for an automotive proving ground supporting multilevel CAV development,” *International Journal of Vehicle Design*, vol. 80, no. 1, pp. 1–22, Jan. 2019, doi: 10.1504/IJVD.2019.105061.
[21] B. Tóth and Z. Szalay, “The role of the virtual environment fidelity in proving ground related vehicle simulations,” presented at the 38th International Colloquium on Advanced Manufacturing and Repairing Technologies in Vehicle Industry, Visegrád, Hungary, May 24-26, 2023.
[22] M. Dupuis and H. Grezlikowski, “OpenDRIVE® – An open standard for the description of roads in driving simulations,” presented at the Driving Simulation Conference, Paris, France, 4–6 October 2006; pp. 25–36.
[23] K. Gangel *et al.*, “Modelling the ZalaZONE Proving Ground: a benchmark of State-of-the-art Automotive Simulators PreScan, IPG CarMaker, and VTD Vires,” *Acta Technica Jaurinensis*, vol. 14, no. 4, Art. no. 4, Nov. 2021, doi: 10.14513/actatechjaur.00606.
[24] V. Tihanyi *et al.*, “Towards Cooperative Perception Services for ITS: Digital Twin in the Automotive Edge Cloud,” *Energies*, vol. 14, no. 18, Art. no. 18, Jan. 2021, doi: 10.3390/en14185930.
[25] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, SAE Ground Vehicle Standard J3016_202104, 2021, Available online: https://saemobilus.sae.org/content/j3016_202104
[26] B. Toth and Z. Szalay, “Development and Functional Validation Method of the Scenario-in-the-Loop Simulation Control Model Using Co-Simulation Techniques,” *Machines*, vol. 11, no. 11, Art. no. 11, Nov. 2023, doi: 10.3390/machines11111028.
[27] Z. Szalay, M. Szalai, B. Tóth, T. Tettamanti, and V. Tihanyi, “Proof of concept for Scenario-in-the-Loop (SciL) testing for autonomous vehicle technology,” in *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*, Nov. 2019, pp. 1–5. doi: 10.1109/ICCVE45908.2019.8965086.

THE APPLICATION OF THERMAL PHENOMENA IN FIRE DETECTION

A TERMIKUS JELENSÉGEK ALKALMAZÁSA A TŰZJELZÉSBEN

NAGY Rudolf [1]

Abstract

The preventive fire protection of establishments at risk of a possible outbreak of fire is a very important part of the built-in fire protection systems. The effective use of technical devices for active intervention in the protection of life and property depends on their professional selection, installation, operation and maintenance. The origin of all this lies in an adequate knowledge of fire detection methods and their harmonisation with the physical environment of the installation. In order to detect fire in the space to be protected, the combustion properties of the materials present must also be synchronised with the technical conditions of the signalling technology. The automatic and rapid detection of fire is also one of the most important prerequisites for effective damage control. This also includes the rapid localisation of the fire scene, which provides the physical environment for combustion. Recognising the thermal signals of the fire action occurring in this area before the fire has developed beyond control and separating them from other disturbing thermal phenomena that may occur in normal operation is a key factor in triggering the appropriate detectors in fire protection systems.

Keywords

fire, heat, combustion, fire safety, detector

Absztrakt

A tűz lehetséges kitörésével veszélyeztetett létesítmények megelőző tűzvédelmének igen fontos részét képezik a beépített tűzvédelmi berendezések. Az élet-, és vagyonvédelem aktív beavatkozást végrehajtó technikai eszközök effektív alkalmazásának alapja a szakszerű kiválasztás, telepítés, valamint az üzemeltetés és karbantartás adekvát módja. Az említettekből mindezek origóját a tűzérzékelés módszereinek megfelelő ismerete és a létesítményi fizikai környezettel való összhangba hozása jelenti. A tűznek védendő térben való felismeréséhez a jelenlévő anyagok égését kísérő tulajdonságait is szinkronba szükséges hozni a jelzéstechnika műszaki feltételeivel. A tűz automatikus, gyors jelzése az eredményes kárelhárításnak is az egyik legfontosabb előfeltétele. Ebbe ugyancsak beletartozik az égés fizikai környezeti feltételeit megteremtő tűzhelyszín gyors lokalizálása. Az itt előálló tűzhatás hőtani jeleinek még a tűz megfékezhetetlen kifejlődése előtti felismerése és más rendeltetésszerűen jelentkezhető zavaró termikus jelenségektől való elkülönítése kiemelt szereppel bír a tűzvédelmi berendezések megfelelő érzékelőinek kiváltásában.

Kulcsszavak

tűz, hő, égés, tűzbiztonság, érzékelő

[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

Mára a beépített tűzjelző rendszerek az épített környezetünk biztonságtechnikájának elengedhetetlen komponensei. Az azokban hasznosított jelzéstechnika a legmodernebb műszaki megoldások teljes arzenálját felvonultatja, hogy kielégíthessük a tűzbiztonság valamennyi igényét. Az azokban megjelenő műszaki megoldások az egészen triviális hőtágulás elvén működőktől, a félvezetőkön keresztül a fejlett integrált áramköri detektorokig terjedő valamennyi lehetőséget kiaknázzák a tűzzel szembeni védelem érdekében.

