American Journal of Research, Education and Development

RED

ISSN 2471-9986

American Journal of Research, Education and Development

IMPRESSUM

American Journal of Research, Education and Development
ISSN: 2471-9986

Publisher: DEVLART LLC
250 Camelback Ridge Ave. Henderson, NV 89012
red@devlart.hu

Table of Contents

Options for the implementation of land-based wildfire prevention in Hungary

Author: Péter Debreceni, National Food Chain Safety Office, DebreceniP@nebih.gov.hu, ORCID: 0000-0002-1886-9076

Abstract

Wildfire statistics from the last decade show that the temporal and spatial patterns of wildfires have changed in Europe. Some large forest fires have occurred in the Nordic countries past few years. The fire season starts earlier and the length of the endangered periods increases in the Mediterranean and Central Europe. The European Forest Fire Information System (EFFIS)[1] shows that 95% of forest fires are caused by human negligence or intentional causes.[1] Complex reasons have been identified behind the negative trend. In response to these alarming trends, a priority should be greater attention to land-based fire prevention practices as part of integrated fire management. These practices can translate into more fire-resistant and resilient landscapes and communities that are better equipped to face the expected risks. In this paper, I would like to explore a new approach based on European research that could be the basis for further development of the Hungarian wildfire prevention system.

Keywords: effective forest fire prevention, land-based wildfire prevention, forest fire risk estimation, integrated wildfire management

Corresponding author: Péter Debreceni, National Food Chain Safety Office, DebreceniP@nebih.gov.hu, ORCID: 0000-0002-1886-9076

[1] https://effis.jrc.ec.europa.eu/

Introduction

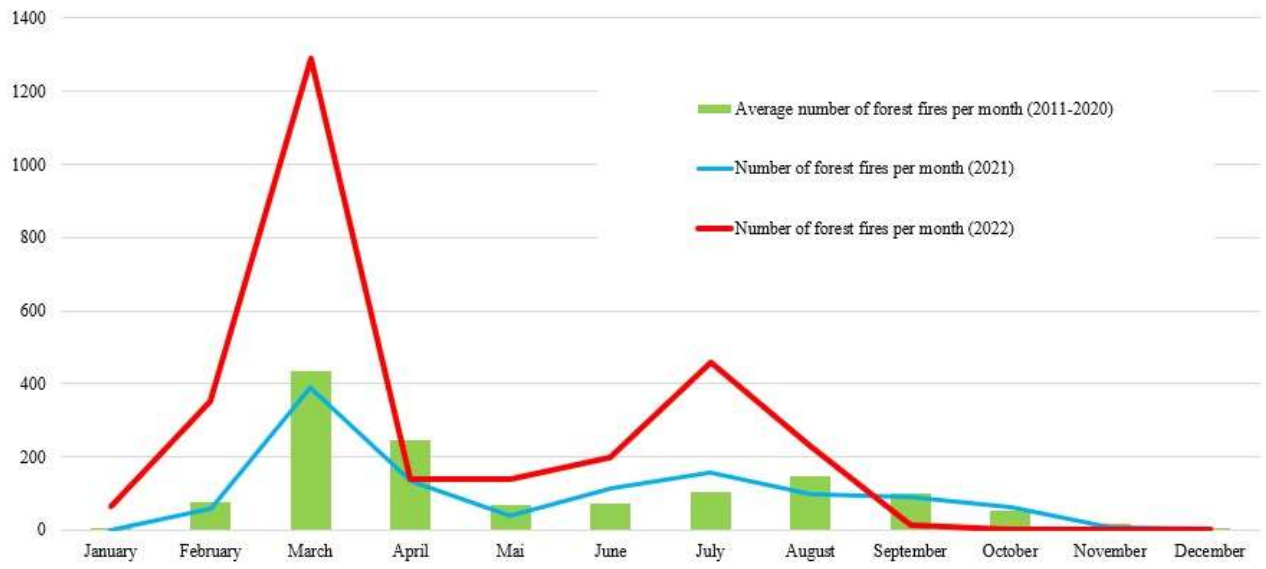
Wildfires are one of the most common natural disasters in the world, damaging hundreds of millions of hectares every year. Natural caused wildfires have been a part of everyday life since prehistoric times and can significantly shape the composition and dynamics of ecosystems, including forest land and cultivated landscapes. Since the beginning of agriculture, the use of fire has contributed human development. Extensive fires have been shaped the landscape, and influenced crop productivity and air quality. Vegetation has been adapted to the frequency and intensity of wildfires in some parts of the world. Other types of them are tolerant or can be sensitive to the effects of wildfires. Wildfires at the wildland-urban interface[2] can also threaten human assets due to population growth and land use expansion. [2]

The effects of climate change are being analyzed by intergovernmental bodies, and foreign and domestic researchers. [3] The results predict that within a few decades, the Carpathian Basin will experience a more uneven distribution of precipitation and an increase in average daily temperatures in summer and autumn. The effects of climate change will be reflected in longer fire danger periods and an increase in the number of wildfires. The spatial and temporal distribution of wildfires will change and fire intensity is expected to increase. Therefore, the organizations responsible for preventing and extinguishing wildfires are going to be faced an even greater challenge in the future. [4] [5] The impacts of climate change also cause problems for nature conservation and environmental security. These problems affect all actors in society. [6] Because of the mosaic landscape structure in Hungary, wildfires affect not only forest land, but also other wooded and agricultural land. Therefore wildfire management requires integrated cooperation between several disciplines, management bodies, and authorities. Cooperation is regulated by legislation and by agreement between organizations. It is a social and governmental expectation that the bodies responsible for wildfire prevention and fighting against wildfires can work together effectively and respond promptly to emergencies during wildfire risk. The priority of this study is that more than 70,000 wildfires have occurred in the last decade. This will result in an increase in fire-fighting for the fire service. A major challenge for the authorities responsible for wildfire prevention is to revise the fire prevention strategy, taking into account European trends and new scientific results.

[2] Wildland-Urban interface: WUI areas can be defined as landscapes where anthropogenic urban land use and forest fuel mass come into contact.

Wildfire season features

Based on the temporal distribution of forest fires, there are two distinct high-endangered periods in Hungary each year. Spring fires occur between mid-February and the end of April, depending on rainfall. Spring fires accounted for 56.3% of all fires in the last 10 years. In the last decade, only in spring 2013 has there been enough rainfall to miss the spring fire season, with only a few small fires recorded. In six springs between 2011 and 2021, the proportion of fires was above 50% of the annual fire events. At the beginning of last decade, the wildfire season started in late February, depending on spring precipitation. This trend seems to have changed in the last three years. Mainly due to the extreme lack of rainfall, the number of wildfires started to increase from the second week of February, and high fire rates were recorded until the end of April. There were 1.5 times more wildfires than the ten-year average in 2022. In May and the first half of June, depending on the distribution of precipitation, the wildfire risk decreases and there are no outliers in fire statistics.



1. Figure: Distribution of forest fires per month (2011-2022) [4]

Based on the number of wildfires, the second high-fire-risk period of the year is between July and September. During summer heat waves, there is a high wildfire risk period. The number of fires during this period is below the number of fires during the spring. The proportion of area burned per fire can be much higher. During the summer drought in the past two years, several large crown fires have occurred in the pine forests of the Great Plain and the wooded, shrubby areas of the northern part of the country. Based on spatial data analysis, I found that the vast majority of forest fires do not

occur in the interior of forest blocks, but in areas adjacent to agricultural land. [7] Most of the spring forest fires occurred in Northern Hungary and Northern Great Plain region. Geospatial analysis of the spatial distribution of forest fires shows that 58% of the fires occurred in the 500 m zone around residential areas. 89% of all forest fires occured no more than 2 km from residential areas. [8]

I compared the spatial location of fire outbreak points with the Corine Land Cover Database[3] in geospatial analysis. The results of the spatial analysis are shown in Table 1. The values in the table show that the vast majority of wildfires occur in residential areas or some kind of agricultural land. Only 16% of fires occur directly in forests and shrubland. Wildfires are caused by a lack of knowledge of fire safety rules and negligence near inhabited areas. In agricultural areas, fires are caused by the burning of grass associated with traditional land use or the burning of stubble during the harvest.

1. Table: Distribution of the number of wildfires in the Corine land cover categories [4] (created by the author)

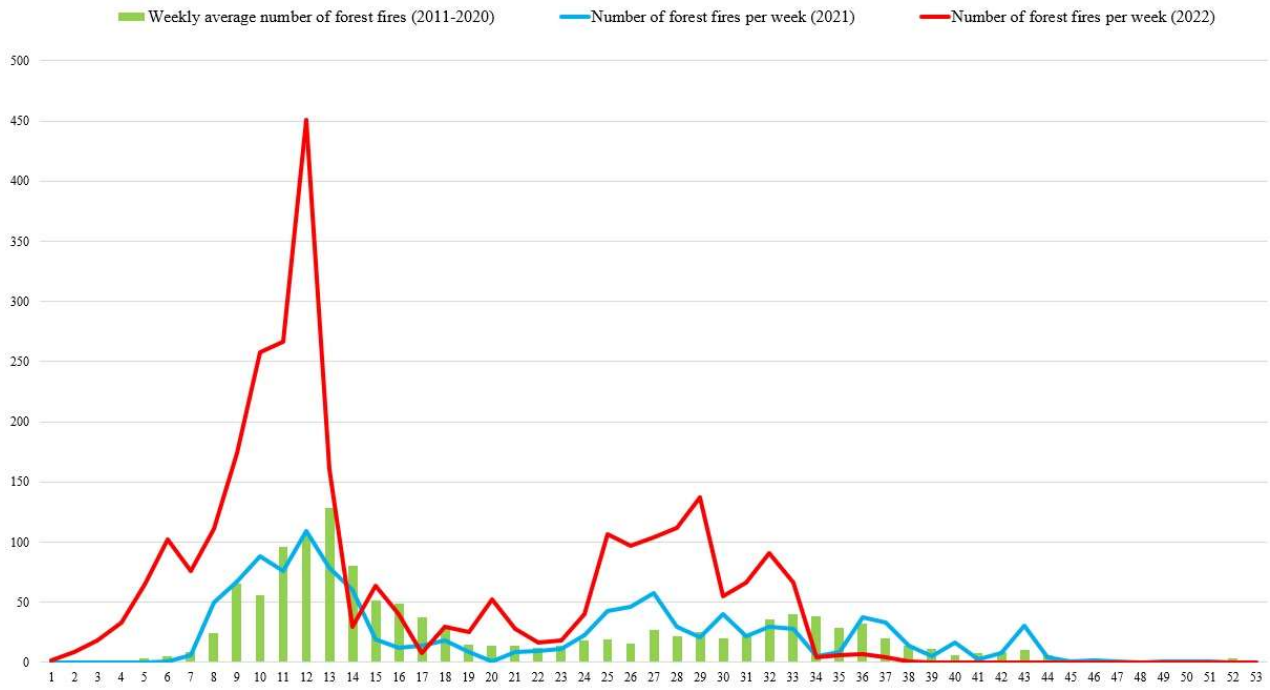
Land cover classification	Rate of fire events (%)
Residential area	22,4
Agricultural areas	51,7
Forest land	8,7
Natural grasslands and pastures	9,6
Transitional woodland/shrub	7,6

99 % of wildfires are human-induced (negligence or arson). Most fires are induced by negligence and only a small proportion of fires are caused by arsonists. Typical forest fire causes are the incorrectly extinguished fires of hikers, and the illicit agricultural fires, throwing cigarette butt and sometimes slash burning. Surface fire is the most common type of wildfire. 95% of fires during the fire season are surface fires. Low-intensity surface fire means when there has been no damage to the woody stem level. In this case, only the dried grass and leaves on the lower level were burnt. Low-intensity surface fires occur every year between February and April before the foliage. A high-intensity surface fire can develop when a brush or young forest burns. In crown fires, the fire spreads at the crown level or in the higher shrub level independently of the surface fire. Crown fire can occur mainly in pine stands in the sandy area of the Great Plain.

[3] Corine Land Cover Database: https://land.copernicus.eu/pan-european/corine-land-cover

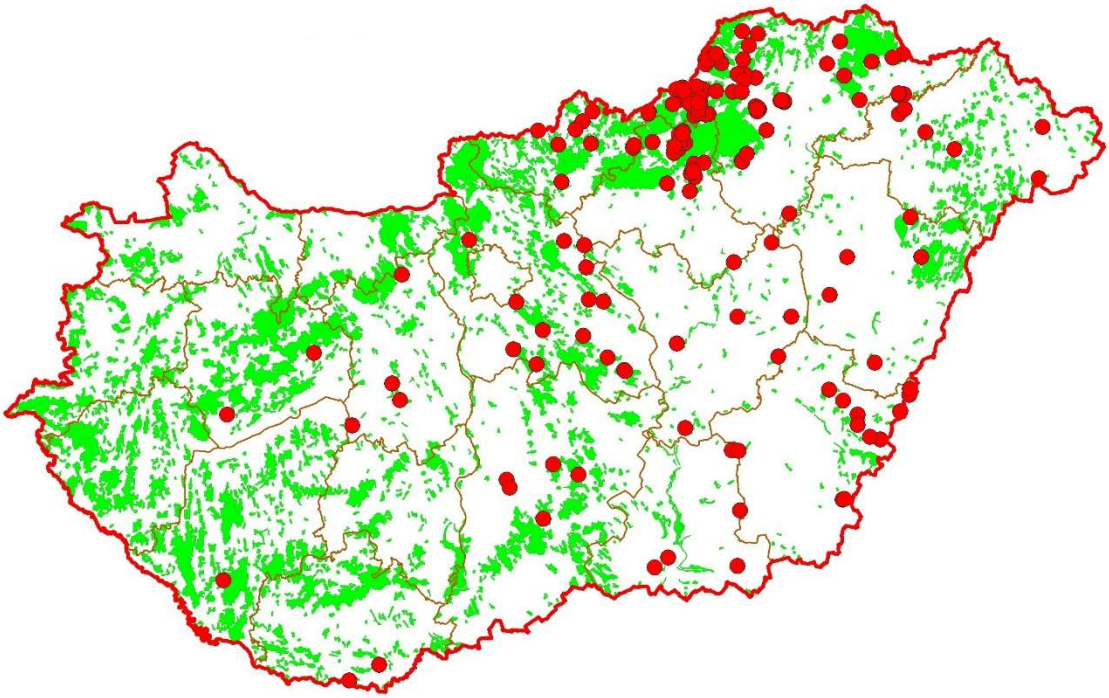
Impact of climate change on wildfire risk

As discussed in the previous chapter, there have also been changes in the trend in fire numbers in recent years. Forest fires have a significant impact on the condition of natural areas and the quality of life of the population. The increase in the number of large fires and the need to extinguish fires in a single day ties up significant firefighting resources during the fire season. As a result of intense fires caused by drought, two people died in wildfires in 2022. The negative trend is expected to continue in the coming years.



