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 Content

Effectiveness of telemedical care for upper respiratory diseases during the COVID-19 pandemic

Márk Matusz MC HDF

prof dr. Gyula Kóródi NUPS

dr. Zsolt Fejes PhD MC HDF

Dr. János Rikk KJU

ABSTRACT

Upper respiratory diseases pose a significant health challenge for people and health systems. During the COVID-19 pandemic, the role and use of telemedical devices in health care has increased significantly. Possible benefits of telemedicine: Reduces Infection Risk, Availability and Access Improvement, Time and Cost Efficiency. The research uses the meta-analysis method to examine how telemedical tools contributed to relevant outcome indicators, such as improved patient access and physicians' work efficiency, reduction of workload on the health care system, patient safety, and so on. Overall estimate: the telemedicine group (treated) reached diagnosis in a significantly shorter time ($p<0.001$), the telemedicine group (treated) was able to treat significantly more patients ($p<0.0339$) and provide diagnosis. Egger's test results suggest no serious publication bias

KEYWORDS

telemedicine, COVID-19, availability, workload, effectiveness

INTRODUCTION

Upper respiratory tract diseases are pathologies that extend from the nasal cavity to the lower part of the larynx and in most cases are caused by viruses. These diseases are extremely common and occur widely throughout the world. Upper respiratory tract diseases pose a significant health burden, as they affect many people and often involve hospitalization and social costs.

Upper respiratory diseases pose a significant health challenge for people and health systems. These diseases are highly contagious and spread easily in mass community events, schools, kindergartens and workplaces. The congestion of hospitals and medical offices may increase during the period of this type of illness, putting a serious strain on the already burdened health systems.

Since the emergence of the COVID-19 epidemic, telemedicine - the delivery of healthcare by remote means - has made huge advances in healthcare services. Doctors and patients alike are using telemedicine options in epidemic situations, as it allows for the safe and efficient continuation of healthcare while minimising the risk of face-to-face encounters and infection.

During the COVID-19 pandemic, the role and use of telemedical devices in health care has increased significantly. With the help of these tools, healthcare providers enable patients to receive medical care and counseling from their homes, especially in the treatment of upper respiratory tract diseases.

Possible benefits of telemedicine:

1. Reduces the risk of infection: During a personal visit to medical institutions, patients are exposed to the risk of infection, especially in the waiting room and while waiting. Telemedicine offers the possibility for patients and doctors to consult without meeting in person, reducing the risk of infection for both parties.

2. Improving access and availability: Telemedicine makes it easier for patients, especially those living in remote or inaccessible areas, to access healthcare services. This improves patient access to medical care and expert counseling.
3. Time and cost efficiency: With telemedicine, patients do not have to travel to doctor's offices or hospitals, which saves them time. In addition, transport and parking costs are reduced. It also saves doctors time and costs, as virtual consultations make care more efficient and faster.

It is important to note that telemedicine may not replace face-to-face medical consultations in all cases, especially in cases where physical examination or additional diagnostic tests are necessary. Doctors should determine the condition of patients and the appropriateness of a particular case for telemedicine treatment.

Overall, telemedicine can provide a solution for the continuation of health services and the safe care of patients during the COVID-19 epidemic. With the development of available technologies, telemedicine becoming more widely available and accepted in the field of health care.

The aim of this research is to use meta-analysis to comprehensively evaluate and analyse the effectiveness and efficacy of telemedicine tools in the management of upper respiratory tract infections during the COVID-19 epidemic. The research examines how telemedicine tools have contributed to changes in relevant outcome indicators, such as improved patient access and physician work efficiency, reduced workload in the healthcare system, patient safety, etc.

Hypothesis

During pandemic Covid-19, the use of telemedicine teleconsultation and remote diagnostics functions in the healthcare process made healthcare more efficient for upper respiratory diseases (the most common disease among MH personnel).

METHODS

The meta-analysis makes it possible to summarize the results of previous studies in a comprehensive and objective way to obtain a more accurate picture of the effectiveness of telemedical devices and the development of the treatment of upper respiratory tract diseases during the COVID-19 pandemic. This can contribute to broadening knowledge and better decision-making for patients and healthcare providers. This research approach allows the results of different studies to be collected, compared and combined into a single, comprehensive study.

Literature research

In the literature search, we chose the keywords to find as many publications as possible, based on which we have a high chance of getting answers to our questions.