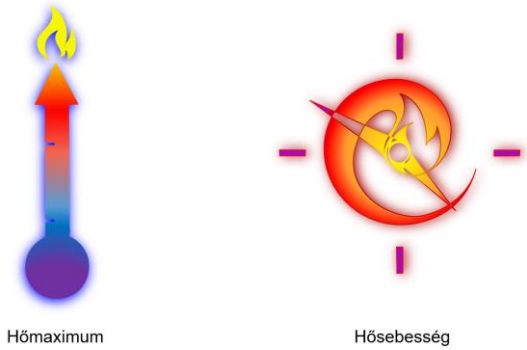
Az élet- és a vagyonvédelem ezen területe a társadalmi élet színterét adó szórakozás, pihenés-vendéglátás, valamint a különféle szolgáltatásokat nyújtó közösségi rendeltetésű helyek, illetőleg az ipari, mezőgazdasági termelés folytató nagyüzemek, stb. létesítményeit kiszolgálja. A technikai civilizációnk fejlődése miatt épített környezetünk egyre nagyobb volumenű és egyre újabb eredetű veszélynek vannak kitéve a tüzek oldaláról. Az ezt kiváltó okok között találjuk a költséghatékonyságra törekvés eredőjeként „megszülető" mind nagyobb befogadóképességű és az egyre szélesebb funkciókat integráltan kielégíteni képes építmenyek és a komplex infrastrukturális kapcsolatokkal rendelkező épületkomplexumok létrejöttét. Ezek és a társadalmi, környezeti változások a tűzbiztonság mind változatosabb kockázati tényezőivel szembesítenek bennünket. Az ezekből származó tűzesetek előidézte károk elhárításra fordítható erőforrásaink egyik legkritikusabb tényezője az idő. Így a tűz megnövekedett veszélyének csökkentésére, illetőleg a hatékony reagálásra állandó, nagy megbízhatóságú, automatikus felügyeleti rendszereket kell alkalmaznunk. A modern beépített tűzvédelmi berendezések kiemelkedő jelentősége abban rejlik, hogy az időben kiadott riasztás révén megfelelő időelőnyt biztosít a tűzzel fenyegetettek az épületen kívül, a csatlakozó terepszintre, illetőleg biztonságos átmeneti védett térbe meneküléséhez. Továbbá lassítani lehet a tűz terjedését elősegítő termikus változások kifejlődését, valamint optimalizálhatók a tűzoltáshoz kivonuló beavatkozók számára rendelkezésre álló tűzoltási feltételeket. Tehát minél korábban sikerül detektálni a kialakult tűz veszélyt, annál eredményesebben avatkozhatnak be az aktív tűzvédelmi berendezések, valamint a tűzoltók a tűz megfékezése és elszigetelése érdekében. [1]

A tűz során felszabaduló hő a tűzhelyszín környezetében hőmérsékletváltozás okoz, amely kölcsönhatásai jó alapot képeznek az égés okozta hőmérséklet jelzésére. Persze megfelelő jelfeldolgozás és érzékelési eljárás szükségeltetik, hogy kizárhatók legyenek a munkahelyeken sok helyütt fellehető és rendeltetésszerűen alkalmazott eszközökben végzett felfűtésből vagy égető, pörkölő eljárásokból származó hőhatásoktól való elkülönítése. Ehhez a védendő helyiségtől függően tudni kell elkülöníteni a szabad tűzfejlődés és a szabályozott körülmények mellett magasra szökő hőmérsékleti viszonyokat. Jellemzően ezek más-más hőmérsékleti tartományba tartoznak, melyekhez igazítani kell a tűzjelzés céljából megválasztott érzékelőket. Ennek eredményeként használhatók úgynevezett hőmaximum, illetve hősebesség-érzékelők. Az első csoportban találjuk azon érzékelőket, melyek jellemzője az egy adott hőmérsékleti határ elérését detektáló eszközök, míg utóbbiak a szokványostól eltérő gyors hőmérsékleti felfutásokra utaló termikus változáshoz köthetően azonosítják a tűz megjelenését. [2]

A létesítményekben kitörő tűz termikus folyamatait két ellentétesen ható folyamat eredőjeként egyszerűsíthetjük le. Egyfelöl van magának a tűznek mint hőtermelő folyamatnak az öngerjesztő lezajlása, melynek intenzitása a fizikai és anyagi feltételek kínálta maximum irányába fejlődik. Míg ezzel szemben ható változásként rögzíthetjük a tűz számára

az önfenntartás feltételeit szolgáltató anyagi tényezők csökkenésének folyamatát. Amint az utóbbi, az égés tökéletlen oxidációval járó kémia átalakulásainak dinamikája kezdi el dominálni a termikus változásokat, a tűz hanyatlani kezd. Ennek a szakasznak az elérése azonban már messze túl van azon a határon, amely az élet- és vagyonvédelem reális célkitűzéseihez kapcsolódnak. Az ehhez tartozó határmezsgyét egy a zártéri tűzfejlődés kitüntetett fázisához a teljes lángbaboruláshoz köthetjük, melynek kritikus jellegét a termikus változások szinte ugrásszerű növekedése adja. Ezért a tűz megjelenését még - az ezt termikus szempontból jóval megelőző - a kifejlődés korai szakaszában kell detektálnunk. Az ekkor végbemenő hőtani változások jellegzetességeit kell tudnia egyértelműen beazonosítania a tűzjelzőkben alkalmazott érzékelőknek, amennyiben az egyéb, például füst, stb., valamely oknál fogva nem állnak rendelkezésünkre. [3]

Szerencsére a tűz a szabályozatlan jellegéből eredően az általa kiváltott termikus jelenségek alapján jól elkülöníthetők más hőmérsékleti változásoktól. Az ezt biztosító paraméterek egyike az idő. Vagyis egyfelől az időegység alatt keletkezett hőenergia felszabadulásával jellemezhető. Ezt más néven hősebességként definiáljuk. Természetesen az is egy járható út az érzékelésben, ha egy olyan hőmérsékleti értékre kalibráljuk a termikus változásokat nyomon követő detektorunkat, amely mással össze nem téveszthető módon jelzi a tűz jelenlétét a védett térben. Ezt detektálják az úgynevezett hőmaximum érzékelők. [4]



1. ábra: Hőmérséklet-érzékelők csoportosítása
Forrás: Szerkesztette a szerző

Az alkalmazási elveket érintő megfontolások

A tűz valamennyi érintett tűzhelyszín környezeti jellemzőiben változást eredményez. Az érzékelés elve ezen változásokhoz igazodva valósítható meg. Az érzékelő alkalmazhatóságát alapvetően befolyásolja, hogy milyen technológiai környezetben kívánják azt alkalmazni. A hőmérséklet-érzékelők az anyag és a hőmérsékletváltozás közti kapcsolatok sokrétűségére támaszkodva, több alkalmazott műszaki megfontolás tekintetben is kielégítik ezen technikai feltételeket. Megfelelő karakterisztikák beépítésével és a telepítési szempontok figyelembe vételével sikeresen alkalmazhatók a tűzérzékelésére. A tüzek fellobbanását kísérő hirtelen hőhatás termikus jelenségének elektronikai egységek általi közvetlen felismerését, a termoelektromos jelenségek önmagukban is lehetővé teszik. Például a félvezetők egyes képviselőit a villamos vezetőképesség határozott változása különösen alkalmassá teszik erre.

A beépített tűzjelzőkben használt hőérzékelők tűz következtében előálló hőmérsékletnövekedés hatására lépnek működésbe. Azon terekben, ahol az érzékelő határértékeként bekalibrált hőmérsékleti érték az ott felléphető rendellenes termikus jelenségektől egyértelmű elhatárolását adhatja a tűz megjelenésének, ott telepítendők a hőmaximum érzékelők. Ezek olyan esetek lehetnek, mint például az tüzelőberendezés szabályozott körülményeket biztosító tűzteréből kiszabadulva elharapódzó tűz vagy a gyújtóforrásként számba vehető elektromos fűtőberendezések túlhevülése. Ebből eredően a gyakorlatban az irodai funkciót betöltő épületek tűzjelző rendszereinek érzékelői sorában a többségében kiosztott füstérzékelőkkel szemben hőérzékelőket tervezünk be a melegítő konyháknál.