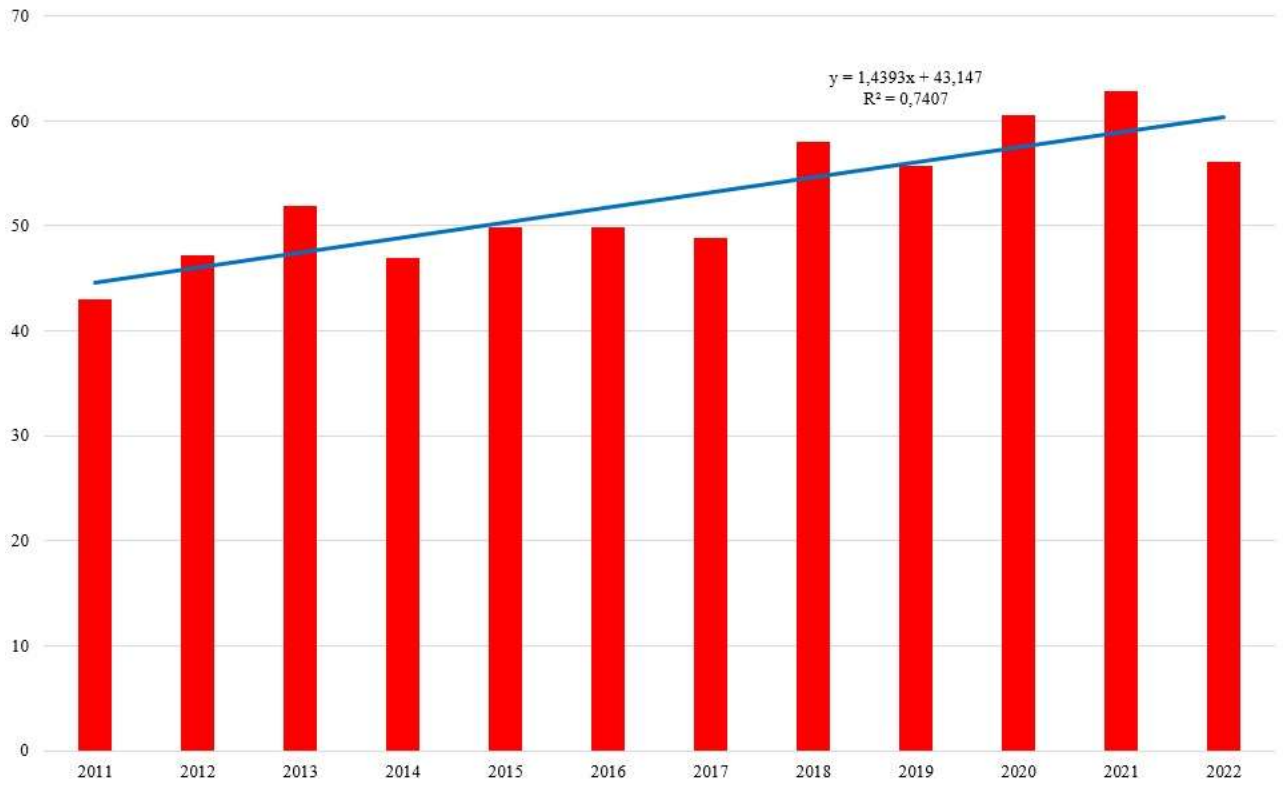
2. *Figure: weekly average number of forest fires and deviation from average (2011-2022) [4] (created by author)*

Wildfires also caused damage in regions of the country where it was not previously common. Complex reasons have been identified behind the negative trend. At both Community and national levels, there is evidence that forest fire response capacity is facing increasing challenges, despite close coordination between authorities and improvements over the past decade. In addition to climate change and new weather patterns, other fire risk factors should be studied. Scientific studies of land use patterns, social patterns, cultural and recreational practices, and the impact of fire on the environment, as well as fire policy, will help in the development of a new fire strategy. There were large fires in Hungary last year, which caused considerable difficulties in extinguishing due to the intensity and burnt area of the fires.



3. Figure: wildfires over 50 hectares (2011-2022) [4] (created by author)

Fire statistics for 2011-2022 show an upward trend in the number of fires below 0.5 ha (Figure 4). These smaller fires require the intervention of the fire brigade throughout the year, even in cases where it would be safe to burn the fire if the fire rules were followed. In addition, the spread of fire can become uncontrollable under favorable topographic, biomass, and meteorological conditions.



4. Figure: Proportion of fires smaller than 0.5 ha (2011-2022) [4] (created by author)

The progression of fires is influenced by human activity, the location and structure of combustible dead fuel, and changes in moisture content due to meteorological conditions. Knowing the high risk periods is important to take timely and effective preventive measures. [9] These adverse changes encourage public authorities to increase their capacity to respond.

Forest fire risk evaluation in Hungary

Due to Hungary's mosaic landscape structure, forest fires affect not only forest land but also other wooded land and agricultural areas. Forest fire prevention, therefore, requires integrated cooperation between several organizations. The tasks of forest fire prevention in Hungary are set out in the Forest Act and its implementing decree and the Ministerial Decree on Forest Fire Protection. The fire prevention system in Hungary consists of the following components. Forecasting fire danger periods and assessing the risk of forest fires, supporting firefighting activities with IT systems, preparing fire prevention plans, and organizing public information systems and educational programs.

The fire hazard classification of forest land is prepared by the forestry authority and updated every year. The classification is based on tree species data recorded in the forestry register. The

classification is carried out at the forest section level. After the classification, each forest section will have its fire hazard indicator, on a three-level scale. The indicator expresses the quantity and combustibility of the combustible biomass in the forest section. The classification is based on the data registered by the forestry authority, and with its help, professional expectations can also be properly enforced.

5. Figure: Map of fire hazard classification of forest land (source: https://erdoterkep.nebih.gov.hu/)

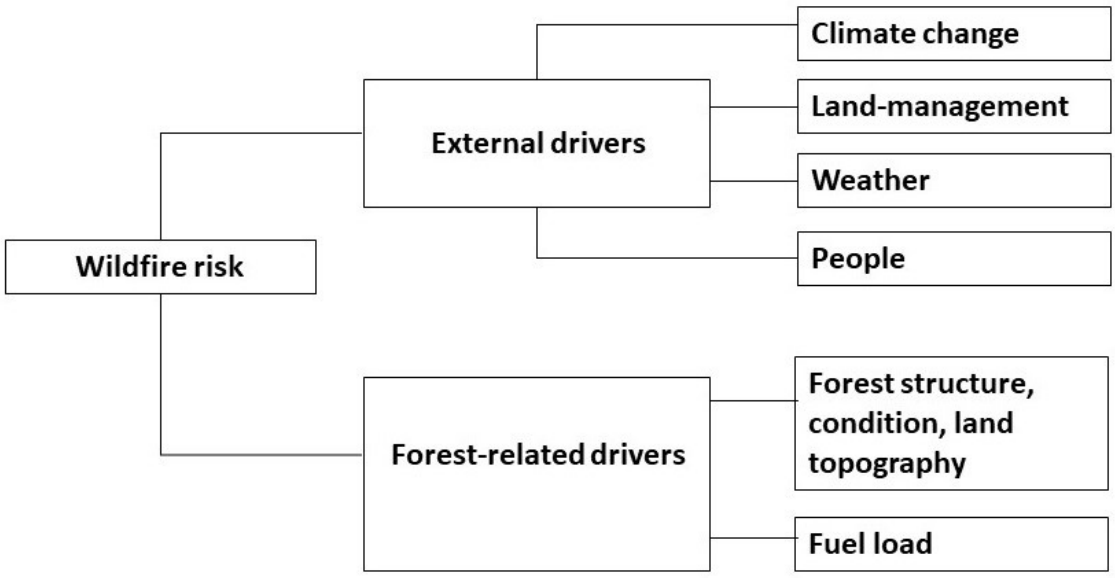
Based on the classification at the forest section level, the forest manager must prepare a forest fire protection plan and is obliged to keep specific tools and work groups ready in case of a forest fire. Farmers with between 10 and 100 ha of the fire-prone forest must prepare a simplified protection plan. Farmers in fire-prone areas larger than 100 hectares must prepare a complex forest fire protection plan. The forest fire protection plan includes the risky forest areas in the farmer's territory and the prevention activities. The plan also includes a map system, which the forestry authority provides free of charge to forest managers. The classification is also available on the public forest map operated by the forestry authority on the World Wide Web. Hungary provides the use of forest maps as part of a web map service for the GIS system of disaster management.

In high-risk periods, the forest authority can order a fire ban in consultation with the fire service. The risk periods and the delimitation of the areas affected by fire risk must be displayed on the website of the forestry authority. The map is continuously available during the fire season on the

websites of the relevant authorities[4][5] and cooperating organizations. The decision depends on three main parameters: meteorological conditions, the daily value of the Fire Weather Index (FWI) published by the Joint Research Center[6] (JRC), and the frequency of fires. The assessment and analysis of forest fire risk are carried out every year from 1 February to 31 October. The forestry authority and the fire service will announce the increased risk of fire. The domestic forest fire risk assessment is based on the hazard classification of forest areas and the use of the FWI published by the JRC.

Wildfire drivers

The risk assessment should also examine the factors that play a role in the development of forest fires and the increase in the number of fires. In this approach, external and forest-related drivers play a role in the development of wildfire risk. [10]



6. *Figure: Wildfire risk and wildfire drivers [10] (created by the author)*

[4] Forest fire ban on official website of National Food Chain Safety Office (http://erdotuz.hu/kezdolap/)
[5] Forest fire ban on website of Ministry of Interior Directorate General for Disaster Management (www.katasztrofavedelem.hu/).
[6] https://effis.jrc.ec.europa.eu/about-effis/brief-history

The risk of forest fires is influenced by external drivers such as climate change, land use, weather, and human behavior. Rising average temperatures and periods of drought cause more high-risk days. Fuel also becomes combustible on high-risk days. Combustible fuel can accumulate in abandoned rural areas. Changing climatic conditions may extend the growing season. This can lead to changes in the composition of plant species and an increase in combustible fuel, which can lead to fire hazards. The distribution area of tree species is influenced by climatic conditions. It can increase the area of tree species that are susceptible to fire. Changes in rainfall patterns and more frequent droughts are affecting areas of Europe where forest fires have not occurred in the past.

Human activities often contribute to wildfires. Although fires can also be caused by natural causes (lightning, spontaneous combustion), data from the European Forest Fire Information System (EFFIS) show that the majority of fires in Europe are caused by humans.

The main link between the two main components of fire risk assessment, i.e. forest-related factors and external factors, is land management and activity planning. Fire management is also a form of land use. While the decline of rural areas may contribute to forest fires in some areas, in other cases urban sprawl has resulted in people moving to near fire-prone areas. Accumulating fuel on abandoned or intermittently managed agricultural land also contributes to increasing fire risk and fire spread. Management decisions can also influence the composition and quantity of combustible biomass. The risk of fire in afforestation is increased by the lack of cultivation and inappropriate selection of tree species. At the same time, the risk of forest fires is reduced by thinning forests and establishing and maintaining a fire protection system, as well as by selecting resistant tree species for planting that are appropriate to the site. The risk of forest fires can be further reduced through forest fire management measures. [10]

A new approach in wildfire prevention

As discussed in the previous chapters, there have been changes in the trend of fire events in recent years. Similar to the trend in Europe, forest fires have a significant impact on the condition of natural areas and the quality of life of the population living near fires. Wildfires also caused damage in regions where there were no previous fires. Complex reasons have been identified behind the negative trend. At both Community and national levels, there is evidence that forest fire response capacity is facing increasing challenges, despite close coordination between authorities and improvements over the past decade. In addition to climate change and new weather patterns, other

fire risk factors should be studied. Scientific studies of land use patterns, social patterns, cultural and recreational practices, and the impact of fire on the environment, as well as fire policy, will help in the development of a new fire strategy. Some large fire also occurred in our country last year and extinguishing them is a major challenge due to the intensity and extent of the fires.

Fire prevention practice in Europe has moved towards integrated wildfire management, where more attention needs to be paid to land-based fire prevention practices. Integrated fire management is a system of forest fire prevention, preparedness, and response policies. According to climate change projections, Mediterranean countries in Europe will be the most affected by fires. However, adverse changes are also expected in Hungary. In addition to an increase in the annual number of days with high fire risk, the impact of large fires is also increasing in the center and northern part of the country. In recent years, the fire season in our country has started earlier and ended later. This puts a greater burden on the fire service. [11]

Fires in Europe are predominantly caused by human causes, highlighting the critical role of the human factor in fire prevention. [12] The national data collection system reveals a situation similar to that in EU countries. The vast majority of fires in the spring fire season are related to agricultural activities. The rest of the year, fires are caused by grass burning and human negligence. [13]

Among the external drivers shown in Figure 1, land management and public information can help increase the effectiveness of fire prevention. Forest management practices as a forest-related driver can control forest structure. Appropriate land management practices can also control the amount of combustible fuel. To introduce a land-based wildfire management to forest fire prevention, changes need to be made in the following areas.

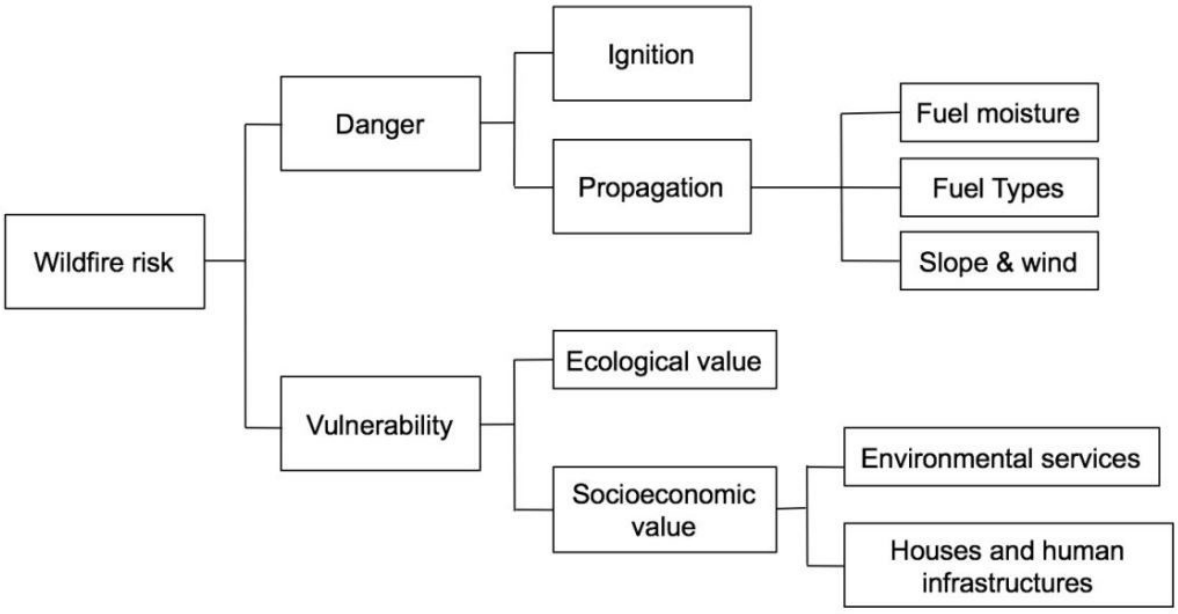
- Government
- Mapping and estimating forest fire risk
- Planning and fuel load management
- Tudatosság növelő kampányok, képzés
- Common strategy for wildfires

Government

Uniform legislation has been developed at the government level over the last two decades. The tasks and implementation levels have been clearly defined. There is a regular exchange of information between the responsible organizations and joint training sessions are organized every year. Incorporating the application of risk assessment methods into forest fire legislation could be a future task. Connecting experts at different levels of government, regular meetings between responsible organizations and information sharing are important to achieve a common approach.