Keywords: upper traction respiratory disease, telemedicine, availability, workload, patient safety

- 'uppertraction respiratorydisease' the condition to be influenced, as defined by the leading symptoms, is easily understood by the patient
- 'telemedicine': which we are testing the effectiveness of in the cases mentioned above
- "availability", "workload" and "patient safety": which are expected to show the parts of the articles found that may contain useful data,

In which databases were searched: PubMed, Scopus, Web of Science

When did the search occur: 2023.

The search analyzed scientific publications specifically during the COVID-19 pandemic and in the period since then until the conclusion of the research.

Statistical methods

Since a medical scientific paper can only be published by supporting its findingswith data, the new findings should be based on systematic, pre-planned

data collection. These data should then be critically evaluated using statistical methods. A finding may be accepted as a new result if it can be supported by such evidence. However, this procedure has consequences. Statistical methods lead to probabilistic decisions, which follow the logic of hypothesis testing (t-tests, nonparametric tests, khi square tests, regression analysis, ANOVA, etc.) They may have a risk of error and may contain erroneous results despite a significant result. These should be borne in mind when processing them. It is necessary to specify the method for selecting the correct result from the communications that may contradict each other.

The meta-analysis

After the publication of several original papers, experts in the field have published a review article evaluating the results according to their own professional understanding. So the key to the "authenticity" of his publications was mainly the author's scientific experience and good foresight.

This is why the method of preparing summary communications emerged and is followed in the present work. One component of this meta-analysis:

All relevant data are collected from the original bulletins for each professional subject to the examination. These are necessarily similar test results, they can vary from different (measurement) methods, and so the numerical values and even the measurement scales may be different. The collected data cannot be compared with conventional statistical methods. That is why we need a meta-analysis, which is a set of statistical procedures comparing results from studies that are informative on specific issues, but which may be substantially different and may have been conducted in different settings. This is used to re-evaluate the test results presented in each publication using scientific statistical procedures that follow strict rules. We can then make findings that take into account all relevant published results and exclude the potentially subjective selection and/or weighting of different scientific ideas. The findings are based on the overall picture presented or demonstrated by

the data presented in published communications. The meta-analysis toolbox also includes procedures to detect and possibly correct errors and biases.

Typical issues and procedures of meta-analysis:

- Difference between the results of the control and the treated group: is the test group better than the comparison group?
- What is the effect of the treatment?
- Do any of the above results depend on some clustering factor or continuous variable?
- Is there an overall publication bias in the published results?
- Are there outcomes that differ greatly from the others in the publications?

For the first two types of questions, we estimate an effect average from published data. The random effects model should be chosen if the published results are obtained under different conditions, or even using different methodologies, or comparing results from completely different measurements. In this case, the estimated expected value is in fact an estimate of the average of the different expected values (several expected values) that are reflected in different test results. This requires different weightings to be given to different communications, mainly according to the different (statistical) reliability of the results reported. In this work, we mainly used raw data.

In the present work, Egger's test, the Duval & Tweedie trim and fill test and correction procedure were used to "measure" publication bias. In the Egger's test, $p<0.1$ is indicative of publication bias. And for the D&T procedure, we specify how many "missing" measurement data the procedure found, and the corrected estimate of the expected value that it calculates taking these into account.

This was done with Comprehensive Meta-Analysis (CMA) v3.3 (Biostat, Englewood, NJ USA) program. The data preparation and data collection is done with Excel, including the 'Wan at all' transformation calculations given in the Data Preparation subsection.

The meta-analysis results are reassessments of previously reported results. So they contain all the same errors as the original communications. As the methodology of meta-analysis itself is a set of statistical procedures, the results of these procedures may also be subject to risk of error and uncertainty. We should always make an effort to look for these sources of error and be aware that they exist and are likely to affect the results we use for our analysis.

Data preparation

For the meta-analysis calculations, the 3-figure data characteristics (mean, standard deviation, n) from the publications are given for both groups (control and treated groups). If these are not included in the communication, the median and the 2 other quartiles or the minimum and maximum values (or even all five numbers) are reported instead of the mean and standard deviation. In such cases, estimates should be made from these data. There are procedures proposed for this estimation, we used (Wan, X. at all, Estimating ... BMC Medical Research Methodology 2014 14:135-156).