Más esetekben azonban, amire a levegő az általában vett hőmérsékleti határértékre felmelegszik, már gyakorta egy meglehetősen kiterjedt tűzhelyszínnel szembesülhetünk. Ilyenkor jó szolgálatot teketnek a tűz hatékony detektálásában a hősebesség-érzékelők, amelyek már akkor jelzést adnak, ha a tűzfejlődés miatti gyors hőmérsékletnövekedés egyértelműsíti a tűz jelenlétét. Ez azért lényeges, mert a tűzjelző rendszer által felügyelt tér levegőjének hőmérséklete ettől függetlenül nem biztos, hogy eléri az általában vett detektálandó hőmaximumot. Ilyenkor a tűz beazonosítása eredményesebben hajtható végre, mint az egy adott határértékre kalibrált hőérzékelőknél.

A tűz keltette hőmérséklet ilyenformán való érzékelésének alkalmazása olyan technológiai területeken is előnyös, ahol használata kiküszöböli az alacsony hőmérsékletre temperált vagy esetenként jelentős léptékben lehűlni képes légtér helyiségeit kell felügyelni az épületekben. Így ugyanis a maximum paraméterként mutatkozható hőmérséklet elérése a hideg környezet hővelvonása miatt jócskán késleltetett lehet.

Viszont sikeresen illeszthető olyan beépített tűzjelző rendszerekbe, amikor füstjelzők alkalmazása nem célravezető például ott, ahol az intenzív légcsere miatt a füst részecskéinek érzékelési zónából történő elsodródása a tűz időbeni észlelésének elmulasztásával járhat. Segítségével kizárhatók az olyan esetek is, amikor füstfejlődés nélküli égési jelenségektől kísért termikus folyamatok vetítik előre a tűz kitörését. Egyes az éghető anyaghalmok belsejében lappangó és lassan fejlődő tűzeknél hasonló a helyzet, mivel a füstérzékelők ilyen ömlesztett, például öngyulladásra hajlamos anyagok technológiai anyagmozgatási műveletei keltette por a füstérzékelőket hasznavehetetlenné tenné ezekben a környezeti feltételek közepette.

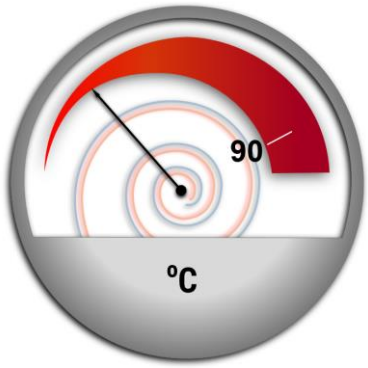
Magától értetődően az alkalmazott érzékelők zónákban történő kiosztásának menynyisége a várható tűzhelyszínkét tekintendő helyiség fizikai dimenzióinak és az adott eszközre vonatkoztatott védősugara vagy sávjának arányai alapján kerül megállapításra. ezeket a tervezői szabványok vagy gyártói útmutatók is rögzítik. Egyuttal a védett helyiségekben fontos tekintettel lenni valamennyi az érzékelés korlátozó tényezőre az érzékelők elhelyezésének megválasztásakor. [5]

HŐMÉRSÉKLET-ÉRZÉKELŐK

Hőmaximum-érzékelők

A tűz automatikus detektálására a hőmérsékletmérés már régóta használt eljárás. Ahhoz azonban, hogy a normál üzemviteli és egyéb munkakörnyezeti hőhatásoktól el tudjuk különíteni a tűz jelentette változást, egy karakteres egyedül a tűz okozta állapot beazonosítására használható érzékelési eljárást kell kiválasztani. Ahogyan azt előzőleg már vázoltam ezek közül több lehetőség is kínálkozik. A legkézenfekvőbb, valamely környezeti

határállapot kitűzése, mégpedig egy meghatározott, a tűzkeletkezést összetéveszthetetlenül mutató hőmérsékleti maximum elérése révén, melynek vázlata látható a 2. ábrán.



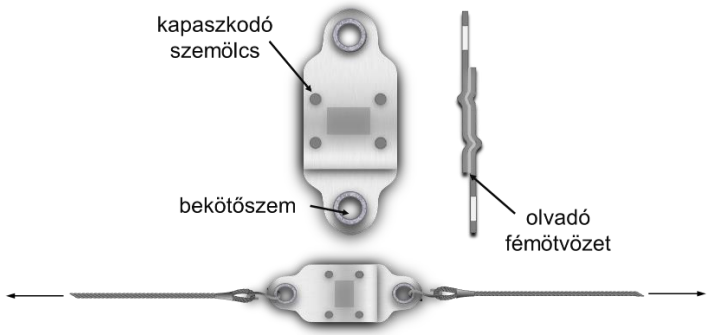
2. ábra: Ikerfémes hőmérséklet-érzékelő vázlata
Forrás: Szerkesztette a szerző

Az ilyen adott hőfok elérésére kalibrált érzékelők a karakterisztikájában megjelölt hőmérséklethez tartozó fizikai változók eléréskor a mért paramétert közvetve, de akár közvetlenül is villamos jellé átalakítva detektálják a tűz megjelenését a védett térben. A fizikai változók alapján a jelzés kiváltása szerinti kategóriái lehetnek:

- térfogati,
- mechanikai,
- pneumatikai,
- tenziometriai,
- elektrooptikai,
- termoelektromos, stb. [6]

Olvadóbetétes érzékelő

A hagyományos érzékelő típusok közül működési elvét tekintve az egyik legegyszerűbb eszköz az olvadóbetétes tűzjelző. A tűzjelzőt egy viszonylag alacsony, de konkrét olvadáspontú forraszanyaggal fixen egymáshoz rögzített két fémlap adja, ezt láthatjuk a 3-as ábrán.