Mapping and estimating forest fire risk

Wildfire risk assessment is essential for planning fire prevention measures. The risk assessment helps to identify areas at risk of wildfire. The identification of the elements of fire risk indicates the methods of risk reduction and the way of land use. The fire risk of an area depends not only on human factors and the number of wildfires recorded. Fire starts when the moisture content of dead fuel falls below the extinction moisture content. Wildfire risk is a combination of the daily fire risk and the impact of the vulnerability of the area affected by the fire. Wildfire risk from weather effects gives an estimate of ignition and fire spread. The vulnerability of the area affected by the fire is characterized by ecological and socio-economic parameters. Socioeconomic parameters refer to environmental services and human infrastructure.



7. *Figure: Basic components of wildfire risk assessment [12] (created by the author)*

Several approaches and methodologies are used to assess forest fire risk in the EU Member States. A method has been defined at different scales (national, regional, local) for each country. In many cases, systems have been set up for different purposes. This also causes problems as some fire risk concepts are used in different senses in some Member States. For this reason, it is difficult or impossible to compare fire risk management measures in the Member States. The European Commission's Joint Research Centre is developing a forest fire risk index that fulfills the criteria of fire risk and vulnerability. This wildfire risk model identifies high risk areas those parts of the country where the population is exposed to the effects of wildfires. Medium-risk areas are those where ecological values and social and economic values are at risk. [14] The large-scale risk assessment carried out by the JRC classifies the wildfire-affected regions of Hungary (Northern Hungary, Great Plain) as high-risk areas. This fact shows that fire risk assessment and its usability should be considered an important issue shortly. By adapting the methodology, we can help to refine the JRC's risk assessment and give a new direction to domestic risk assessment by incorporating new components.

Planning and fuel load management

Not all wildfires can be completely prevented, but good landscape planning and forest management plans can improve the resilience of the landscape and species. Planning should reduce the likelihood of fires occurring, the severity of the damage, and the impacts on people and the environment, and assist firefighting activities.

The national landscape strategy states that the practice of field and forest management should be adapted to local conditions as far as possible and sustainability should be taken into account. Climate-smart land management is characterized by diverse crops and a mosaic landscape structure. The aim is to maintain permanent plant cover. Consensual rehabilitation interventions are needed to adapt to the landscape. In some areas, changes to the way the landscape is used should also be considered. Traditional landscape use is declining, resulting in a smaller and smaller area of mosaic landscape. Forests have an important role to play in mitigating the effects of climate change. Planting mixed forests is of paramount importance in forest management. Mixed forests can ensure forest survival under changing climatic conditions and compensate for forest damage. [15] The accumulated dead fuel is often destroyed by burning. However, burning ignores safety rules and leads to uncontrolled wildfires. [4]

There is no legislation on wildfire prevention at the Community level. Lighting wildfire is defined as a local problem at the national level. Planning is needed to reduce the vulnerability of landscapes to wildfire. There are elements of planning at the national and regional levels. Planning at the national level should take into account the capacity of public authorities, institutional infrastructure, and environmental specificities.

Forest managers must prepare a forest fire plan in Hungary. [16] No risk assessment and no fire protection plan are carried out in areas not covered by trees. In those areas, there is no information available for fire fighting in case of fire. Lack of protection plans is a major risk in firefighting. therefore, protection plans need to be renewed at the national level. Some of the basic information is already available for risk assessment by the responsible authorities. Missing data can be identified once the methodology has been adapted. The complex risk assessment includes an assessment of the risk elements, a description of the preventive measures, and the basic data necessary for the preparation of the fire protection plans. The responsible authorities can prepare an official response plan based on the risk assessment. This describes the actions to be taken in the event of a wildfire. Farmers and managers can prepare a simplified risk assessment for managed areas based on the prevention plan prepared at the national level. The methodology for preparing the management plan is set out in the national fire prevention plan. In high-risk areas, a specific forest fire management plan should be drawn up, detailing the specific activities related to forest fire prevention and management. The management plan shall include all fire prevention activities and techniques aimed at increasing the resilience of the forest to forest fires and reducing the severity and spread of forest fires. The second part of the management plan is the emergency plan, which provides important information to fire and rescue services in the event of a forest fire. It is essential that the forest fire management plan accurately reflects the current situation on-site. Forestry activities can change the structure of the landscape, so fire prevention plans need to be clarified in case of changes. [17]

The combustible material is any living or dead biomass that supports combustion in a wildfire. Flammability depends on moisture content. Fuel management can reduce fire risk, so forest management is also a biomass management activity. Logging removes fuel from the forestland. Logging removes biomass from the forest area. Combustible fuel can accumulate on unmanaged forest land, which can lead to a high fire risk under adverse meteorological conditions. Prescribed burning is a good way to remove combustible fuel. There is no tradition of prescribed burning in Hungary. There are no trained professionals who can carry it out safely. One of the priorities for the

future is the development of implementing rules for prescribed burning and training material for fire brigades and farmers.

Awareness-raising campaigns and training

The experience of sociological research [18], professional workshops and international knowledge transfer programs [19] have shown that increased knowledge on wildfire prevention can be achieved through awareness raising, information communication campaigns, and training of professionals. Forest Authority's forest fire prevention communication program has been designed with multiple objectives. The training program aims to reach out to relevant social groups, to train professionals, to present practical cost-effective methods and good practices. Training materials were developed in the training panel for forestry, nature conservation a,nd fire protection professionals and teachers. Training and information program is based on a communication plan and annual action plans. A training program, approved by the University of Public Service, has been developed for forestry and nature conservation professionals working in the public service. For people living in areas of the country where there is a risk of fire, publications are produced to help them learn about the conditions under which wildfires start. This training material teaches how to avoid uncontrolled fires and provides information on management methods and activities that can help reduce the risk of wildfire. [20] [21]

A common strategy for wildfires prevention

The current approach is not enough effective to prevent fires in high-risk periods. Our main strategy is to extinguish all wildfires. [10] Climate change is contributing to changes in fire season patterns and fire characteristics. Changing the fire environment means that the current approach will not be effective in the long term and will pose a major challenge to the fire service. These circumstances require us to change our wildfire strategy. Three pillars of a new strategy based on Community scientific research. [17]

1. Wildfire-resistant landscapes

2. Wildfire-resilient communities

3. Adapting safe and effective fire fighting techniques to changing wildfire environment

The strategy requires all stakeholders to be involved and to incorporate the best scientific results. Low-intensity fires will be tolerated and used to create a fire-resistant landscape where it is possible. This approach requires the integration of risk assessment into land use practices. Forest fire prevention measures are supported by the European Union through the Common Agricultural Policy (CAP). Funding should be used to better manage forests to improve their resilience to forest fires. The EU Rural Development Fund is actively supporting the restoration of burnt areas and training and advisory services for farmers. [10] A new forest fire risk management methodology is being developed at the Community level. Missing data should be examined before the national strategy is developed. The development of a national strategy should be based on cooperation between the authorities responsible for wildfire prevention. So effective prevention methods can contribute to safer firefighting, and not only in the field of wildfires. [22] [23]

Conclusion

There have been changes in the trend of wildfire rates over the past decade. Wildfires have a significant impact on the condition of natural areas and the quality of life of the population living near risk areas. Wildfires have also caused damage in parts of the country where there have been no fires in the last decade. Complex reasons have been identified behind the negative trend. Wildfire response capacity is facing increasing challenges, despite existing close coordination between authorities and improvements over the past decade.

The current approach is not enough effective to prevent fires in high-risk periods. Our main strategy is to extinguish all wildfires. Climate change is contributing to changes in fire season patterns and fire characteristics. Changing the fire environment means that the current approach will not be effective in the long term and will pose a major challenge to the fire service. These circumstances require us to change our wildfire strategy.

The components of the fire risk from climate change need to be identified to develop a new effective fire prevention system. Wildfire risk is a combination of the daily wildfire danger and the vulnerability of the area affected by the fire. Land use patterns need to be reviewed to create a fire-resistant landscape for the future.

The development of land-based wildfire prevention strategy requires the development of the following components, taking into account new scientific findings.

Wildfire risk assessment requires a daily fire danger forecast and an assessment of the vulnerability of fire-affected areas.

It is important to plan fire prevention measures in the forest management plan to achieve a fire-resistant landscape. Planting fire-resistant tree species in afforestation is recommended.

Fuel management can reduce the risk of wildfires. Its implementation requires rained professionals and methods adapted to local specialties.

Awareness-raising campaigns and training will provide useful information to the public on wildfire prevention.

The best use should be made of EU funding opportunities.

When wildfires occur, a coordinated, rapid, and effective response is crucial.

References:

1. San-Miguel-Ayanz, J., Durrant, T., Boca, R., Maianti, P., Libertá, G., Artés-Vivancos, T., Oom, D., Branco, A., de Rigo, D., Ferrari, D., Pfeiffer, H., Grecchi, R., Onida, M., Löffler, P. 2022. Forest Fires in Europe, Middle East and North Africa 2021, Publications Office of the European Union, Luxembourg, 2022, doi:10.2760/34094, JRC130846. (https://effis-gwis-cms.s3.eu-west-1.amazonaws.com/effis/reports-and-publications/annual-fire-reports/Annual_Report_2021_final_topdf1.pdf) (Download: 31.10.2022)
2. *Words into Action Guidelines: National Disaster Risk Assessment, Hazard Specific Risk Assessment* (2017). UNISDR. Forrás: www.unisdr.org/files/52828_06wildfirehazardandriskassessment.pdf
3. IPCC, 2022: Climate Change 2022: Impacts, Adaptation, and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [H.-O. Pörtner, D.C. Roberts, M. Tignor, E.S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, B. Rama (eds.)]. Cambridge University Press. Cambridge University Press, Cambridge, UK and New York, NY, USA, 3056 pp., doi:10.1017/9781009325844.
4. Forest Fire Information System operated by National Food Safety Office
5. Abonyi Anita – Debreceni Péter – Nagy Dániel – Szabados-Molnár Dominika: Erdő- és vegetációtüzek Magyarországon. Átalakuló területi, időbeli jellemzők, Erdészeti Lapok, 60. 4. (2015) 106-108. http://erdeszetilapok.oszk.hu/01802/pdf/EPA01192_erdeszeti_lapok_2015-04_106-108.pdf
6. Padányi József - Halász László: A klímaváltozás hatásai. – Tanulmány Nemzeti Közszolgálati Egyetem, Budapest: 2012., 254 oldal https://www.uni-nke.hu/document/uni-nke-hu/padanyi_klimavaltoz_tanulm.pdf
7. Bodnár László: Lakott területet érintő erdőtüzek vizsgálata, és a védekezés egyes lehetőségei. *Hadmérnök*, 15. 1. (2020), pp. 45-61.
8. Bodnár, L. and Debreceni, P. (2023) "Complex Analysis of Wildfires in Hungary in the Last Decade", *AARMS – Academic and Applied Research in Military and Public Management Science*. Budapest, 21(3), pp. 21–48. doi: 10.32565/aarms.2022.3.2.
9. Van Wagner Estair: *Development and structure of the Canadian Forest Fire Weather Index System*. Vol. 35 of the Forestry Technical Report series. Canadian Forestry Service, Ottawa, Canada. 1987.
10. European Commission, Directorate-General for Environment, Nuijten, D., Onida, M., Lelouvier, R., *Land-based wildfire prevention : principles and experiences on managing landscapes, forests and woodlands for safety and resilience in Europe*, Nuijten, D. (editor), Onida, M. (editor), Lelouvier, R. (editor), Publications Office of the European Union, 2021, https://data.europa.eu/doi/10.2779/695867
11. de Rigo, D., Libertà, G., Houston Durrant, T., Artés Vivancos, T., San-Miguel-Ayanz, J., *Forest fire danger extremes in Europe under climate change: variability and uncertainty,* EUR 28926 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN: 978-92-79-77046-3, doi:10.2760/13180, JRC108974
12. Oom, D., de Rigo, D., Pfeiffer, H., Branco, A., Ferrari, D., Grecchi, R., Artés-Vivancos, T., Houston Durrant, T., Boca, R., Maianti, P., Libertá, G., San-Miguel-Ayanz, J., et a.l. 2022. Pan-European wildfire risk assessment, EUR 31160 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-55137-9. doi:10.2760/9429, JRC130136

13. Debreceni Péter: Magyarországi vegetációtüzek keletkezési okainak vizsgálata és osztályozása *Műszaki Katonai Közlöny,* 31 : 4 pp. 111-128. , 18 p. (2021) doi: 10.32562/mkk.2021.4.8
14. San-Miguel-Ayanz, J., Costa, H., de Rigo, D., Libertà, G., Artés Vivancos, T., Houston Durrant, T., Nuijten, D., Löffler, P., Moore, P., Baetens, J., Konstantinov, V., Duche, Y., Joannelle, P., Debreceni, P., Nagy, D., Zaken, A.B., Mitri, G., Assali, F., Alaoui, H.M., Piwnicki, J., Szczygieł, R., Almeida, R., Mara, S., Eritsov, A., Sandahl, L., Moffat, A., Gazzard, R., 2019. Basic criteria to assess wildfire risk at the pan-European level. Publications Office of the European Union, Luxembourg. ISBN: 978-92-79-98200-2 https://doi.org/10.2760/052345
15. National Landscape Strategy (2017-2026) the Department of National Parks and LandscapeProtection, Ministry of Agriculture (https://kormany.hu/dokumentumtar/national-landscape-strategy-2017-2026)
16. Decree of Ministry of Municipalty 4/2008 on forest fire protection (https://njt.hu/jogszabaly/2008-4-20-2L)
17. Building wildfire resilience into forest management planning. Forestry Commission Practice Guide Forestry Commission, Edinburgh. (2014) ISBN: 978-0-85538-886-7
18. Szabó-Tóth Kinga – Havasi Virág – Urbán Anna – Mihályi Helga: Az erdőtüzek szociológiai vizsgálata Borsod-Abaúj-Zemplén megyében. Empirikus kutatások és elemzések. Miskolc: Miskolci Egyetem Szociológiai Intézet, 2012.
19. Plana, E., Font, M., Green, T. (Editors). 2015. Operational tools and guidelines for improving efficiency in wildfire risk reduction in EU landscapes. FIREfficient Project. CTFC Editions. 88pp ISBN: 978-84-608-5083-0
20. Firelife Erdőtűz megelőzési és képzési projekt After LIFE Communication Plan 2019-2022 (https://portal.nebih.gov.hu/documents/10182/1199137/FIRELIFE_afterlife_com_plan_HUN.pdf/cf002290-cf95-d2c0-7d81-2eb36520a07a)
21. Firelife Erdőtűz megelőzési és képzési projekt (http://erdotuz.hu/eloadasok/)
22. Rácz Sándor - Finta Viktória: *Occupational safety of firefighters in radiological emergencies — Issues in Hungary.* Rad Conference Proceedings 2 pp. 75-79. , 5 p. (2017).
23. Varga Ferenc: Structural and operational model for volunteer fire brigades. *Hadmérnök,* 13. 2. (2018), pp. 345-359.