Further preparatory counting is required if there are "before" and "after" results for both (control and treated) groups. In this case, we first determine the effect for both groups. This is similar to meta-analysis as determining the difference between the control and treated groups, only here we estimate the difference after - before (can be done using standard meta-analysis methods). The resulting estimated values are used for further calculations. We can compare these predicted before-trip differences of the control and treated group with the standard meta-analysis. Since this is also an estimate, it increases uncertainty. However, it makes use of results that would have to be excluded from the data due to improper data transmission.

It is also possible that none of the data descriptors required for the calculations (3 numbers or 5 numbers) appear in the article in numerical form, but are only presented in some kind of a figure. In this case, we can use the data read from the graph to avoid having to exclude the article due to lack of data. This procedure also carries more risk of error. One of them is the necessary inaccuracy of the

reading. Perhaps more serious is another: the notices sometimes confuse the concepts and data of standard deviation and standard error (S.D. and S.E.). This can be particularly the case in figures where it is almost impossible to see if the figure does not contain the deviation given in the accompanying text.

RESULTS

Definition of efficiency indicated in the hypothesis:

We considered a more effective care if

- the patient received a diagnosis in a shorter time
- the workload of the medical personnel has been quantifiably reduced
- quantifiable improvements in patient safety

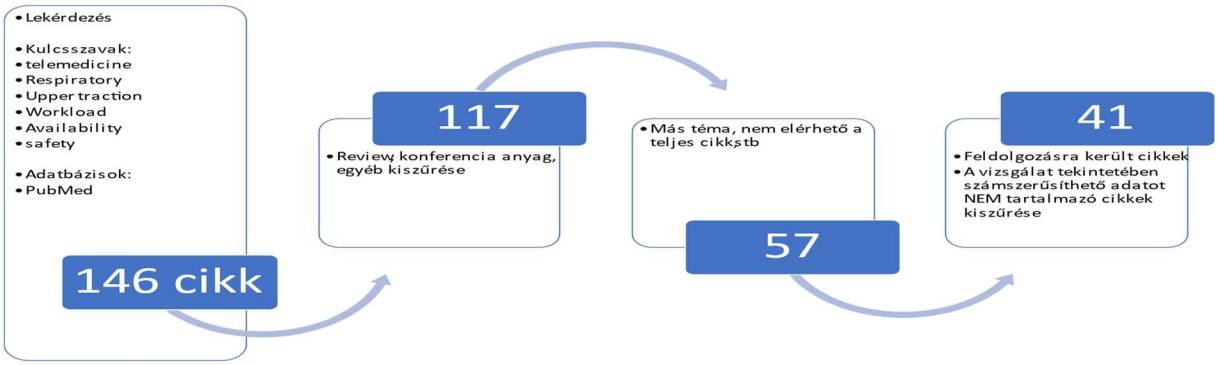


Figure 1. Literature search and article selection algorithm

The results of the search show that the topic is up-to-date, the number of publications is significant, and there is both military and civilian interest in the subject.

Data were collected article by article. The specification of data parameters varied from article to article. The papers also contained a number of data that were not relevant to the hypothesis. One important criterion in selecting the publications was whether they contained data of value to the study.

Sequences of numbers suitable for statistical processing were collected in a table in a form suitable for further processing. There were several times that the data

had differences in units of measurement, which were also matched for comparability.

Control — treated comparisons — Patient pathway effectiveness

Based on the data of the processed articles, I explicitly examined whether the use of telemedicine is an effective means of accessing the diagnosis, i.e. whether the patients received a diagnosis in a significantly shorter time thanks to some telemedical method.

I considered as the treated group those who used telemedicine and as the control group those who received a medical diagnosis in the traditional way.

Az összesített becslés: a telemedicinát választó (kezelt) csoport szignifikánsan ($p<0,001$) rövidebb idő alatt jutott el a diagnózisig.

Looking at the results of the individual articles, it can be seen that out of all the data, only 1 was significantly ($p=0.047$) better than the control.

For all the others:

better than control, but not significantly in 1 case,

- better than treated, but not significantly in 8 cases), finally

- significantly better in the 11 cases treated.

This review is important because in some of the original articles the data was not reported, the values could only be read from the figure, so there was no well-documented statistical comparison. So it is already a new result where there was a meaningful difference — article by article. Specifically: 19 out of 21 cases have better results in the treated group, of which 21 are significantly better. Thus, it is no wonder that the estimated average showed a significantly better treatment outcome.