3. ábra: Olvadófémes érzékelő és bekötésének módja
Forrás: Szerkesztette [7] nyomán a szerző

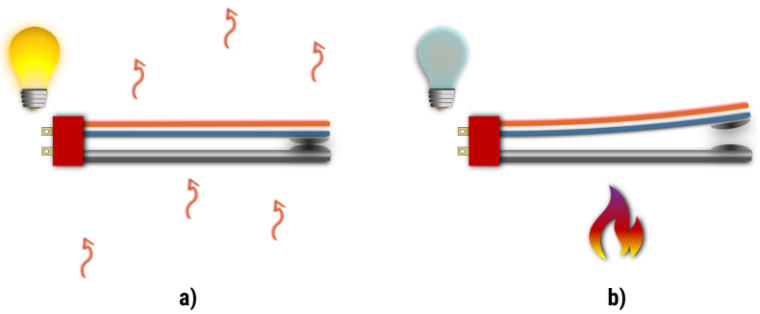
A jelzés kiváltása a rajtuk kialakított bekötőszemekhez mechanikusan kapcsolódó előfeszítések miatti, adott az ún. Wood-fém olvadáspontjának megfelelő hőmérsékleten történő szétválásukkal realizálódik. A tűz keltette hő következtében a tapadási erő megszűnik a forrasztás által összetartott két egymásba kapaszkodó lemez között. Ilyenformán a fémötvözet megolvadása miatt az előfeszített mechanikai rendszerben elhelyezkedő olvadóbetétes csatlakozás elveszti a szilárdságát és a jellemzően rugóerővel vagy ellensúllyal ellentartott szerkezeti elemek elmozdulása váltja ki a jelzést.

Azonban a hőmérséklet-csökkenést követően ezt az olvadófémes betétet cserélni kell, mivel a rendszer, csak így állítható vissza alaphelyzetbe. A más-más hőmérsékleti tartományokban működtetendő eszköznek a változó hőmérsékletekhez igazítása az ötvözet olvadáspontjának kalibrálásával oldható meg. A Wood-fém eltérő összetétele ezt az értéket is módosítja. Az ötvözetben megtalálható ón, ólom, és bizmut alkotta fémelegy ötvözési arányainak változtatásával az eszköz a kívánt hőmérsékleti határértékre beállítható.

Bimetallos hőérzékelők

Az ezt a műszaki megoldást felhasználó eszközök a beépített tűzjelző rendszerekben mára már nem alkalmazott, azonban egyes speciális területeken, például vasúti mozdonyok vagy egyéb belsőégésű berendezések motortereiben előfordulnak. Olyan helyeken alkalmazandó, leginkább, ahol a maximált hőmérsékleti értéken való jelzéskiváltás egyszerű, nagy megbízhatóságú technikai kivitelű formája elsőrendű követelmény a tűzkeletkezés gyors megelőzése érdekében. Tulajdonképpen a gépjárművek termosztátjai is hasonló elven működnek.

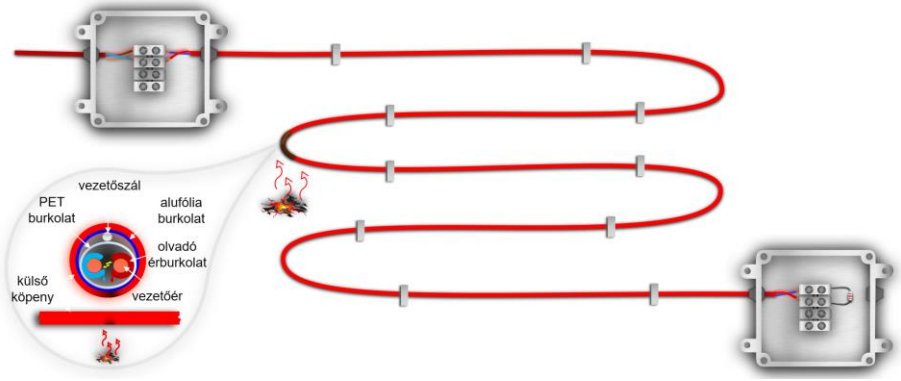
Működési elve is ehhez mérten rendkívül egyszerű, ahogyan az a 4-es ábrán szereplőkből is leszűrhető. Egy meghatározott hőmérséklet elérése esetén a fizikailag egymáshoz rögzített kettős fém eltérő hőtágulása elhajlást eredményező deformáció szenved el. A tűz veszélyével nem járó hőmérsékleti tartományokban ez nem jelentkezik, így a bimetálos kapcsoló zárva tartja az áramkört. A tűzkeletkezést kiváltani képes hőhatás eltérő hőtágulást keletkeztet a két fémben. Mivel a nagyobb hőtágulási együtthatóval rendelkező fém a fix rögzítés miatt nem képes hosszirányú megnyúlással felvenni a tágulással megnövekvő méretet, ezért a hozzá rögzített fémet meggörbítve próbálja felveszi a szükséges méretváltozást. Ekkor az ikerfémek szilárd mechanikus kapcsolatának köszönhető alakváltozás megszakítja az áramkört jelezve ezzel a kalibrációval megjelölt veszélyes hőmérsékleti érték elérését. Természetesen az áramköri csatlakoztatás kérdése az itt bemutatottól eltérően az adott műszaki kialakítás viszonylatában egyedi kivitelezésű is lehet. [8]



4. ábra: Bimetál hőmérsékleti határértékre kalibrált hőmaximum-érzékelő működési sémája normál környezeti hőmérsékleten (a) és tűzjelzéskor (b)
Forrás: Szerkesztette [9] nyomán a szerző

Olvadó szigetelésű érzékelőkábelek

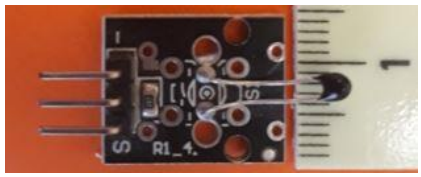
Jól ismert, hogy a kábelek szigetelésének tűzhatásra bekövetkező károsodása a villamos vezetékhálózatokban alkalmazott érpárok fémes érintkezését idézheti elő. Ez a vezetők közötti az 5-ös ábrán illusztrált módon zárlatot idéz elő, amely az áramköri paraméterek mérésével azonosítható. Ezt hasznosítják az olvadó szigetelésű vonali tűzérzékelőkben. A tűz miatt megsérült vezetékben az érpár között kialakuló zárlat bekövetkezését használják fel erre a célra. A szigetelésként szolgáló polimerek olvadáspontját kémiailag a várható tűzhatás adott hőmérsékletéhez igazítva létre hozható egy konkrét hőmérsékleten riasztást indítani képes hőmaximum érzékelő kábel. Az vonali hőérzékelő kábelt nem csak létesítményekben, de más nehezen hozzáférhető helyeken is lefektethetik a rejtett tüzek keletkezése veszélyének kivédésére, mint például szállítószalagok görgősorai közötti takart tereinél, stb.