Analysis of throw-ins in the Premier League and La Liga championships

János Tóth jr., Benedek Bán

Hungarian University of Sports Science

Abstract

The goal of our research is to draw the attention of sports professionals to the importance of throw-ins as a tactical element in football, as they occur more frequently than free kicks. In our study, we took the English Premier League and the Spanish La Liga as a basis. We want to emphasize the importance of throw-ins. This was confirmed by our study where we analysed all matches played in both leagues and found that there is a difference in the number of free kicks and throw-ins. The English Premier League had a total of 15046 throw-ins, while the Spanish La Liga had 15883 pcs. On the other hand, free kicks were only 8317 in the English and 12693 pcs in the Spanish one. The research revealed that there is a significant difference in favour of throw-ins. Throw-ins performed backwards dominated in both leagues, with 8286 in the English league and 7715 pcs in the Spanish league.

Keywords: throw-in, football, comparison

Introduction

Certain set pieces in football (free kick, penalty kick, kick off) have received greater attention in recent years. Coaches have gained access to detailed analyses and studies, which have gradually led to an emphasis on examining and improving the performance of these set-piece situations during training. As a result, the throw-in as a tactical aspect has not received much attention. We have come to the conclusion that there are more throw-ins than free kicks during a match in general.

Football has become more prominent in recent decades compared to previous years. According to Gerald H., the globalization of football had already taken place at the end of the 20th century[1]. With the development of technology, the examination of certain statistical measurements in sports have received more attention. Nowadays, clubs have specialists working to improve specific areas (including fitness coaches, video analysts, and free kick specialists). Their task is to provide the club with the best possible quality development in their respective areas. With the development of football, the rules have changed over the years, so the correct way of movements/techniques of throw-ins have also changed. The International Football Association Board (IFAB) is responsible for creating the rules in football. For the correct execution of a throw-in, the player must face the field, stand on the sideline or outside the sideline with both feet, bring the ball forward with both hands above the head and return the ball from the point where it left the field.[2]

Csanádi also studied the technique of the throw-in in previous decades.[3] We were focusing on the technique, common errors, and teaching methods of the throw-in in our study. The technical

description/criteria is clearly the same as described in the rule, also the throw-in can be performed either standing or while running. In both cases, you must pay attention to the correct execution (for example not performing the movement while jumping or having equal force in both arms at the moment of throwing).

If a team has a player with a strong physique who is able to throw the ball a great distance, this can be seen as a tactical advantage for the team in the case of throw-ins[4]. This kind of progress in the sport makes it possible to throw the ball near the goal even from the halfway of the field. Furthermore, with the global spread of the sport, the creation of some acrobatic throw-ins also occurred during matches.

The ball leaves the field during a throw-in. According to the rule, there is no offside position at the moment of the throw-in, which is why strategic practice can become more prominent in the players' mind. Using throw-in figures and tactics, the throw-in team has a serious opportunity to score goals. These figures can be used in ball retrieval and attack management.

Our goal is to draw the attention of sports professionals to the fact that throw-in deserves more emphasis than before (from a tactical perspective), as it can occur more frequently in a match than other set pieces. In many cases, the throw-in is not thrown in a conscious direction/place during a match, but rather they try to get the ball to a free teammate as soon as possible. According to a study, players who don't know what to do with the ball in their hands often literally just throw it away[5]. D. Clarke believes that if someone can come up with a good tactic for the throw-in it can lead to serious goal-scoring opportunities. He emphasizes that accuracy and communication are necessary for successful short throw-ins. As a result, having a good tactic can give an advantage in attack during a throw-in, making it difficult for the opposing players to react to the ball's direction as well as potentially leading to a goal-scoring opportunity in the match for the team.

In many cases, the players performing the throw-in do not have in mind which area of the football field the ball should be thrown into, as throw-in practice did not receive significant attention during preparation/training. One reason for this might be that, unlike other set pieces, a goal cannot be directly scored from a throw-in.

According to T. Bradbury, the throw-in should be a tool for the team to keep the possession of the ball and hopefully with a well-constructed offensive formation the team will launch an attack at the moment of the throw-in. It should also be a player-centered moment, as the player executing the throw should be allowed to make the right decision. This is why the topic is worth examining, as if we observe many matches from the sidelines, we can discover that many coaches ask their players to throw the ball forward along the sideline. This may not be a good decision in all cases, as there are often more defenders than an attacker, making it more difficult to keep the possession of the ball[6].

Based on the matches studied in the United States, they concluded that the closer a throw-in is to the team's goal, the less likely it is to be kept. In fact, throw-ins executed within 20 meters of a team's goal are more likely to lose the ball than keep it. This type of study provides the possibility that the variations of the throw-in practice are depending on the area of the field where the ball left the sideline.[7]

Hypotheses

Three statements have been formulated.
Firstly, we claim that there are more throw-ins in a match than free kicks.
Our second statement is that forward throws-ins occur more often than backwards throws.
Last, but not least, we were claimed that more than 2/3 of the throws will be successful on first contact.

Method

We based our research on matches played in the Premier League 2021/22 season and La Liga 2021/22 season. A total of 380 matches were played in one league (n=760). During our research, we used online websites and broadcasting platforms as sources. By using Eredmények.com, the official websites of the teams in the league in the given year and other statistical websites, we were able to create Excel worksheets with the statistical parameters related to throw-ins, so we could examine the questions necessary for the procedure and comparing the results of the top teams. During the investigation we focused on the direction of the throw-in. Was the throw-in successful? Successful throw-ins were determined by whether the first touch after the throw-in was successful. The total number of free kicks and throw-ins were also examined. We were able to compare the throw-ins from every parameter and examined the questions of our research from the obtained data. For conformation we applied a paired two-sample T-test in the Excel worksheet for statistical analysis.

Results

We based our research on matches played in the English Premier League 2021/22 season and the Spanish La Liga 2021/22 season. Both leagues have the same number of the rounds and same number of the teams. Therefore, to analyse one league, as mentioned earlier, we will examine 380 matches.

Table1: Total Results

	Premier League	**La Liga**	**Average La Liga**	**Standard deviation La Liga**	**Average Premier League**	**Standard deviation Premier League**
total throw-in	15046 pcs	15883 pcs	41.7 pcs	9.4	39.5 pcs	9.1
forward throw-in	2907 pcs	3277 pcs	8.6 pcs	26.7	7.65 pcs	22.3
backward throw-in	8286 pcs	7715 pcs	20.3 pcs	54.3	21.8 pcs	33.4

successful throw-in	11775 pcs	12532 pcs	32.9 pcs	19.9	30.9 pcs	16.2
failed throw-in	3120 pcs	3148 pcs	8.2 pcs	11.05	8.2 pcs	11.1
free kick total	8317 pcs	12693 pcs	33.4 pcs	8.5	21.8 pcs	5.7

The table shows the aggregated data based on the analysed parameters. We would like to add that for both leagues, after all the throw-ins examined, we will not take into account 151 throw-ins in the English league, and 203 in the Spanish league, as these were occurred after an injury, when the ball is returned to the opposing team. The direction of the throw-in was determined based on the body position, at what angle did the ball was thrown onto the field (0º-60º backwards, 61º-120º neutral, 121º-180º forwards).

The average of all throw-ins in the English league was 39.6, while the free kicks are almost half of that with 21,8 throughout the season. The two-sample t-test shows a difference between the number of throw-ins and free kicks ($p<0.001$). Examining the standard deviation, we can see the difference during the matches in the league, as the throw-in shows a value of 9.1, while for free kicks, this value is 5.7. The average number of successful throw-ins are 30.9, while for unsuccessful throw-ins we get a much lower number of 82.1. The statistical calculation shows a significant difference between the number of successful and unsuccessful throw-ins ($p<0.001$) in this case as well. During the standard deviation analysis, successful throw-ins indicate a value of 16.2 while unsuccessful throw-ins show a value of 11.1.

After the success rate, the direction was also examined. The average number of forward throw-ins is 7.65, while for backward throw-ins is 218.05. Statistical calculations also show a significant difference in the results in this case as well ($p<0.001$). The standard deviation for forward throw-ins is 22.3, while for backward throw-ins, it is 33.4. There is a significant difference in the standard deviation in this case.

The average number of all throw-ins performed in the Spanish league is 41.7 while for free kicks the average is 33.4. Using a two-sample t-test, a statistically significant difference can be detected ($p<0.001$). After examining the standard deviation following the mean values, we can see a difference in the values. We get a throw-in value of 9.4, while the standard deviation for free kicks is 8.5. Looking back at the English league, the difference in standard deviation is greater than in the Spanish league.

Moreover, we will not take into account 203 throw-ins in the Spanish league, as a result the average of successful throw-ins is 32.9 while unsuccessful throws-ins show much lower number (8.2). With the help of statistics, we can discover a significant difference in this case as well ($p<0.001$). The standard deviation for successful throws is 19.9, which is higher than the standard deviation for unsuccessful throws, which is 11.05. When examining the direction of the throw-ins, we can observe that the average for forward throws is 8.6 which is much lower compared to the throw-in done backwards, which is 20.3. This difference can also be observed in the value of the standard deviation,

since the standard deviation of the forward throw-in is 26.7 while for throw-ins made backwards is almost double that value (54.3).

Conclusions

A significant difference can be discovered between the number of free kicks and throw-ins in both leagues, thereby confirming our first statement. Additionally, it can be said that during the matches of both leagues the throw-ins were mostly directed backwards, indicating a focus on keeping the ball and not taking a greater risk for potential loss of possession. Based on this, our second statement was not confirmed. Both leagues have the same number of matches, so it can be stated that in the Spanish league, forward throw-ins were more prevalent. This can be attributed to the fact that the style of play in the Spanish league is more attacking and maintaining the possession of the ball anywhere on the field. Interestingly, when comparing the two leagues, there were significantly more long throw-ins in the English league than in the Spanish league, which may be of interest as a study has shown that throw distance can be increased by starting the throw with a quick backward spin.[8] Furthermore, when examining the ratio of successful and unsuccessful throw-ins in both leagues, it can be seen that more than two-thirds of the throw-ins were successfully executed, thus confirming our third statement.

It was interesting to examine the matches of both top leagues from the perspective of throw-ins and draw conclusions from this and it may provide assistance for further research by comparing other leagues.

Bibliography

[1] Gerald H. (2010): Futball és globalizáció, Göttingen

[2] IFAB: https://www.theifab.com/laws/latest/the-throw-in/

[3] Dr. Csanádi Á. (1978): Labdarúgás I. Sport Lap- és könyvkiadó, Budapest, 829 old.

[4] Loren E. K. & Marc S. (1981): The soccer throw-in Journal of Physical Education, Recreation & Dance,57,-59. old.

[5] Dave C. (2022): How to take advantage at throw ins, Soccer Coach Weekly (https://www.soccercoachweekly.net/coaching-advice/how-to-take-advantage-at-throw-ins)

[6] Tim B. (2021): Tragedy of Throw ins, SoccerWire (https://www.soccerwire.com/resources/the-tragedy-of-the-throw-in)

[7] Eliot M. (2018): Game of Throw ins, American Soccer Analysis (https://www.americansocceranalysis.com/home/2018/11/27/game-of-throw-ins)

[8] Nicholas P. L. & David J. E. (2007): Kioldási szög maximális távolsága a futball-bedobásokban (https://arxiv.org/abs/physics/0601149,243.-260. old.)

1. Dr. habil. NÉGYESI Imre PhD. egyetemi docens[7]
Nemzeti Közszolgálati Egyetem, Informatikai Tanszék

e-mail: Negyesi.Imre@UNI-NKE.HU

2. FEHÉR András tanársegéd[8]
Nemzeti Közszolgálati Egyetem, Informatikai Tanszék

e-mail: Feher.Andras@UNI-NKE.HU

Cyber security of the Controller Pilot Data Link Communications (CPDLC) system

Abstract

The CPDLC has significantly improved the efficiency and accuracy of communications, leading to increased air safety. It is clear that it has become an essential tool in modern air traffic control systems and will continue to play a critical role in ensuring their safe and efficient operation. Technological innovations have further enhanced the CPDLC, providing additional capabilities and further improving communication between pilots and pilots. Accordingly, the aim of this publication is to present the operation and built-in protection mechanism of an air navigation system developed in the 20th century but still in use today, highlighting the built-in vulnerabilities.

Keywords: CPDLC, controller pilot data link, cyber security, information security

Introduction

Aviation involves a complex system of factors including aircraft design, maintenance and operation, air traffic control and pilot training. Failure or malfunction of any one of these factors can lead to air accidents with catastrophic consequences. It is therefore essential that all necessary measures are taken to ensure that accidents and incidents do not occur in the first place.

Aviation cybersecurity - maintaining safe, secure and continuous operations - is one of the industry's top priorities. Technological advances and digitalization bring many benefits but also many challenges for aviation, given the cyber security vulnerabilities in this complex environment. The aviation sector is an attractive target for cyber-attackers with a wide range of motivations, from stealing data or money to causing disruption and damage.

This publication introduces the reader to the basic cybersecurity concepts and environment in aviation, and to the CPDLC. This technical solution may reduce the amount of voicebased radio communications, which can be used to increase airspace capacity and aviation safety. The widespread use of the CPDLC means that all civil aviation stakeholders need to pay more attention to cyber security than ever before. Furthermore

[7] ORCID: 0000-0003-1144-1912
8 ORCID: 0000-0002-8060-9056

below, the fundamental cybersecurity factors that affect the operation and applicability of the CPDLC system are also presented, keeping in mind the CIA (Confidentiality, Integrity, Availability) principle.

CYBERSECURITY IN AVIATION, CIA PRINCIPLES

When discussing the CPDLC's cybersecurity risks, it is important to parallel and address them with the factors that affect the information security of the system. The cybersecurity is a set of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage or unauthorized access. It can be seen that there is a close link between information security and cybersecurity, and therefore we don't intend to separate them in our work.

The unravelling of the letters of the "CIA principle" mentioned above may also be necessary for a more thorough understanding of the principles of cyber and information security. The CIA triage is a basic framework to guide the planning and implementation of information security measures. It is a pillar of information security and is used by organizations of all sizes and types to ensure that their critical assets are protected against cyber threats. The three principles are interdependent and complement each other, and together they provide a comprehensive approach to information security. Confidentiality and integrity, for example, are closely linked, as ensuring the confidentiality of sensitive information also helps to maintain integrity. Likewise, availability is closely linked to both confidentiality and integrity, as disruptions to it can compromise both confidentiality and integrity. To effectively implement the CIA triad, organizations must develop and maintain a comprehensive information security program that addresses all three principles and includes policies, procedures and security controls that are tailored to the specific needs and risks of the organization. The program should also include ongoing monitoring and testing to ensure effectiveness and continuous improvement.

Aviation safety is a core value for the provision of fast and reliable air transport services, and international cooperation on safety by governments and industry groups through the International Civil Aviation Organization (ICAO) has contributed to making commercial aircraft the safest way to travel. The 193 countries working together through ICAO are currently working to achieve the agreed global safety goal of zero fatalities by 2030, while strengthening regulatory capacity, and pursuing a number of programs and targets that address current key areas of global aviation safety planning, oversight and risk reduction. An analysis of this paper reveals a second objective, to enable the safety standardization necessary to integrate today's exciting innovations in aircraft propulsion, design, autonomous control and personal mobility, while maintaining or improving the reliable and continuous performance of the aviation system.