Publication bias:

Egger's test result is $p=0.872$ so there is no serious publication bias.

Control — Managed Comparisons — Workload

For this question, I examined whether the use of telemedicine is an effective tool for reducing workload. The question can also be formulated indirectly, i.e. whether a significant number of patients were treated in the same amount of time thanks to some telemedical method.

I considered those who took telemedicine as a treatment group, and a control group who performed their health activities in the traditional way.

Overall estimate: the telemedicine (treated) group was able to treat and provide diagnosis to significantly ($p<0.0339$) more patients.

Looking at the results for each article, it can be seen that the treated group was better in all cases from all the data.

Publication bias:

Egger's test result is $p=0.797$ so there is no serious publication bias.

Control — treated comparisons — Patient safety

The number of articles included in the meta-analysis did not contain a sufficient number of reliable results regarding patient safety, so I ignored this aspect in the processing and evaluation of the results.

CONCLUSIONS

Our research goal was to find an answer to the question of whether telemedicine is effective in comparing the control-treated groups from the evaluable data of the filtered communications, not with the traditional rewiev evaluation, but by the method of meta-analysis.

Based on the data examined, the results of the meta-analysis of the data from the literature review we designed and conducted clearly show that telemedicine is a more significantly effective tool in reducing both the time to diagnosis and the workload of health care staff.

In both cases, the degree of publication bias was negligible.

The control-treated comparison answered the question of whether telemedicine is an effective method. At the same time, the degree of impact has not been determined, this requires further research. Within this, it is worth examining which group breakdowns may affect the results, but this will require a larger number of scientific papers to be reviewed.

REREFERENCES

The Effects of Explosion Propagation in the Environment

Miroslava Vandlíčková, University of Žilina, Faculty of Security Engineering, Slovakia,
miroslava.vandlickova@uniza.sk, ORCID: 0000-0002-3271-1603

Abstract

During the execution of military operations in the area of combat activity, soldiers are exposed to risk factors of the surrounding environment, which includes components containing explosive substances. The participants involved into an armed conflict use weapons and weapon systems to eliminate the adversary, which can also cause extensive material damage and casualties among the civilian population. Special equipment containing elements of ballistic protection is produced for military purposes to protect soldiers from possible injuries. However, each military technique, transport means and personal ballistic protection of an individual has its protection limits, which the adversary can overcome by oversizing the charge, appropriate placement of the charge or good tactics. [1] For these reasons, it is necessary to know the methods of using explosives and the effects of explosion propagation in the environment to that the article is addressed.

Keywords: explosion, shock wave, explosion heat, minimum explosion temperature, effects of shrapnels

Corresponding author: Ing. Miroslava Vandlíčková, Ph.D., vice-dean for education, University of Žilina, Faculty of Security Engineering, 1. May Street 32, 010 26 Žilina, Slovakia

Introduction

An explosion can generally be called as a transformation of the state of matter, which is accompanied by a sudden change of physical or chemical parameters, and during which a significant amount of heat and light energy is released. Detonation is an explosion with the release of energy at a speed higher than the speed of sound and is accompanied by the creation of a shock wave, while at deflagration the energy is released at a speed lower than the speed of sound in the surroundings. This fact is related to the amount of pressure that is created at the place of the explosion. Detonation velocity is the speed at which detonation propagates through an explosive. For loose industrial explosives it takes on a value of around 3,000-5,000 m/s, for plastic explosives, depending on the conditions, it has a value of around 3,000-7,000 m/s.

A shock wave is created during detonation as a result of the fact that the combustion products are not able to escape enough into the surroundings, and at the high explosion temperature reached, they are heated and compressed. During detonation the maximum explosion pressure reaches significantly higher values than during deflagration, which means that detonation usually has much more destructive consequences than deflagration.

Despite the fact that deflagration transition to detonation is theoretically possible, in practice in most cases, deflagration is caused by a thermal event, while detonation is initiated by a shock wave.

Chemical and physical principles of an explosion

According to the nature of the origin and progress, explosions can be divided into physical, chemical and nuclear. Physical explosions can be:

- kinetic (e.g. explosion of a flying meteorite),
- thermal (e.g. explosion of pressure cooker, pressure boiler),
- electrical (e.g. lightning bolt),
- elastic compression (e.g. frozen water in a bottle).