5. ábra: Olvadó szigetelésű hőérzékelő kábel
Forrás: Szerkesztette [10] nyomán a szerző

Termisztoros pontérzékelő

A termisztorok olyan félvezető technológián alapuló elektronikai eszközök, melyekben a hőmérséklet változását markáns ellenállásváltozással lekövető érzékelőket alkalmaznak. Ezen változások karakterisztikája két irányú lehet. Lehetnek negatív (angol rövidítésük: NTC) és pozitív (angol rövidítésük: PTC) ellenállásváltozást mutatók. Maga a félvezető termisztor igen kicsi, ez jól kivehető a 6-os ábrán leolvasható méretekből is. Ez is közrejátszik nagy érzékenységükben. Mivel így elhanyagolható léptékű a termikus tehetetlenségük, ezért szinte azonnal felveszik a környezetükben uralkodó hőmérsékleti értékeket. Sokhelyütt találkozhatunk ezzel az hőérzékelővel, mint egy küszöbérték detektálására kalibrált érzékelővel. [11]

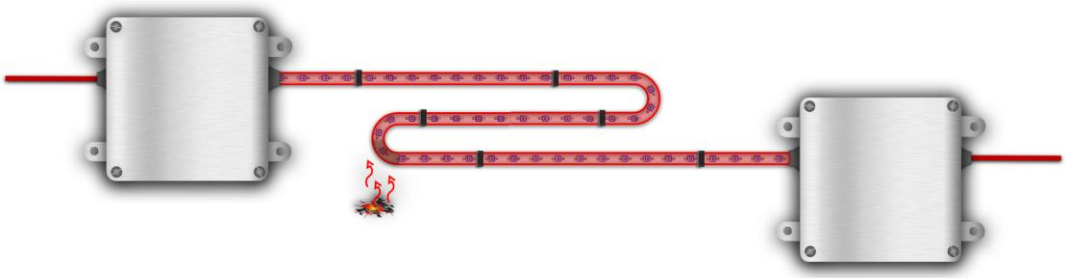


6. ábra: Termisztor áramköri felépítésének mérettartománya
Forrás: Készítette a szerző

Emellett hősebesség mérésre is alkalmas. A gyakorlatban ezt két termisztor ellenállásváltozása egyidejű logikai áramköri összehasonlításával oldják meg. A hősebesség mérésnél az eltérések a két érzékelő környezeti hőmérsékleti hatásoknak való kitettségéből ered. Az egyik termisztor a környezetével közvetlen termikus kölcsönhatásban van és ezért folyamatosan lekövetheti az ott bekövetkező hőmérsékleti változásokat. A másik termisztort azonban hőszigetelő anyaggal elkülönítik a felügyelt helyiségben lezajló közvetlen hőhatásoktól. Ez jól kimérhető ellenálláskülönbséget vált ki a két termisztorban.

A védett térben a lassan változó hőmérsékletek esetében ez az ellenálláskülönbség meghatározott tartományon belül fog mozogni, melyet megfelelő elektronika beillesztésével kiegyenlítenek. Technikailag ezt egy szabályozó ellenállások közbeiktatásával kompenzáló áramköri elem biztosítja. Ellenben a nagyobb termikus tehetetlensége következtében a tűzhatás okozta hirtelen hőmérsékleti ugrást már a környezetétől elszigetelt termisztor nem tudja adott, a normál viszonyok közötti kisebb léptékű eltéréssel lekövetni. Ehhez képest az azt jóval meghaladó különbségérték lép fel az ellenállás változásában, melynek hatására az áramköri kiegyenlítés felborulása miatt az eszköz tűzjelzést ad a tűzjelző központ felé.

A pontérzékelők és a vonali érzékelők közötti egyfajta átmenetet képeznek a multi szenzoros érzékelő kábelek, amelyekben a 7-es ábrán bemutatott módon szabályos távolságokra félvezető detektorokat fűznek fel. Az így a megfelelő sűrűséggel egymást követően a védett szakaszban elhelyezkedő szenzorok láncolatában a hőhatásra kiváltott jel adott termisztorhoz köthetően kellő precizitással beazonosítható a tűz keletkezésének helyeként. [12]

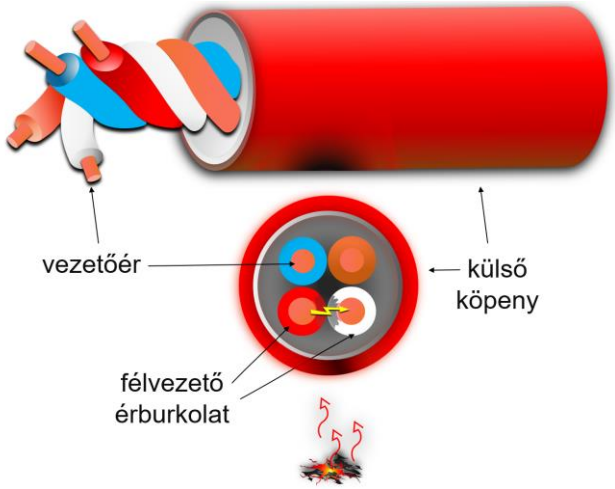


7. ábra: Multiszenzoros érzékelőkábel alkalmazásának elvi vázlata
Forrás: Szerkesztette a szerző

Termisztoros vonali tűzjelzőkábel

A félvezető termisztorok tűzjelzésre történő felhasználásának széles spektrumát mutatja, hogy vonali tűzjelző kábelekként is kivitelezhető a tűzjelző rendszerrel felügyelt terek védelme. Ez esetben a tűzjelző kábelben futó érpárok szigetelő anyagául használják fel a termisztorokban is alkalmazott félvezető anyagokat. A jellemzően jelentősebb hosszirányú kiterjedésű védett térben vagy gép, berendezés, illetőleg raktári tárolórendszer, stb. tűzkeletkezés szempontjából kritikus szakaszain végig vezetve a tűzjelző kábelt, megbízhatóan lefedhető a teljes védendő szakasz.