Aviation involves a complex system of factors including aircraft design, maintenance and operation, air traffic control and pilot training. Failure or malfunction of any one of these factors can lead to air accidents with catastrophic consequences. It is therefore essential that all necessary measures are taken to ensure that accidents and incidents do not occur in the first place. Aviation safety is a multi-faceted concept, with the prevention of accidents and incidents at its core. It includes all measures taken to ensure that aviation is safe for all concerned. It may include procedures, rules and precautions to prevent accidents and incidents, to minimize risks and to ensure the safety of passengers, crew and ground handling personnel. The manufacture and maintenance of aircraft, the training of pilots and the role of air traffic control are all critical factors in the safety of air transport. By taking the necessary measures to ensure aviation safety, we can ensure that aviation remains one of the safest forms of transport in the world.

The global digital infrastructure is present in almost every aspect of life. This is leading to a paradigm shift in communication (in information exchange). This change is not only driven by rapid technological advances, but also by the unprecedented scale of the overall interconnectivity of systems and networks. The world is witnessing a steady increase in cyberattacks across all sectors. This trend can be observed in the tenth edition of ENISA[9] 's Threat Landscape (ETL[10]) report, the annual report on the state of cyber security threats. It identifies the main threats, the main types of threat actors and attack techniques observed.

Aviation is no exception to cyber-attacks, characterized by its complexity, due to its complexity, high media coverage and critical role in the socio-economic development of states. The aviation sector is an attractive target for cybercriminals, who are nowdays using also the power of artificial intelligence in cyberspace. The industry can obtain the most sensitive personal data, for example through the Passenger Traffic Systems, which have access to passengers' passport and payment details, among other things. In line with the steady increase in demand for air travel over the years, the civil aviation industry has undergone a series of digital transformations aimed at harnessing the power of technology to increase the efficiency and capacity of the sector. However, these digital advances have exposed the air transport industry to cybersecurity threats for all stakeholders, where a successful cyber-attack could have a negative impact on the financial standing of companies and individuals, reputation, continuity of services, and even the safety and security of people and facilities.

Due to the global nature of the aviation industry, the interdependencies of systems and data flows also cross national borders and organizations. Therefore, a holistic approach to addressing cyber threats and risks to aviation must be based on a global framework based on cooperation between States and all relevant stakeholders. ICAO is therefore the ideal forum for the international aviation community to develop cooperation to ensure that efforts to address aviation cyber security are consistent, coordinated, inclusive of all aviation domains and consistent with the priorities of international civil aviation, with a focus on aviation safety.

CPDLC

CPDLC is a technology that enables text-to-text communication between air traffic controllers and pilots, facilitating more efficient and accurate communication in air transport. It is used in many countries to improve safety, reduce workload and increase capacity in busy airspace. Despite its benefits, the deployment and use of CPDLC also poses challenges like cyber security, standardization and equipment compatibility issues. To solve problems effectively, it is essential to have a good understanding of the subject under consideration, in this case the design, operation and role of the CPDLC system in air traffic control.

The concept of the CPDLC data link goes back to the 1983 meeting of the International Civil Aviation Organization in Montreal. In airports and associated airspace around the world, air traffic and VHF frequency band controller-to-aircraft communications are steadily increasing. It is estimated that world air traffic will double by 2037, with major European airports each handling up to 3,000 take-offs and landings

[9] ENISA – The European Union Agency for Cybersecurity
[10] ETL – ENISA Threat Landscape

per day. Meanwhile, the number of unmanned aerial systems (RPAS[11]) is forecast to exceed conventional air traffic, leading to airspace congestion. To reduce these pressures, technology to offload traditional voice communications has become necessary. CPDLC complements voice-based control and eliminates ambiguous communications, making air traffic more efficient and safer.

In recent years, questions have been raised as to whether the security of the CPDLC system is up to the level of technical sophistication of our time and whether it can withstand the resulting cyber-attacks. The original system was not designed with cybersecurity risks in mind, but rather aircraft crews, aircraft pilots and air traffic controllers. Flight safety lies in the trust between air traffic control and the pilot. Controllers rely on pilots not to deviate from the clearances they have been given, and pilots trust them not to give instructions that jeopardize their safety, while ensuring they are on the most efficient route possible.

The system is based on messages between air traffic control service units (ATSU) and aircraft. An ATSU sends its messages to aircraft "Uplink", while the opposite, messages from aircraft to ATSUs are "Downlink" messages. For any message, unless otherwise specified, the receiver, whether ATSU or aircraft, shall respond with a logical acknowledgement message (LACK) if the receiving system considers the received message acceptable for display. The CPDLC operates on VHF[12] frequency via the so-called Air Traffic Network (ATN). This is called VDL2 for short. This is an interface for data exchange between the ATSU and the aircraft, which operates between 118,00 MHz and 136,975 MHz at a data rate of 136,5 kbit/s, 31,5 kbit/s.

Once the connection is established, air traffic controllers can perform control activities using the predefined commands from the system. The extent to which CPDLC can replace voice communication depends largely on the current traffic situation. Although the technology allows for a wide range of complex messages, the most commonly used are:

- SSR -code ("squawk") changes;
- A unique identification code for aircraft (that allows them to be identified, broadcast by transponder equipment on board.)
- Transfer of control to another ATSU, change of frequency;
- Non-time critical control authorizations (e.g. change of altitude, vectoring, route selection, speed control);
- Response to aircraft CPDLC requests.

The messages are composed in a standard format using plain language or abbreviations and codes as specified. Free language should be avoided if the length of the text can be reduced by using appropriate abbreviations and codes. Non-essential words and phrases, such as courtesy terms, should not be used. Mandatory and optional - as already mentioned - uplink and downlink message sequences have been developed for each data link service. It is therefore possible that either the airborne or the ground system may support multiple messages.

This air traffic control system and its technologies must therefore be protected from cyber-attacks, as research has shown. With the widespread availability of low-cost, high-performance devices such as

[11] RPAS – Remotely Piloted Aircraft System
[12] VHF – Very High Frequency

software-defined radios (SDRs), the air traffic control community has lost the significant technological advantage that protected its communications in previous decades. Of course, monitoring traffic does not in itself pose a cybersecurity risk, but anyone with such radio equipment can access and monitor data communications and easily decode these messages. In our research on this subject, we have come across several websites where enthusiastic amateurs, or even professionals, share incoming data, experiences from sightings, creating a complete operational picture, including aircraft affiliation, aircraft type, flight plan, flight destination or possibly private information. Aircraft communications equipment, in particular the CPDLC system, has become an easy target for cyber-attacks. According to the 2020 security strategy of the association of ANSPs, (CANSO[13]), the introduction of increased automation and the reliance on system-wide data exchange means that related cyber security issues are now a key area requiring common industry-wide solutions. It's clear that the use of the VHF frequency band itself does not imply any security, anyone with a transceiver tuned to the appropriate frequency can freely receive and ultimately transmit.

As CPDLC is primarily used to issue commands between ATSUs and aircraft, we can assume that the main goal of the attacker is to hijack the data link and inject arbitrary data, mainly from the ATSU to the aircraft deck, but also in the other direction. This would allow them to issue direct orders to a selected aircraft while the aircraft is within range. Such commands could include, for example, instructions to change altitude, heading or speed, to activate and deactivate other data link systems, to announce the number of passengers on board or even to declare an emergency. Such an attack may also cause the aircraft to ignore legitimate messages received from the actual air traffic control service, which could lead to flight delays, dangerous conflicts or, in the worst case, air disasters. An attack model is nothing more than an identification of the types of potential attack vector(s) that can or do cause damage to an application or computer system. This model looks at the system and its vulnerabilities from the perspective of malicious hackers, showing the damage that attackers can cause.

The system currently in use does not have any built-in safety features beyond basic message integrity checks. Nevertheless, it is not impervious to all attacks, as the human component of the system makes it capable of detecting many basic attacks. It is very important to understand the background of attacks against CPDLC, their potential impact, and what can be done to mitigate the threats. A system capable of receiving and processing CPDLC signals can be built with minimal financial investment and the right expertise. The necessary tools are readily available commercially and may be sufficient to carry out these attacks.

This may be of particular concern as attacks can be carried out by motivated individuals with the appropriate technical knowledge. It is important to note that cybersecurity threats are constantly evolving and that the implementation of security measures is key to measuring the risk of attacks. Hackers are constantly developing new ways to exploit vulnerabilities in computer systems, which requires a proactive approach to security.

So, the full confidence of aircraft in the instructions of controllers is essential for the operation of the airspace. When an air traffic controller gives instructions to an aircraft, the aircraft is expected to comply unless it cannot, in which case the flight crew will inform the controller as soon as possible. Similarly, the aircraft is expected to comply with the instructions issued by the air traffic controller in a lawful manner without compromising flight safety. Since neither the CPDLC nor the underlying wireless VHF

[13] CANSO – Civil Air Navigation Service Organization

data links have inherent security mechanisms, it is readily available for an attacker to perform wireless message injection, which interferes with the data exchange between air traffic control and the aircraft.

The table below lists the main attack types using the MITER ATT&CK page. These practical examples clearly illustrate how certain forms of attack - messages from third parties - affect the security of the system.

Form	Type of attack	Affected fields of CIA	Practical example
Passive	eavesdropping	confidentiality	access to the air traffic control communications
Active	jamming	availability	channel blocking
	flooding	availability	ATSU / aircraft comm. systems overload
	code-injection	confidentiality integrity availability	communication as a fake actor
	man-in-the-middle	confidentiality integrity	message modification, and communication as a fake actor

1. Table: Possible types of attacks against CPDLC[14]

Conclusions

The increased use of new communication tools, including CPDLC, poses a greater threat than ever before in terms of crimes against aircraft. The identified vulnerabilities can be addressed with the guidance of the CIA principle. The easy availability of low-cost, highperformance devices, such as software-radios, has led to the loss of the technical advantage that previously protected communications. The CPDLC system has become an easy target for cyber-attacks and the use of common technology solutions is required to mitigate the risks. As there are no mechanisms to prevent unauthorized actors from impersonating air traffic controllers or aircraft, anyone with a radio receiver tuned to the appropriate frequency can freely receive and transmit messages. The sensitivity of data and the level of protection also depend to a large extent on the policies of the organizations handling the information. The lack of protection does not necessarily mean that attacks have actually occurred, but the lack of measures can have serious consequences, for example the collapse of air traffic control.

While the implementation of a designed secure version of the CPDLC is not realistic in the short term, our work also offers theoretical solutions to reduce the likelihood of major cyberattacks, and to reflect the cyber security risks of our technological advances. With the worldwide spread of CPDLC, vulnerability to attacks has only become more important. Therefore, understanding the system's vulnerability to attack and implementing mechanisms to mitigate such attacks has become vital to maintaining the safety and security of the air traffic.

It can be concluded that the use of CPDLC has brought significant benefits in terms of efficiency and accuracy of communication, but has also raised new security challenges that users need to address. The vulnerabilities of the CPDLC, such as the possibility of unauthorized access to the system, highlight the

[14] https://attack.mitre.org/

importance of maintaining and improving security measures to protect against potential cyber security threats. It is imperative for the aviation industry to continuously assess and update CPDLC security protocols and work to develop advanced technologies to mitigate potential risks. Ultimately, it is only through the combined efforts of regulators, industry stakeholders and practitioners that the continued safety of the CPDLC can be ensured, continuing to ensure the safety of aviation for all stakeholders.

References

1 ATT&CK: https://attack.mitre.org/ (Download time: 14.02.2023.)
2 BARNETT, A. (2020): Aviation Safety: A Whole New World?; Transportation Science; LIV. 2. p. 84-96.
3 BOEING: Commercial Market Outlook 2018–2037, https://www.pilotcareernews.com/wpcontent/uploads/2018/07/2018-cmo-07-17.pdf (Download time: 02.02.2023.)
4 Canso Standard Of Excellence In Cybersecurity, 2021., https://canso.fra1.digitaloceanspaces.com/uploads/2021/04/canso_standard_of_excellence_in_cybersecurity.pdf (Download time: 10.02.2023.)
5 ICAO (2017): Global Operational Data Link (GOLD) Manual (Doc 10037)
6 ICAO Annex 10, 3.7. Chapter, 2001,https://www.icao.int/Meetings/anconf12/Document%20Archive/AN10_V2_cons%5B1%5D.pdf(Download time: 09.02.2023.)
7 https://www.icao.int/assembly-archive/Session24/A.24.BOUND.1.P.EN.pdf (Download time: 31.01.2023.)
8 https://www.icao.int/Newsroom/Pages/States-aim-for-zero-aviation-fatalities-by-2030-through-ICAO-strategic-planning-capacity-building-and-assistance-initiativ.aspx (Download time: 29.01.2023.)
9 ENISA Threat Landscape (ETL) (2022): https://www.enisa.europa.eu/publications/enisa-threat-landscape2022/@@download/fullReport (Download time: 29.01.2023.)
10 A. FEHÉR: Artificial Intelligence in cyberspace 2. - Realizing cyber attacks with AI, American Journal of Research, Education and Development, 2019/4.
11 A. GURTOV, T. POLISHCHUK, and M. WERNBERG. Controller-Pilot Data Link Communication Security. In: Sensors (Basel) 18.5 (2018). DOI: 10.3390/s18051636.
12 S. ESKILSSON, H. GUSTAFSSON, S. KHAN, and A. GURTOV: Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio. In: 2020 Integrated Communications Navigation and Surveillance Conference (ICNS). 2020, 1B2-1-1B2–9. DOI: 10.1109/ICNS50378.2020.9222945.
13 A. LEHTO, I. SESTORP, S. KHAN, and A. GURTOV: Controller Pilot Data Link Communication Security: A Practical Study. In: 2021 Integrated Communications Navigation and Surveillance Conference (ICNS). 2021, pp. 1–11. DOI: 10 . 1109 / ICNS52807.2021.9441649.
14 Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA, 7. évf. 8() pp 35-50, 2009, ISSN 1785-1181, Downloaded: 14. 01. 2023.
15 Négyesi Imre: Az információgyűjtés jövőképe, Hadtudományi Szemle, 1. évf. 3. szám, pp 95-100, 2008, ISSN: 2676-9816-20-60-0437
16 M-S.B. MAHMOUD – N. LARRIEU and A. PIROVANO: An aeronautical data link security architecture overview; Digital Avionics Systems Conference. p. 4A., 2009, 4-6.
17 https://www.sigidwiki.com/wiki/VHF_Data_Link_-_Mode_2_(VDL-M2) (Download time: 04.02.2023.)
18 A. SKOGLUND and A. WESTERGREN: Intrusion Detection For The Controller Pilot Data Link Communication – Detecting CPDLC attacks using machine learning, Linköpings universitet

Bachelor’s thesis, 2022.STATISTA: Countries and regions with the highest number of fatal civil airliner accidents from 1945 through February 28., 2022, https://www.statista.com/statistics/262867/fatal-civil-airliner-accidents-since-1945-by-country-and-region/ (Download time: 18.01.2023.)

19 M. STROHMEIER : Security in Next Generation Air Traffic Communication Networks; Oxford University, 2016.

20 Rikk János Kutatásmódszertan, Budapest (2014) ISBN: 9789630894951

21 B. D. SZÁMEL and G. SZABÓ: Légtérkapacitás számítás elméleti modellek alapján; Repüléstudományi Közlemények, XXVI. 2. p. 2014., 298-318.

Dr. habil. NÉGYESI Imre PhD. egyetemi docens[15]
Nemzeti Közszolgálati Egyetem, Informatikai Tanszék

e-mail: Negyesi.Imre@UNI-NKE.HU

Physical security of critical installations

Abstract:

If a high-priority facility is planned, several protective measures must be taken. In this publication, I will walk through the physical security factors of a high-priority facility. Before moving on to the physical security of high-priority installations, I will clarify the concept of high-priority installations themselves in the introduction. In the following, we provide a detailed overview of the principles and tools of physical protection.