In addition to the shock wave, the explosion is accompanied by a sound wave, a thermal effect and the fragmentation of the material in the form of shards. The change in the internal energy of the system during an explosion is manifested by the performance of mechanical work associated with movement and a high increase in pressure at the place of the explosion. This property of the explosive is called the working capacity of an explosive.

In order for a chemical explosion to be occured a flammable substance (e.g. flammable gas, flammable liquid vapor, flammable dust), an oxidizing agent (e.g. oxygen from the air) and an initiation source (open flame, hot surfaces, mechanical sparks, electrical sparks, etc.) must be present in a system in parallel. If the concentration of a flammable substance in a mixture with air reaches the lower explosion limit (LEL), which is the minimum concentration of flammable gases, vapors of flammable liquids or flammable dust in a mixture with air, and the initiation source is able to provide sufficiently strong initiation energy, an explosion can occur.

A thermal explosion is caused by decomposition reactions and a sudden ignition, with a significant expansion of gases. For an ideal gas the equation (1) applies, where p is the pressure, V is the volume of the gas, n is the amount of substance given in moles, R is the universal gas constant and T is the thermodynamic temperature given in degrees Kelvin:

$$pV = nRT \quad (1)$$

The model of the explosion caused by the expansion of gases at high pressure best describes most explosions, because it assumes an adiabatic event, in which there is no exchange of thermal energy between the expanding gas and the surroundings due to the high speed of the explosion. Adiabatic expansion in the case of an ideal gas is governed by the relation (2)

$$pV^{\kappa} = const \quad (2)$$

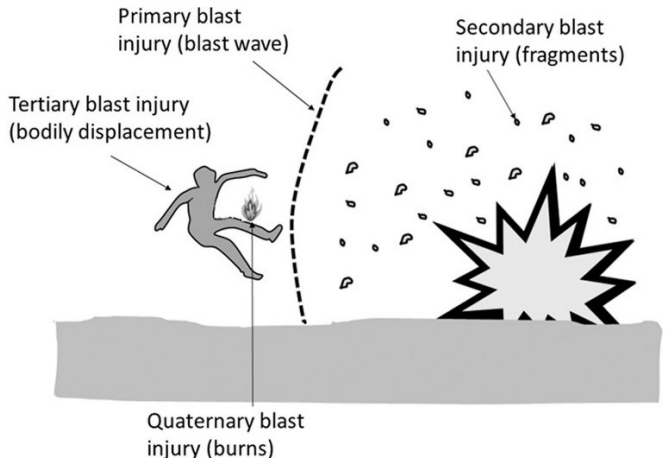
where κ is the Poisson's constant given by relation (3). C_p represents the specific heat capacity at constant pressure (isobaric process), C_v is the specific heat capacity at constant volume (isochoric process).

$$\kappa = Cp/Cv \quad (3)$$

The classical theory of thermal explosion is described on the basis of two approaches, where the first is the Semenov's theory, the second one is Frank-Kamenetsky's theory. Both theories complement each other in some aspects and thus form the basis for classic solutions to problems associated with thermal explosion.

Shrapnel effects

In addition to the action of the shock wave and the effects of the reached high explosion temperature on the affected organisms, fragmented shrapnel also have a significant effect, which, due to the action of the fragment effect, often cause injuries that have the character of gunshot or lacerations. [2]



1. *Figure: Blast injury types [3]*

The origin of the fragments can be of primary or secondary nature. Shrapnels are primarily formed from the basic parts of explosive decoy systems, such as the packaging, the initiation system or the explosive substance itself, and are most often of a metallic nature. [4] However, if there is damage in the vicinity of the explosion, e.g. window panes or other surrounding objects, equipment or parts of buildings, these can act as secondary fragments. The explosiveness B (or brisance), i.e. the ability of an explosive to cause a shattering effect, is clearly defined by the theoretical relationship (4),