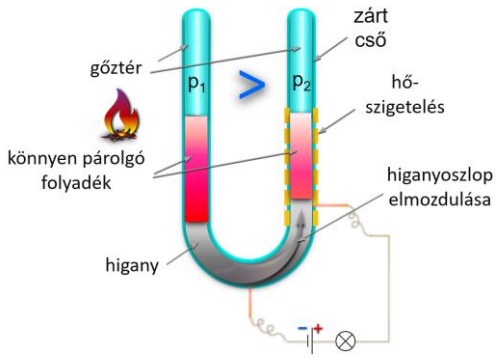
A tűzjelzés kiváltása a 8-as ábrán illusztrált módon zajlik. A tűz hatására az érzékelő kábel érintett pontján a vezetőért érő hő következtében az azokat körülölelő érburkolatok, mint termisztorok, elektromos vezetővé válnak. A termisztorszigetelésű érpárok közötti szigetelőhatás megszűnése miatt a tűzjelző rendszer a kábelben ébredő zárlati áramot tűzjelzésként detektálja. A két-két érpár fennmaradó párosa a hibaellenőrzés funkcióját tölti be.



8. ábra: Jelzéskiváltás keresztmetszeti sémája termisztoros szigetelésű tűzjelző kábelben
Forrás: Szerkesztette [13] nyomán a szerző

Folyadékok felhasználása a tűzérzékelésben

Az elektronikus tűzjelző rendszerek mellett találkozhatunk az elektronikától függetlenül működő hidromechanikus megoldásokkal is. Ez a lehetőség egy műszakilag kézenfekvő választás, hiszen magának a hőmérséklet mérésnek az históriájához is elválaszthattalanul hozzá tartozó elvet, a folyadékok hőtágulását hasznosítja. A korai hőmérőkből is ismert üvegkapillárisban a hőmérséklet emelkedését kísérő térfogatnövekedés a folyékony higany relatív elmozdulását okozza. Az egészségre és környezetre való veszélyessége miatti méréstechnikai alkalmazásának kivezetését megelőzőleg higanyos tűzérzékelőket is használtak hősebesség-érzékelőként. Bár mint az a 9. ábráról kitűnik az eszköz konstrukciós felépítésének alapját adó „U" alakú csőben a folyadék elmozdulását nem annak hőtágulása eredményezi, hanem a higanyoszlopra nehezedő, a tűzben fejlődő hő miatt a fém felett lévő folyadék intenzíven párolgása nyomán megnövekedett belső gőztér nyomása. Ennek következtében elmozduló higanyoszlop az elektródát elérve zárja a jelző áramkört.



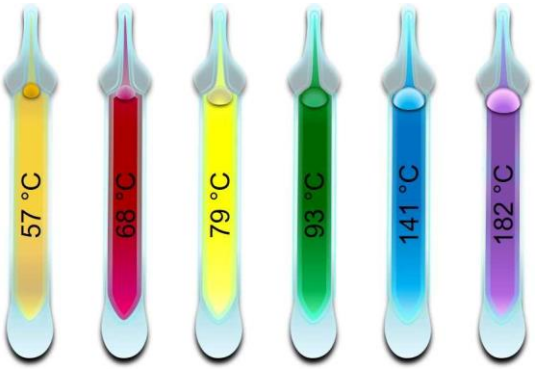
9. ábra: U-csöves hősebesség-érzékelő vázlat
Szerkesztette: [14] nyomán a szerző

A megoldás alapelve, hogy egy a környezettől termikusan elszigetelt szegmense az érzékelőnek termikus tehetetlensége folytán eltérően reagál az egyéb paramétereiben megegyező szerkezeti elemhez képest, más eszközöknél is feltűnik. Nyilván, ha ez egy nem váratlanul ébredő tűzhatás miatt lép fel, hanem lassú, fokozatos hőmérsékleti átmenettel, akkor a cső mindkét végén elhelyezkedő folyadéknak van lehetősége a hőmérsékleti kiegyenlítődésre dinamikus jelenségek kiváltása nélkül. [14]

A folyadékok tűz következtében fokozódó tenziójának kamatoztatása a tűzvédelem másik fontos területén a beépített oltórendszereknél is megjelenik. A beépített tűzoltó berendezések egyik legelterjedtebb típusa az úgynevezett sprinklerek, melyek a tűzeseti hőmérséklet emelkedésének hatására lépnek működésbe és szórófejeiken keresztül oltóvizet juttatnak az égő anyagokra. A sprinkler rendszer alapja egy speciális betét, ami megfelelő hő hatására kiold, így a mögötte lévő vízoszlop szabadon tud távozni a rendszerből, így az oltás megkezdődik. [15]

Az ilyen úgynevezett nedves sprinklerrendszer csőhálózatában jelenlévő oltóvíz szándékolatlan kijutását egy-egy záróelem blokkolja valamennyi sprinklerfejekben. A szórófejeket a már korábban ismertetett woodfémes olvadó betét vagy folyadékkal töltött ampullák zárhatják le. Az utóbbiak esetében a hőmérsékleti határértékekre kalibrálását a bennük lévő folyadék megválasztásával és a bórszilikát törőüvegek, másnéven kvarckörték belső nyomáshoz igazított szilárdsági mutatói adják. [16]

Az adott hőmérsékleten szétpattanó kvarckörték mintegy hőmaximum érzékelőként funkcionálnak. A törőüvegeket színkódolásukhoz rendelt névleges nyitási hőmérsékleteik szerinti sorrendjében a 10. ábra mutatja.



10. ábra: Törőüvegek szinkódolása nyitási hőmérsékleteik alapján
Szerkesztette: [17] nyomán a szerző

A kvarckörtéket a bennük lévő folyadékhoz adott színezékektől kölcsönzött különböző színkódok segítenek azonosítani. Azonban a hőmérsékleti besorolásukat alapvetően a folyadék kémiai összetétele határozza meg. Másfelől a törőüvegekben eltérő méretű légbuborékok is megfigyelhetők. A légbuborék mérete ugyancsak befolyásolja a hőmérsékletérzékenységet, mivel ezek veszik fel a tűz hatására elpárolgó folyadékok gőzeit, így fokozva a folyadékra ható nyomást. Mígnem a zárt ampullák belsejében a nyomásérték eléri az üveg szilárdsági tényezője biztosította kritikus értéket. Az alacsony forráspontú folyadékkal töltött üvegampulla elpattan és a víz útját szabaddá teszi.