Keywords:

ARTIFICIAL INTELLIGENCE, SOCIETY, COGNITIVE INTELLIGENCE, MILITARY RESEARCH

Introduction

The term 'installation' is used to refer to real estate built on or below the surface of the ground, in a building or complex of buildings. Within the vital facilities, we can distinguish three main groups based on the main aspects:

- In terms of ownership, there can be privately owned, state-owned, municipally owned, foreign-owned, or owned by various companies.
- In terms of their function, the facilities may be administrative, judicial, prosecutorial, police, defence, national security, industrial and agricultural, commercial, health, social, energy, financial, IT, nature conservation, environmental, or facilities supporting various productive activities, as well as logistics centres, industrial facilities, warehouses, office buildings.
- In terms of security protection of facilities, they may be the Hungarian Defence Forces, Parliamentary Guard, Police, National Security Services, Armed Security Guard, Private Security Services, or facilities guarded and protected by security systems.[16]

Grouping of vital facilities

After this, the concepts around which the analyzes of the publication are grouped follow.

Outdoor physical protection

After clarifying the concept of priority vital facilities, let's take a detailed look at the principles and means of protection. Within this, we start with the examination of outdoor physical protection. The

[15] ORCID: 0000-0003-1144-1912
[16] CLXVI of 2012 on the identification, designation and protection of vital systems and facilities on the further division of the listed aspects. provided by law.

basic purpose of outdoor physical protection is to prevent and make it difficult for unauthorized access to the facility to be protected. There are several forms of outdoor physical protection solutions:

- trenches;
- fills;
- fences;
- gates;
- barriers;
- roadblocks;
- installed landmarks.

After this, the concepts around which the analyzes of the publication are grouped follow:

- *Trenches:* A steep depression in the land around the installation to be protected, designed to make access difficult.
- *Fills:* Artificially elevating the land around the installations to be protected to make access more difficult. The opposite of a ditch in terms of design, with the advantage of providing cover for part of the area to be protected.
- *Fences:* Fences are placed on the boundary of the protected site, delimit the protected area, prevent access, make it more difficult to enter and provide cover, thus making it difficult to see into the protected area. Fences built for property protection purposes are usually strong, sturdy, and difficult to climb. Fences can be made of wire mesh, metal netting, metal lattice, brick, stone, concrete or a mixture of these. To prevent climbing over, the top of the fence may be fitted with various damaging accessories (e.g., barbed wires, blades, pointed metal spikes) or the top of the fence may be tilted at an angle. They may also use electric property protection, electric security fencing to provide protection. An electric security fence is a security system that includes a property protection base fence on one side and an electric fence that is insulated from the base fence on the other side. An electric fence is a low-current, pulsed system of high-voltage wires that is incapable of extinguishing human life. The electric wires are placed on top of the base fence or on the inside of the base fence, on special insulating supports. The system can be fitted with various electronic sensors which, regardless of the weather, can sound an alarm in the event of touching, cutting or damage, or activate a siren, light signal, or surveillance system.
- *Gates:* Access for persons and vehicles is provided at entrances and exits. A facility may have multiple entrances and exits, which are physically protected by gates, barriers, and deceleration devices. Personnel access may be provided by standard doors, reinforced security doors, personnel gates, swing gates, swing gates, swing gates, swing gates, swing gates, sliding gates, sliding gates, swing barriers, which may be supplemented by access control systems, video surveillance systems, intrusion detection systems, building surveillance systems and intelligent building management systems.
- *Barriers:* Vehicle access is usually achieved by using barriers, which are now available in a wide range of versions, from low-cost, low-maintenance devices with a shorter operating time to heavy-duty, high lever-length, fast-acting barriers designed for extreme use. There are also easily breakable and drive-through proof barriers. The former is made of wood, the latter usually of metal.
- *Roadblocks:* There is also the simple road barrier, which is a traffic barrier post that can be lowered into the ground and lifted out, either electro hydraulically or electro pneumatically. A post that can be lowered to ground level can be used to prevent unauthorised access to the installation to be protected. Where a simple road barrier is no longer sufficient, a safety barrier

closing the entire width of the road should be used. It can be used for traffic control, traffic restriction and facility protection.

- *Installed landmarks:* Traffic control and traffic calming can also be achieved using various installed features such as planters containing trees.

Access control systems

At the end of the previous chapter, the physical protection systems that already use different "obstacles" and different IT systems in combination have already appeared. The access control system is an almost indispensable complementary element that effectively supports the protection of personal and vehicle access. The access systems used can be very diverse in design and principle of operation. The access control system identifies the person entering, determines the right of entry, controls passage by opening doors, gates, barriers and logs the event.

Access control systems consist of three basic functional units:

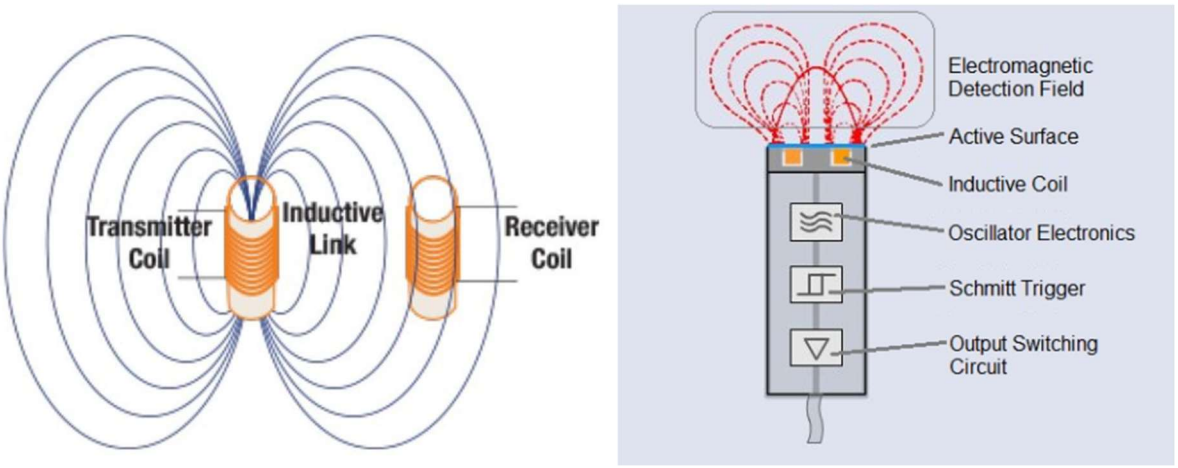
- a central unit;
- an identification unit;
- a passage control system.

The identification system is responsible for identifying the person or vehicle to be entered. In the event of identification, it sends an identification signal to the passage control system based on the authorisation. Identification may be based on stored data, by mobile identification device scanning, or on some biometric characteristic of the person entering. It is the task of the passage control system to determine, based on the pre-downloaded data, whether the person or vehicle entering belongs to the system and is authorised to enter the access point. After comparing the identification data received from the identification system with the authorisation data, the passage control system authorises or denies entry. If authorised, the access point is opened. An alarm signal is sent to the passage control system in the following cases: unauthorised passage, overstaying, activation of tamper protection.

The access information and any alarm signal shall be transmitted to the central unit, but the alarm signal may also be displayed directly on the passage control system. The passage control system shall receive control signals from the central unit or other external signalling systems. The control signals may instruct the passage control system to open (e.g., in case of a fire alarm signal or evacuation order enforcement) or to close (in case of an intrusion alarm signal or full lock enforcement). In case of failure of the central unit, the passage control system shall also be capable of autonomous operation. In autonomous mode, the passage controller shall store log files of access events, which shall be uploaded to the central unit when the connection is re-established. The central unit controls the operation of the access control system. The central unit is where the authorisation data, the operational data, the log files are stored and, if additional security systems are required, the connection is also made. Identification can be done using identification devices, usually assigned to a person or vehicle and encrypted. The access system identifies the person or vehicle to be accessed by scanning the code. The identification device carries the characteristics of the person or vehicle to which it belongs. Identification devices are usually linked to an individual or a vehicle and may not be transferred to another person. It is usually small in form, easy to handle and can be produced in large quantities at low cost. In terms of type, they may be bar-coded readers, in which case the narrow and wide lines and the size of the gaps conceal a numeric or alphanumeric code. The bar code is read optically.

Identification can be done by contactless identification, which is becoming more and more common today. This method uses electromagnetic waves to transmit data. The readers create an intermittent or continuous electromagnetic field around themselves, into which, when the

identification card is inserted, its antenna picks up the interrogation signal, which is processed by a chip in the card, which then emits the response signal and the code, thus transmitting the data necessary for identification. The carrier devices used for this purpose can be either active or passive, depending on their energy supply. The difference between their operation is shown in the pictures in Figure 2.



2. Figure: Active and passive proximity architecture
IPLUS Magyarország Kft. *Tenforg Bt.*

The passive proximity card does not have its own power source. It draws the energy needed to transmit information from the electric field emitted by the reader. An active card has its own energy source, has a longer range and is more protected against various electromagnetic disturbances, but the charge level of the energy source must be monitored. The memory capacity of the chips is hundreds of times that of magnetic cards and can be rewritten multiple times. Stored data can be grouped, isolated, and encrypted using different management software. Contactless IDs are less prone to contamination and have a longer lifetime because they do not wear out during use.

Access can also be granted by PIN[17]. In this case, the PIN code for access must be entered on the keypad of the access control system. It is less used today, because the numbers chosen often contained easily decipherable content (e.g., year of birth, repetitive numbers) and people tended to forget more complex PINs. The big advantage, however, is that it cannot be forgotten at home. Nowadays it is more often used in combination with contactless IDs.

Access cards, devices, can be abandoned, forged, PIN codes can be guessed, i.e., compromised. The most important task of access control systems is to identify the person authorised to enter without any mistake. The most appropriate form of identification today is biometric identification. "There are as many people as there are people!" they say. Each person has unique biological characteristics, which makes them the perfect means of identification. However, biometric identification has only become possible with the development of computers, as special readers are needed to electronically convert unique biological characteristics and the storage of biological characteristics requires significant storage capacity. Identification can be based on fingerprints, geometric features of the hand, retina or iris of the eye, voice characteristics, or thermal imaging. Recent developments include various facial recognition technologies. Access control systems are usually complemented by live guard protection.

Surveillance cameras

[17] PIN: Personal Identification Number

The use of CCTV systems increases the public's sense of security. In addition to monitoring and recording an act or crime, CCTV can also serve as a deterrent. Preventing crime and intrusion is generally a more cost-effective procedure than repairing the damage caused.

The services provided by the World Wide Web and computer networks make it possible for users and authorised users to view the image of a particular camera system from anywhere in the world. Camera systems installed for asset protection purposes can be used for various purposes. The application possibilities of asset protection systems can be quite broad. These include:

- store goods protection
- bank security
- payment point monitoring
- site protection
- public space, surveillance system
- addition of passenger and vehicle entry
- addition of property protection alarms
- protection of family houses
- addition of remote monitoring

Other possible uses of the systems installed for monitoring people and objects can be listed as follows:

- traffic management and control
- motorway (number plate recognition)
- production and quality control
- building management
- investment monitoring and documentation
- entertainment industry cameras
- nature observation

Based on their operating principle, cameras can be digital or analogue. Analogue camera systems are nowadays becoming increasingly rare due to the rapid spread of digitalisation.
Digital camera systems can be operated by an application running on a computer, without the need for a control unit as with analogue systems. For a small number of cameras, an application running on a smartphone with internet access is sufficient. Today, a significant proportion of camera systems are wireless. A digital network consisting of several cameras and camera systems can record and save images from different cameras on a remote server. High level encryption and encoding can be applied to the digital system.

Different types of surveillance cameras:

- Panel camera;
- Tube camera;
- Compact kamera;
- Infrared LED camera;
- Box camera;
- Fixed dome camera;
- Speed dome camera;
- PTZ swivel stool camera;
- Special cameras.

A variant of surveillance cameras that can also be used at night is the night vision camera. Initially, night vision cameras operated in black and white mode without infra-red illumination, with possible software image enhancement. Today, a significant number of night vision cameras have infrared illumination. In night vision cameras, the switching on of the infrared lights in low visibility conditions is usually controlled by an automatic light sensor. As daylight approaches and visibility improves, the lights are automatically switched off. In darkness, sudden strong light changes, for example when a flashlight or a strong infrared light is used to illuminate the night vision camera, can cause the camera image to completely fade and obstruct the observation. In case of adverse weather conditions (rain, fog) the image quality may be degraded. Image quality can be improved by using higher resolution cameras with higher light sensitivity, or by using higher power, controllable supplementary infra-lighting.

Today, surveillance systems are mostly based on intelligent video surveillance systems. Intelligent video cameras are equipped with features that allow them to perform various automated tasks, thus facilitating the work of the observers. Intelligent cameras can have analytical functions such as: motion detection, camera tampering protection, line crossing detection (virtual fence), face detection, abandoned (foreign) object detection, sound detection, running detection, direction of travel detection, shape and form recognition, missing object (theft) detection, license plate recognition, congestion detection, traffic counting. The advantages of automatic analysis of video recordings are that the observer's work is significantly simplified, and a more efficient, faster and more accurate search of the saved video content can be achieved.

Since the GDPR2 came into force on 25 May 2018, data protection has been significantly strengthened. The data controller must clearly indicate to the person entering the area monitored by the camera, before entering the area monitored by the camera, that the area to be entered is the area monitored by the camera. This can be done in text, graphics, stickers, but the point is that it should be displayed in a prominent place. Surveillance cameras should not be used in places where surveillance would be offensive to human dignity, such as toilets, changing rooms, rehearsal rooms. Anyone recorded by a CCTV camera has the right to obtain a copy of the

Intrusion detection systems

Intrusion detection or alarm systems are part of physical security, their purpose is to alert the live protection or to delay or prevent intrusion until the live protection arrives. A properly and professionally installed alarm system will signal to the monitoring centre, where the live alarm is activated, at the moment of a breach of physical security. Alarm systems can be used in the following areas of protection: surface protection, area protection, protection of property, protection of persons. The list of devices for indoor alarm systems is as follows:

- opening sensor;
- glass break detector;
- indoor passive infrared motion sensor;
- indoor ultrasonic motion sensor;
- indoor microwave motion sensor;
- combined indoor motion sensor; indoor weight sensor; indoor vibration sensor; indoor infrared sensor;
- attack sidnal.

After the list, let's take a closer look at the different indoor alarm systems:

– *Opening detectors:* generally used to detect the opening of doors and windows (windows, doors, etc.). Opening sensors can be magnetic or mechanically operated. Magnetic switches have a

significantly better life and reliability than mechanical, micro-switches, but the micro-switch solution is more tamper-proof.

- *Glass breakage detectors:* they can be acoustic or contact detectors that can be glued to the glass surface. Nowadays, acoustic glass breakage detectors are mostly used. The main advantage is that they do not need to be mounted directly on the window and can be mounted anywhere within the radius specified by the manufacturer, but they may be less sensitive if obstructed by fixtures that prevent sound propagation. The more modern models are so-called dual sound detection, which can separate high component sounds from low frequency, high amplitude sound after the sound of breakage, and can also detect breakage of bonded and foiled glass.
- *Indoor passive infrared motion sensors:* they work in the same way as the outdoor version but can only be used indoors. It is passive, i.e., it does not radiate. It detects infrared radiation and heat from the environment. The more modern devices are equipped with tamper protection, i.e., when the detector lens is covered or painted, the radiation emitted by the active infrared transmitter in front of the lens is reflected back in the receiver and gives a detection signal.
- *Indoor ultrasonic motion detectors:* indoor ultrasonic motion detectors follow the Doppler principle in their operation. This means that the wavelength of the signal emitted by the ultrasonic transmitter changes as it approaches the sensor or is reflected off objects as it moves away, i.e. the frequency of the sound returning to the receiver changes, generating an alarm. Wind can produce false alarms and can cover a relatively small area.
- Indoor microwave motion detectors: they also work on the Doppler principle, but instead of ultrasonic waves, they use radio frequency waves of several GHZ. Radiofrequency waves penetrate windows, doors, and walls, so they may detect movement beyond the area to be protected, which can generate false alarms. They are most often used indoors where fixtures and fittings significantly reduce the effectiveness of ultrasonic motion detectors and intrusion from multiple directions is possible. Nowadays, they are mainly used as detection sensors for automatic doors, but their security applications are not significant.
- *Combined indoor motion detectors:* these alarm devices use a combination of passive infrared, ultrasonic and microwave motion detectors, taking advantage of the motion detectors' benefits, e.g., infrared is more sensitive to transverse motion, microwave is more sensitive to approaching and distant motion.
- *Indoor weight sensors:* they detect when the object to be protected is moved, usually using simple micro-switches as sensors.
- *Indoor vibration detectors:* the detector is placed on the surface of the object, room, room to be protected, the detector detects the vibrations, if the vibration exceeds a certain amplitude within a certain time, the detector gives an alarm. Drilling into brick, concrete and metal surfaces produces low frequency vibrations. For the protection of metal surfaces (vaults, safes), passive infrared sensors are also used to detect the use of a flame cutter or oxygen lance in the event of an intrusion.
- *Indoor infrasound sensor:* The indoor infrasound sensor consists of a transmitter, a receiver and a signal processing unit. The transmitter transmits sound waves at a frequency of a few times 10 Hz to the area to be protected. If any point in the protected area is disturbed, the characteristics of the reflected sound waves change, and the device generates an alarm via the signal processing unit.
- *Attack indicators*: also known as panic indicators. They can be manually operated push-button, switch, fold-down cover, or other type of intruder alarm. These devices are operated by hand, but there are also pedals and rails that are mounted on the floor or on the underside of a table and operated by foot. The advantage of this is that the alarm system can be activated even with raised hands in the event of an attack. There are optical intrusion detectors, usually placed in cash registers. They may be of transceiver or photo-sensitive design. The receiver is normally covered. However, if a concealed object such as a stack of coins is moved and light hits the photo-resistor,

its resistance change generates an alarm after a delay of a few seconds. The transceiver unit is used where the environment is not adequately illuminated. The transmitter is positioned so that sufficient light reaches the receiver. Its handling and operation is similar to that of photo-sensitive intrusion detectors.

The next type is the radio attack alarm, which generates an alarm by pressing the radio transmit button built into the device. These are usually mobile devices with a range of less than 100 metres. As technology has developed, radio attack beacons have become smaller and smaller, can be disguised as a ballpoint pen and can fit comfortably in a pocket. A special version is also equipped with a tilt sensor so that if the guard falls, an automatic alarm is triggered.

Alarms can be generated on site, in a remote monitoring centre, or silently or audibly. A silent alarm does not disturb the intruder and is therefore easier to detect, but the nearby environment is not aware of the alarm or the intrusion and cannot take the necessary precautions. Although a loud alarm alerts the nearby environment of the breach and usually deters the attacker, the attacker may take a defensive posture, take hostages, and possibly act rashly. In addition to a local alert, the alert can be forwarded to a specialised remote monitoring company. The transmission can be done by wired or wireless radio frequency.

Summary, conclusions

In this publication, vital systems are referred to in CLXVI of 2012 on the identification, designation and protection of vital systems and facilities. according to the law. It has been said that if a facility of high importance is planned, more protective measures must be taken, so we looked at what physical security factors a facility of high importance might have. In the following, we provide a detailed overview of the principles and tools of physical protection, with the help of which the physical protection of facilities can be implemented. In addition to the collection and transmission of information, the examined systems and devices can create an opportunity to add artificial intelligence to the protection toolbox in the future.

References:

Act of 2005. CXXXIII., „jogiportal.hu,” Online: http://jogiportal.hu/view/ the-personal--and-property-management-as well as-private-investigation-activities-szabalairol-solo-2005-evi-cxxxiii-tv, Downloaded: 28. 01. 2023.

„Automation-insight.blog,” Online: https://automation-insights.blog/2014/03/05/basic-operating-principle-of-an-inductive-proximity-sensor/, Downloaded: 28. 01. 2023.

„BIZTOM Safety technology,” Online: https://biztom.hu/ construction of alarm systems, Downloaded: 15. 01. 2023.

„G-MAX,” Online: https://outdoor-perimeter-security.com/ Downloaded: 14. 01. 2023.

Gabriella Tasnádi, „National Chamber of Agriculture,” Online: https://www.nak.hu/ informative-service/coronavirus/101520-what-is-a-critical-infrastructure, Downloaded: 27. 12. 2022.

György Fialka, dr. Sándor Kovács, dr. András Márton, dr. Mária Márton: Facility protection, Publisher: University of Public Service, Budapest, 2014. Downloaded: 14. 01. 2023.

Négyesi Imre: A megfigyelés és információgyűjtés múltja, jelene és jövője SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA, 7. évf. 8() pp 35-50, 2009, ISSN 1785-1181, Downloaded: 14. 01. 2023.

Négyesi Imre: Az információgyűjtés jövőképe, Hadtudományi szemle 1 3 pp 95-100 (2008), ISSN 2060-0437, Downloaded: 14. 01. 2023.

„IP Security Camera,” Online: http://www.ipbiztonsagikamera.hu/index.php/ camel backs/camera systems, Downloaded: 28. 01. 2023.

„IPLUS,” Online: https://iplus.hu/ business clients/surveillance systems, Downloaded: 28. 01. 2023.

„Soselectronik.hu,” Online: https://www.soselectronic.hu/articles/sos-supplier-of-solution/nfc-technologia-7-pontban-2281, Downloaded: 23. 02. 2023.

„Remote connection,” Online : https://mek.oszk.hu/11100/11104/html/DEFIN/DOPPLER.HTM, Downloaded: 14. 01. 2023.

„ZMAX,” Online: https://zmax.hu/ product category/professional-cultural-wear/two-position-microwave-motion sensors, Downloaded: 14. 01. 2023.

POSSIBILITIES FOR FURTHER DEVELOPMENT OF THE DISASTER MANAGEMENT AUTHORITY SYSTEM

Bence Roland Lakatos – Gyula Vass – László Teknős

Abstract

Transparent, accessible and stable public administration is essential for the internal and external security of all countries. The author seeks to define the path to success for the disaster management organisational system and, more broadly, for public administration itself. Particular attention is paid to both the role of the service state and the characteristics of the systems used. By analysing the data obtained from the research methods to be implemented, the author intends to draw conclusions that will help to improve effectiveness and efficiency. The author intends to measure the costs per case based on the methods he applies and to make public administration more efficient through his proposals.

Keywords: e-governance, disaster management, Industrial 4.0, IoT, efficiency

Introduction

During our research, we aimed to examine the possible methods of increasing the efficiency of tasks carried out by official disaster management systems in Hungary. The methods of increasing efficiency are examined through the applicability of smart services. On the one hand, the official side, while on the other hand, the residential side is analysed.

The objectives of the research include the need to increase security and to research the sustainability of the existing levels, as the increase in the number of facilities posing a potential threat, as well as the constantly emerging new challenges (climate change, migration, pandemic, shortage of raw materials, war, energy crisis, and so on) increase the demand for quality work of the authorities and the examination of continuous improvement opportunities. The examination of systemic resilience is prioritised in the professional disaster management organisation system, as our ability to withstand the ever-changing modern world must be properly adapted to new challenges, as a unified safety net.

The way to e-administration within the service provider country through industry 4.0

People of our time can see the rapid digital development, which is due to the 4th Industrial Revolution, and even, according to some research, the 5th Industrial Revolution due to robotics. *'[...] the technological development agents of Industry 4.0 are an integral part of all sectors of a well-functioning state, whether public, corporate or private, paying particular attention to the search for continuous innovations aimed at creating security and making existing ones more efficient.'* [1] In this wave of development, it is also essential that the provision of State tasks itself undergoes a kind of development, which has

resulted in the completion of electronic, i.e. e-public administration.

The role of the state in the expansion during Industry 4.0 development and development opportunities is essential, since it is involved in the process at all levels, from the legislative process to the implementation side, and can promote but also hinder positive changes, as the state has to stand behind and not in front of innovations from the service and private sectors in such situations. A well-functioning public administration system must inevitably perform service tasks as well. The following figure shows the relationship between the participants of the public administration system and the client.

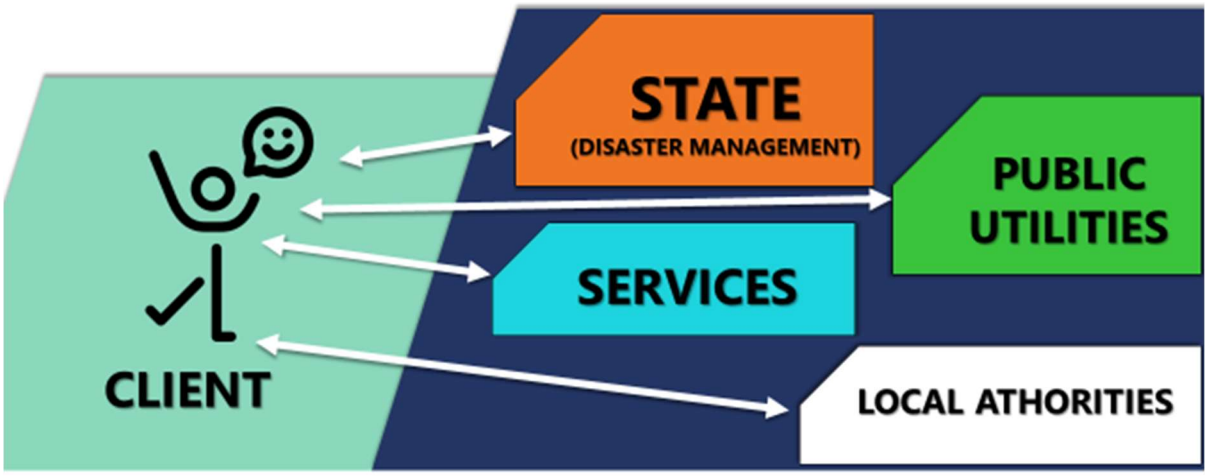


Figure 1. The relationship between the client and other participants (created by authors)

Figure 1 shows the client in contact with the state, local authorities, utilities and service sectors. Although the place of disaster management was shown in the figure in an organisational approach, we can say that considering the scope and tasks, we cannot only include it here since in the case of Public Utilities, the temporary provision of the public service of providing waste management, the administrative tasks of water protection, including water quality protection, or damage prevention tasks are also included. Further analysing the case of local governments, let us think about the public safety representatives who assist the mayors in the fields of civil protection, Industrial Security, and even fire protection. In particular, to ensure the public's safety, the competent Department of Disaster Management carries out market surveillance procedures in relation to construction products, fire-technical products and carbon monoxide equipment. A complex system requires a complex approach. All segments of public administration penetrate our lives, which is why e-public administration needs to be efficient and sustainable. [2] The development of e-public administration has also brought along technologies, processes, regulations, and conditions affecting the work of the organisation used so far in the field of disaster management to undergo a continuous wave of changes. The impressions and expectations of the e-administration on both the public and the client's side were examined with questionnaires. The following figure summarises the results and lists the most significant advantages and disadvantages.

Figure 2. Advantages and disadvantages of E-administration (created by authors)

Advantages include increasing efficiency, cost-effectiveness, quickness, permanent access and simplicity. Increasing efficiency also comes from ensuring that information is shared and accessed immediately. By expanding efficiency, it does not equal effectiveness, since in the case of efficiency it is necessary to examine the results and the costs in parallel since it is possible to examine both sides (achieving a specific goal with the minimum energy expended, achieving the highest results) in this way. Cost-effectiveness, as an indicator of efficiency, means public savings resulting from paperless processes (it is free of printing and paper producing costs) and meeting clients in person (human resources: administrative and security personnel salary costs, operating costs of buildings used), is reflected on the benefits side. Quickness refers to the immediate use of available services (broadband, reliable and fast optical wires are also crucial in this area). Permanent access was also highlighted in the conducted questionnaires, as the system, in the case of automated systems, is accompanied by an immediate administration opportunity. Simplicity, as another key advantage e-public administration systems should have, means the system can be used on a transparent interface, conveniently, without having to go anywhere. As for disadvantages, it was indicated several times that the surface feels inconvenient and distracting, cumbersome, overcrowded, and non-transparent. This is due to what is called the lack of white space surface, i.e. the lack of transparency and looseness. The lack of physical connections also appeared as a problem, since during the application of these systems the direction of connection fades into the background, and in many cases, it is completely lost. Another disadvantage is the lack of consistency and responsiveness, which is the guarantee of the neutral surfaces of the used device, i.e. everywhere (PC, mobile [iOS, Android, Windows Mobile OS, Blackberry Mobile OS], tablet, etc.). A uniform user and authority management interface, and a uniform image should be available.

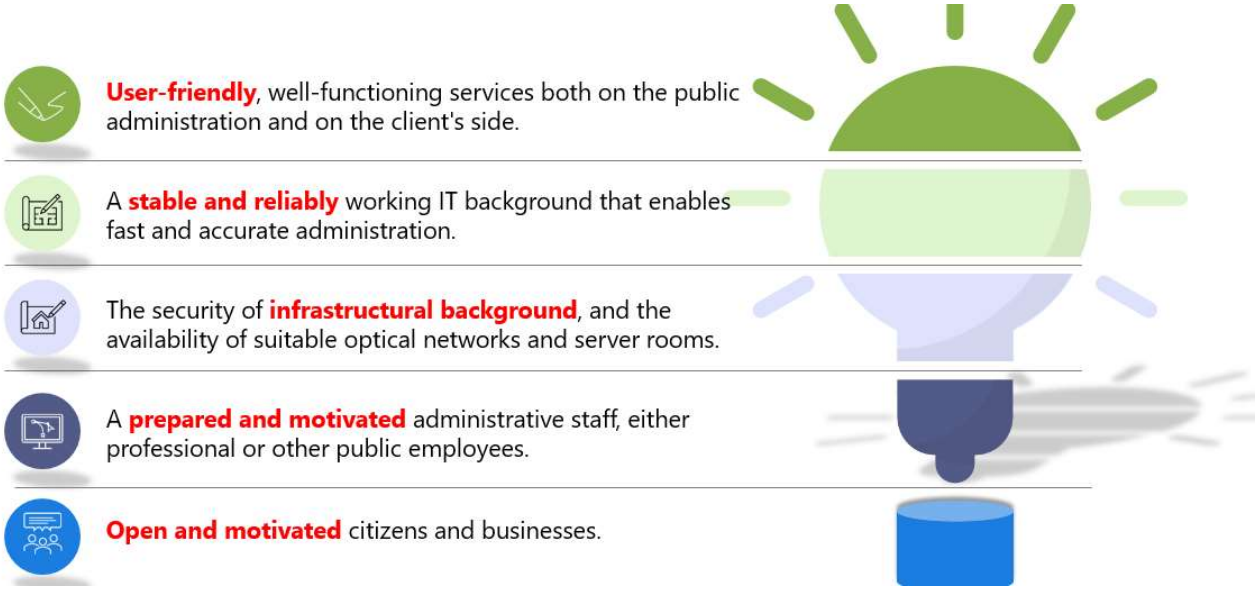


Figure 3. Successful and Efficient E-administration (created by authors)

In addition to reducing the above-listed disadvantages for the operation of public administration, the aim is to increase the number of advantages. What is, however, needed for an electronic administration system to be efficient and successful? First of all, there is a need for software and application with a user-friendly interface, which takes into account, from the side of those performing authority tasks, that it should be transparent, reduce administrative burdens, and at the same time help clients to access the necessary data while guaranteeing the transparency of business processes without IT knowledge. Stability and reliability are also important characteristics since accessibility and reliability must be guaranteed both on the authority and on the client's side, and for this, an appropriate infrastructure background is also required. The infrastructural background includes the use of a set of electronic, electromechanical and mechanical equipment, i.e. computers, laptops, and phones (hardware), both on the user's and authority's side, which is capable of running a program or application (software) that appears as an intellectual product performing the function of a defined e-administration. Among the theses developed by John von Neumann in 1946 was the universality of computers as a principle.