A törőüvegekben a folyadékok anyagi minőség szerinti kiválasztásának szempontjait képezi elsődlegesen forráspontjuk, valamint a záróelem környezetében várható hőmér-

sékletek tűzhatástól való elkülönülését garantáló viszonyokhoz rendelhető hőmérsékleti értékek. Az ezektől függően elvárt különböző névleges nyitási hőmérsékletek beállításához az 1. táblázatban szereplő vegyületek akár egyedileg vagy folyadékelegyeik formájában is használhatók. Fontos azonban, hogy egyfelöl tenziójuk és hőtágulásuk elegendően nagy legyen az adott üvegburkolat repesztési nyomásának eléréséhez az elműködési hőmérsékletként megkívánt határértéken. [18]

Anyag	fp °C	*Relatív válaszidő (víz= 100)*	*C • D = C' (J/ml)*	*Viszkozitás (mPa • s)*	*Hővezetési tényező (W/cm • K)*	*dP/dT (számított) (bar/K)*
izopropanol	*82*	*114*				
víz	***100***	***100***				
KCI oldal (35,5 %)		*86*				
etanol	*80*	*75*	*1.921*	*1.20*	*0.0289*	*9.1*
metanol	*64*	*88*	*1.988*	*0.60*	*0.0352*	*9.08*
glicerin	*290*	*97*	*2.955*	*830*	*0.0498*	*15.26*
etil-acetát	*76*	*65*				*12.0*
toluol	*110*	*59*	*1.473*	*0.59*	*0.0239*	*11.32*
n-dekán	*173*	*66*				
ciklohexán	*80,1*	*63*			0,12*	*9.30*
triklór-etilén	*86*	*62*	*1.344*			
tetraklór- etilén	*120*	*62*	*1.423*		0,11*	
etil-acetoacetát	*69*	*62*				
aceton	*56*	*60*	*1.674*	*0.31*	0,16*	*10.47*

C • D = C' - Hőkapacitás és sűrűség szorzata = térfogatfüggő hőkapacitás

** [19] alapján vett érték*

1. táblázat: Néhány törőüvegeinél alkalmazható folyadék hőtani jellemzői
Forrás: Szerkesztette [18], [19] nyomán a szerző

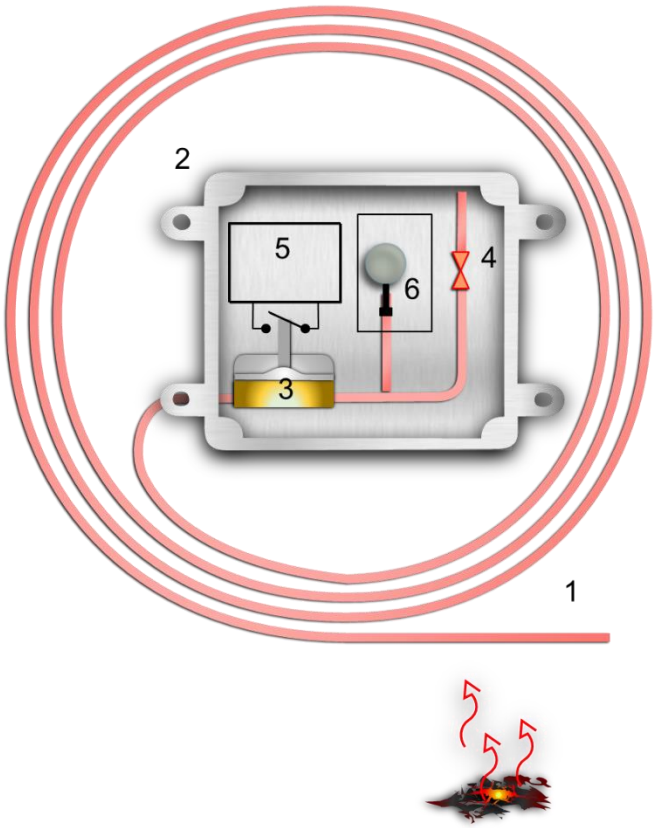
Hősebesség elvén alapuló érzékelők

A hősebesség-érzékelők korszerű változatai a mért jel karakterisztikájának hirtelen növekedéseként detektálják a tűz jelenlétét. Amennyiben a hőmérséklet emelkedésének mértéke túlhalad egy bizonyos hőfoknövekedési értéket egy megfelelő hosszúságú időintervallumon belül, a jelfeldolgozó logikai áramkör tűzjelzést ad ki a tűzjelző központ felé. Ezen érzékelők modern megoldásai NTC/PTC félvezető detektorok ellenállásának jelgörbéi alapján „kapcsolják össze" a meghatározott hősebesség értéket a tűz jelenlétével. A gyakorlatban ez az időegység alatti hőmérséklet növekedési érték néhány fok/perc nagyságrendben mozog. [20]

Hősebesség-érzékelők megoldást jelenthetnek minden létesítményben, amelyekben széles hőmérséklet tartományt átfogó termikus hatások várhatók, azonban az ezek során lezajló változások üteme mérsékelt.

Nyomásváltozás felhasználása hősebesség-érzékelésnél

A tűz hatását kísérő termikus jelenségek sorában nem elhanyagolható fontos a környezeti állapotjelzők változásai között a gázok térfogatváltozása. Ez ugyancsak felhasználható érzékelési lehetőségként. A megoldás már jól ismert, hiszen rugalmas elmozdulásra képes zárt spirális csövekbe töltött gázok kiterjedésével és az elmozdulás hőmérsékleti értékekhez kalibrálásával. Ez egyszerűen kivitelezhető vizuális leolvasásra is igénybe vehető, például a hagyományos technológiai berendezések kezelőinek szánt érzékelőknél. Azonban az alapelv vonali hősebesség-érzékelőknél is felhasználható kis átmérőjű réz vagy acél csöves formában, akár hengerpalást mentés spirálban kihúzva, mint azt a 11. ábra illusztrálja.



11. ábra: Pneumatikus hősebesség-érzékelő működési vázlata
1 – érzékelő rézcső, 2 – érzékelő háza, 3 – membrán-kontaktus, 4 – kompenzáló kapilláris,
5 – ellenőrző elektronika, 6 – öntesztelő
Szerkesztette: [21] nyomán a szerző

A riasztás indítása a vékony csőrendszerben elhelyezkedő gáz kitágulása nyomán történik. A szándékolt jelzéskiváltáshoz vezető tűz és a felügyelt környezetben bekövetkezhető természetes hőmérsékletváltozások elkülöníthetőségét a kompenzáló kapilláris teszi lehetővé Bernoulli-törvényét követve. Ugyanis a lassú nyomásnövekedés a szűkítés egyik, illetve másik oldalán nagyon csekély áramlási sebesség mellett egyenlítődik ki, így számottevő jelzést keletkeztető nyomáskülönbség nem jelentkezik. Ellenben a tűz esetén a felügyelt térben elhelyezkedő csőszakaszban a megemelkedő hőmérséklet gyorsan növeli meg

a gáztérfogatot, így az viszonylag gyors áramlással kényszeríti át a kiterjedő gázt a kapillárison, ami a kapilláris jóval szűkebb keresztmetszetén a pneumatika törvényeit követve felgyorsulva igyekszik áthaladni. Az e két áramlási sebesség miatt nyomásnövekedés adódik a rendszerben, ami egy rugalmas membránon keresztül képes akár mechanikusan működő jelkiváltó kapcsolók működtetésére is.

KÖVETKEZTETÉSEK

A beépített tűzjelző rendszer és a felügyelt terek közötti állandó kapcsolat fenntartásáért az érzékelők „felelősek". Funkciója alapjában véve egyszerű adatok tárolása, azok ellenőrzése, a beérkezett jelek értelmezése és feldolgozása és a gépben lévő program szerinti beavatkozás. Egy ilyen eszköznek megbízhatónak kell lennie és a környezeti hatásokkal szinergiában kell működnie, mert a tűzbiztonság elvárt szintje csak így valósulhat meg.

Éppen ezért a termikus jelenségeken alapuló tűzérzékelők a műszaki-technikai fejlődés valamennyi korszerű megoldását tudnia kell adaptálnia a félvezetőelekrtonikától a legkülönfélébb elektromechanikus és pneumatikus érzékelőkig bezárólag. Ezek az akár szélsőséges műszaki kihívást jelentő technológiai feltételekhez és épületfizikai viszonyokhoz igazodva is komplex megoldást kínálnak a szakavatott tervező arzenáljában a tűzvédelmi koncepció megvalósításához. A kockázatelemzéssel feltárt tűzveszély elhárítására készített aktív tűzvédelmi műszaki megoldásaink az érzékelők nem kellően precíz megválasztása már kiinduló fázisában megingathatja a tűzbiztonság megteremtését célzó valamennyi preventív intézkedésünk sikerét.

Ebből adódóan az alkalmazott beépített tűzjelző berendezéseink érzékelőinek rendszerbe integrálása alkalmával különös gonddal kell eljárni. Mivel azok hőmérsékletérzékelő elemeinek kifogástalan műszaki állapot mellett is csak a tűz termikus változásainak késedelem nélküli és megbízható lekövetésével tudják megteremteni a feltételeket az aktív és passzív tűzvédelem valamennyi eltervezett funkciójának megvalósulásához.

HIVATKOZÁSOK

[1] Robert Burke: *Fire Protection Systems and Response,* 2008., ISBN: 978-1-56670-622-3, 77. o.;

[2] Beda L., *Épületek tűzbiztonságának műszaki értékelése*, ZMNE Doktori (PhD) értekezés, 2004.

[3] Beda L.: *Tűzmodellezés és tűzkockázat elemzés*, Ybl Miklós egyetemi jegyzet, 6. o. 1999.;

[4] Csepregi Cs., *Tűzjelző rendszerek*, Florian Press Kiadó Budapest 2001.;

[5] TvMI 5.4:2024.02.01. *Beépített tűzjelző berendezés tervezése, telepítése*;

[6] Антонов А.В., Голякова Е.И., Сацук И.В., Филкова А.П., *Краткий Курс Лекций по Дисциплине - Производственная и Пожарная Автоматика*, Сибирская Пожарно-Спасательная Академия, Гпс МЧС России, Железногорск, 2022., ISBN 978-5-906874-96-2, 14. o.;

[7] MSZ 15602-82 *Hőhatásra szétváló kapocs*, Szabványgyűjtemények 47, Tűzvédelem II., Magyar Szabványügyi Hivatal, Budapest, 1987., ISBN 963 402 412 2 II. kötet, 565. o.;

[8] Kemencés J. *Nyomástartó berendezések biztonságtechnikája*, OMKT, Budapest, 2010., ISBN 978-963-89258-0-2, 71. o.;
[9] Marston R., *Security Electronics Systems and Circuits — Part 1*, Nuts & Volts Magazine (February 1998), https://www.nutsvolts.com/magazine/article/security-electronics-systems-and-circuits-part-1, (letöltve: 2024. 02. 10.);
[10] Duran Electronica, *Installation & User Manual, Linear Heat Detection Cable*, 2017., https://www.duranelectronica.com/english/wp-content/uploads/2017/07/I-manSAFE-CABLE-v04.pdf, (letöltve: 2024. 01. 23.);
[11] Bellus L., *A tűzjelzés fizikája II.*, Védelem – katasztrófa- és tűzvédelmi szemle, ISSN: 1218-2958, 2002, 9. évf. (5), 49 o.;
[12] Mohai Á., *SecuriSens TSC 511 hőérzékelő kábel II.*, Védelem – katasztrófa- és tűzvédelmi szemle, ISSN: 1218-2958, 2002, 9. évf. (6), 21 o.;
[13] Kovács I., *Óravázlatok Beépített tűzvédelmi berendezések című tárgyhoz*, Budapest, 1995., 13. o.;
[14] Arany S., Fetser I., *A hő és füstelvezetés elmélete és gyakorlata a tűzmegelőzésben*, Budapest, 1991., ISBN 963-593-114-x, 116. o.;
[15] Berek L., *Biztonságtechnika*, Egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014., 45. o.;
[16] Huet R, et al: *Delayed Fracture of Glass Bulbs Used in Fire Sprinklers*, Fire Technology, 53, 629–647, 2017, DOI: 10.1007/s10694-016-0584-4;
[17] Hegel Engineering, *Fire Sprinkler System*, https://www.hegelengineering.com/single-post/fire-sprinkler-system, (letöltve: 2024. 02. 10.);
[18] United States Patent Office: 4,938,294 *Trigger Element for a Sprinkler*, Johann G. Mohler, Petr Bohac, Jul. 3, 1990, Appl. No.: 275,173, Online: https://patents.google.com/patent/US4938294A/en;
[19] European Patent Office: Patent EP 0838242 A2 *Thermally responsive frangible bulb*, Pepi, Jerome Stefansson, Nettleship, Stephen James, Daly, Brian Ernest, May. 6, 2002, Appl. No.: 97307891.8, Online: https://patents.google.com/patent/EP0838242B1/en;
[20] Laczik D., *Hamis tűzjelzés kiszűrésének elvi és gyakorlati lehetősége a tűzvédelemben*, Hadmérnök, ISSN: 1788-1929, 2012., VII. évf. (1), 15-31 o., http://hadmernok.hu/2012_1_laczik.pdf, (letöltve: 2024. 02. 11.);
[21] Balázs G., *Különleges érzékelők*, Védelem – katasztrófa- és tűzvédelmi szemle, ISSN: 1218-2958, 1995, 2 évf. (4), 31. o.;

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