No special equipment should be required to perform the tasks, but the most widely available configurations should be able to run smoothly and without obstacles on operating systems. [3] In fact, for every organisation-level change, it is essential to prepare and train the workforce, in this case, the public administration staff, at the appropriate level, and to ensure motivation for the application of the new system. Once these are obtained, the last element becomes absolutely necessary, which can be considered one of the most important ones, namely, the existence of openness and motivation for the application of the new system on the part of citizens and businesses. The grassroot structure of these is essential for an innovative process improvement system to contribute to

successful and efficient e-administration. [4]

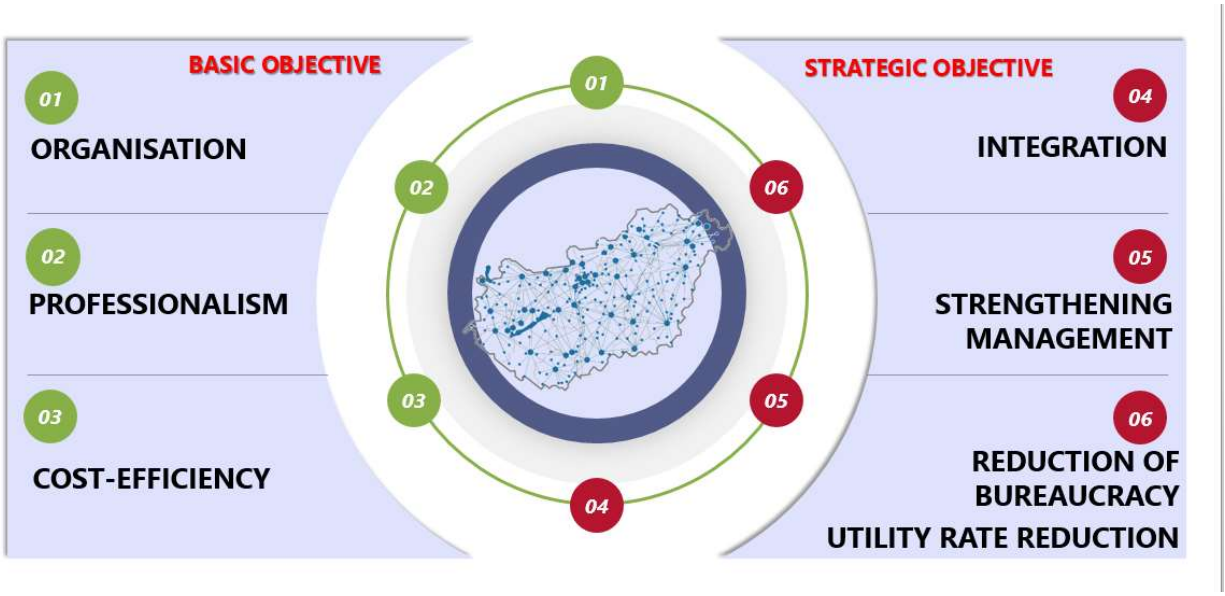


Figure 4. Basic and strategic objectives of the service state (created by authors)

As could be seen in the relationship between clients and other participants, in terms of location and in order to increase trust in public administration itself, there is a need for authorities located within the state administration, which are not only marked as 'service providers', but also a service provider state structure. The client is in the centre of the state system of providing services, and the state must play a role in eliminating all obstacles, be they physical, electronic, long-distance, digital, etc. Figure 4 depicts the basic and strategic goals that are broadly related to the state and in a much narrower sense can be also used to analyse the organisation of disaster management in Hungary. Organisation is put as the first basic objective since it is crucial to share tasks, powers and competencies as rationally as possible, and to this end, it is necessary to carry out centralisation and decentralisation in the departments of public administration.

In this case, the structure can be divided into central, regional, and local levels and other organisational units which is a well-established system in terms of competence. Professionalism is also a priority goal, as professionals working in public administration must have a national dedication for what they do, professional and up-to-date knowledge, and carry out their work along ethical and motivated goals. Cost-effectiveness as a basic objective means that organisations should do the work with the lowest possible administrative burden, minimum service fees and shortening of administrative deadlines. As for strategic goals, three should be highlighted, which are strengthening management, reducing bureaucracy and the related reduction of public utilities. Integration is of paramount importance since the integrated approach of authorities brings special advantages at the systemic level, and based on this, an effectively organised state administration system becomes feasible. In order to increase efficiency, strengthening the management approach is also considered strategically important, since with the

appropriate level of task-oriented sharing of the human resources available to us, a manager-oriented structure becomes available, in which the application of brainstorming is also a priority task. [5] The third objective is the reduction of bureaucracy and the reduction of utility costs since it is essential to implement deregulation in the procedural and material environment of public administration, as well as in the legal environment of organisations. The state-level reduction of public utility costs is also an important aspect since the public sector has significant dimensions, so the goal is to minimise the energy consumption of the tools, machines, technologies and processes used, and with possible innovative investments, footprints can be reduced at a realistic rate of return. Providing and establishing e-public administration as an employed service provider task may be assured at an appropriate level by the end of the second decade after the turn of the millennium. The goal is to implement these systems and solutions that speed up and facilitate administration in accordance with arising new challenges. [6] In the course of this research, the analysis of the properties of the systems was carried out, and during the examination of the possibility of developing an application called Intelligent Control, the found requirements for the applied systems are simplicity, quickness, being up-to-date, accuracy, transparency, and efficiency. [7] However, as a result of the events that have taken place in the world in a short period of time, a new approach can be introduced from a new point of view. The seventh most important feature, namely, cost-effectiveness means the system used must be cost-effective and sustainable.

In the 1990s, Mathis Wackernagel and William Rees defined the conceptual elements of the ecological footprint and developed a method for calculating the load. [8] These metrics were the basis of the analysis of resource and energy requirements during the examination of sustainable development. These principles and methods can also be applied during the examination of public administration in the applied systems, devices and workstations.

Cost-effectiveness in the context of the operation of the applied specialist systems means that their function can be fully fulfilled even with minimal energy requirements, which means minimising the ecological footprint of public administration. This should be a priority objective of all research and examination related to official activities. The other one is sustainability, which means that by the choice of the systems and methods used, while minimising the resources to be spent on a case, security can be guaranteed while taking into account the needs and interests of the client so that the characteristics of providing a service can prevail. This suggestion can be viewed as the greening process of public administration.

Proportion of energy costs of administration

Galileo Galilei, an Italian philosopher of the 16th century, whose work has produced significant results in the fields of physics, astronomy, mathematics, and natural sciences, said and wrote 'measure what can be measured, and make measurable what cannot be'. Implementing this idea, the research touched upon the task of determining the proportion of energy costs of administration in the performance of official tasks of professional disaster management bodies, since almost everything in our world can be measured, and what cannot, can also be measured

in the end. This provides an appropriate basis for comparison to draw certain conclusions. It is possible to measure what tools are used by staff performing official activities, how long they run per working day, and the amount of official work itself can be measured as well. Based on this, the unit fraction of working capacity can be calculated. In order to calculate the energy cost ratio of the administration, it is necessary to sum up the data of all workstations serving authority activities powered by electricity, divided by the delta value of the working time expressed in hours. The energy demand, power, and thus the value of P can be obtained by dividing the sum of the energy changes and the change of time. Eta, i.e. efficiency, is obtained by dividing the value of P by the value of Q, i.e. how many decisions were made during a given work time. EH, as the energy cost ratio indicator is obtained by dividing eta and the electricity price by the number of staff. The formula for the calculation method, alongside an explanation of the related abbreviations, is shown in Figure 5.

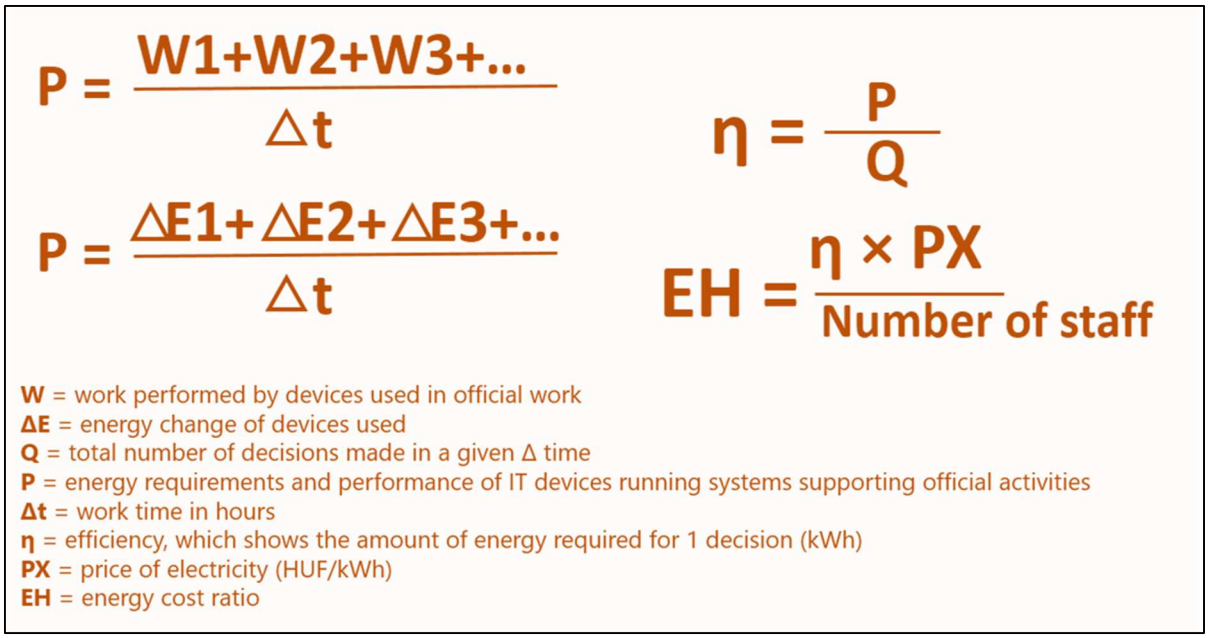


Figure 5. The formula of energy cost fraction of the administration (created by author)

Collection of data for the application of the above calculation method was carried out between 20 September - 28 October 2022 (30 working days and 9 legal holidays) and took place at the workstations of the Disaster Management Authority Department of the Szabolcs-Szatmár-Bereg County Directorate in Nyíregyháza. For the research, Gosound EP2 smart sockets were applied to each workstation in order to collect data. Each workstation is equipped with a PC with two monitors. During the research, a database was created, as a significant amount of data had been recorded, from which the correlations are being drawn, and the results are expected by early 2023.

Summary

In conclusion, in the system of professional disaster management organisations, authority tasks play a prominent role in the protection of the safety and protection of the population. The correlation between the participants of

the service-providing state and the clients was presented, as were the advantages and disadvantages of e-administration based on the data analyses carried out. In the case of the properties of the systems used, another property was defined, with two sub-properties, which were introduced as the concept of the greening process and the ecological footprint of public administration. Furthermore, the essentiality of ensuring resilience at the organisational level in order to make a difference and adapt was also brought to attention. The tools, applications, methods, and practices that can be developed, with minimal costs, with which efficiency, security, and stability can be further increased need to be found. Through the analyses of the data obtained during the research, the aim is to develop a work organisation methodology, the application of which in practice makes it possible to reduce the expenditure costs of the staff performing official tasks, however, the efficiency increase can be maintained, thereby reducing the ecological footprint of the administration itself.

References

[1] Lakatos, B (2020): A lakosság önvédelmi képességét javító tűzvédelmi applikáció vizsgálata, in: Hausner Gábor (szerk): Szemelvények a katonai műszaki tudományok eredményeiből II., Ludovika Egyetemi Kiadó, Budapest, p. 233.

[2] Cimer, Zs., Vass, Gy., Zsitnyányi, A. and Kátai-Urbán L. (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances, Symmetry, 13 (8). pp. 1-16.

[3] Hábermayer, T. (2020): Az ár- és belvíz elleni katasztrófavédelmi feladatok korszerű megoldásának lehetőségei, PhD dissertation, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar KMDI, Budapest, 239. p.

[4] Vass, Gy. (2017): Industrial Safety Training in Disaster Management Higher Education In Hungary. Pozhary i Chrezvychajnye Situacii: Predotvrashenie Likvidacia, 8: (2), pp. 80–84.

[5] Lakatos, B. (2021): Investigation of Smart Tools in Order to Improve the Effectiveness of the Administration of Disaster Management I. Belügyi Szemle, 69 (1). pp. 142–157.

[6] Teknős, L. (2020): Az éghajlatváltozás és a rendkívüli időjárás hatásaiból adódó katasztrófavédelmi feladatok kockázatalapú megközelítése. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, Budapest, 76. p.

[7] Lakatos, B. (2021): Presentation of the General Industrial Safety Authority Tasks and Powers, Belügyi Szemle, 69 (4). pp. 8-20.

[8] Wackernagel, M. and Gall, A. (2007): An overview on ecological footprint and sustainable development: A chat with Mathis Wackernagel, International Journal of Ecodynamics. 2 (1). pp. 1-9.

Dr. Bence R. Lakatos ff. major
head of department
Szabolcs-Szatmár-Bereg Country Disaster Management Directorate,
Nyíregyházi Disaster Management Office, Disaster Management Authority Department
Email: dr.lakatos.bence@katved.gov.hu
ORCID ID: 0000-0002-4934-3608

Dr. Gyula Vass
associate professor
University of Public Service, Faculty of Law Enforcement, Institute of Disaster management
Email: vass.gyula@uni-nke.hu
ORCID ID: 0000-0002-1845-2027

Dr. László Teknős ff. captain
senior lecturer
University of Public Service, Faculty of Law Enforcement, Institute of Disaster management
Email: teknos.laszlo@uni-nke.hu
ORCID ID: 0000-0003-0759-5871

ISSN 7234561-6