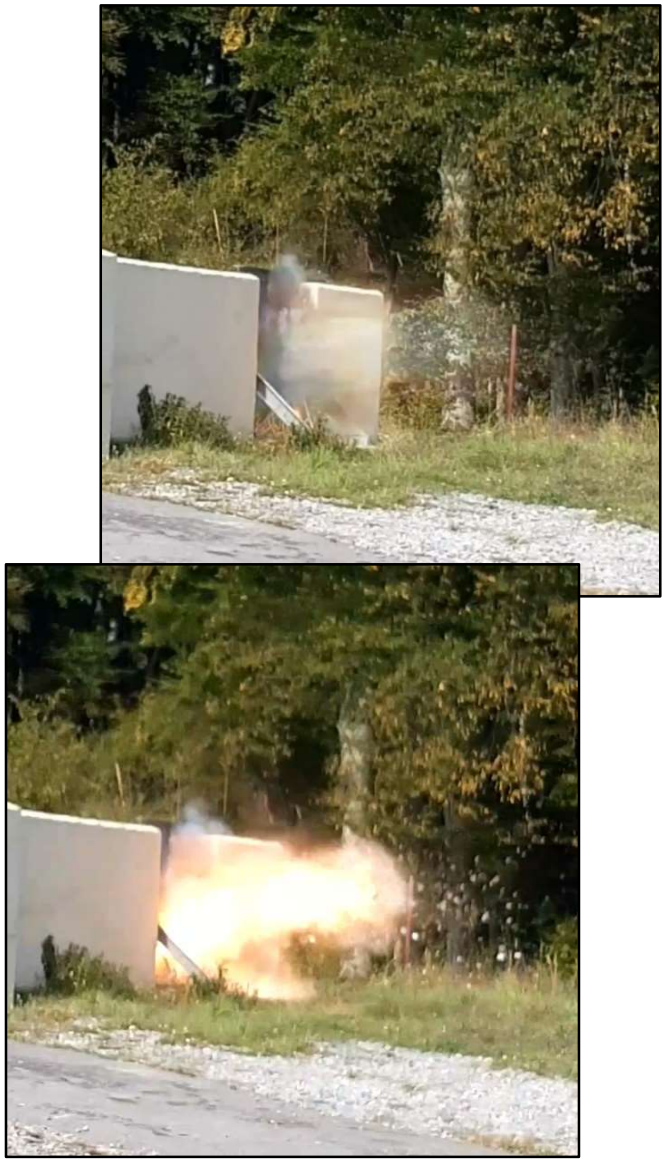
$$B = D.h.E \quad (4)$$

where D represents the detonation speed in m/s, h is the density of the explosive in g/m3 and E is the energy of the explosion, most often given in kJ/kg. However, the calculations of brisance show significant deviations due to the product of several quantities, the determination of which is mostly burdened with a certain error, therefore the brisance is often determined empirically, by experimental measurements. For example the frequently used Hess´s test for determining brizance is based on the principle of compression of lead cylinders during the explosion of a given amount of explosive.

The term explosive system implies that it contains a complex of elements, while it is capable of carrying out an explosive transformation of the contained explosive in a certain time and space. Explosive systems exist in various forms and designs from the simplest to complex structural complexes that differ in their components. The occurrence of improvised explosive systems - especially their initiation devices - is gradually expanding. [5]

For the armed forces, explosive systems are currently also important in connection with the so-called breaching, or urban breaching, which simply means forcible entry into the building in its weakened parts (e.g. doors, windows, etc.) by prying open the door, blasting the lock or using a bomb. In case of forced entry, of course, all the above effects of explosive systems must be taken into account. Photos created from a video capturing the explosion of the charge, on which a pressure wave, resulting in the curvature of the surface of building materials and their reversible deformation, are recorded, can be seen in the fig. no. 1 and no. 2. The photos also document a significant burst of flame accompanied by the release of a large amount of thermal energy and the achievement of a high explosion temperature, and last but not least, it is possible to see the fragmentation of flying shrapnel from the charge, surrounding building material, or door, or windows.

2. *Figure: Trapped pressure wave, flying shrapnels and curvature of the surface of building materials caused by the explosion of the charge placed in the door of the structure [1]*



3. *Figure: Pressure wave, burst of flame and flying fragmented shards of construction materials created as a result of the explosion of a charge placed in a weakened place of the structure [1]*

Conclusion

The products created in the explosion expand into the surroundings under high pressure and try to find equilibrium with the surrounding environment, which means that they try to equalize the pressure. The result is the formation of a shock wave. During its action and expansion, there is a rapid drop in temperature, because energy losses occur due to heating of the surrounding environment. Simultaneously with the temperature the pressure also drops that reaches high values only for a very short time (in the order of ms).

In addition to blast injuries, the effects of a shock wave can also often be observed on surrounding buildings in the form of a general surrounding of a building by a shock wave through the deformation of individual floors and construction up to the breaking of windows and window coverings.

References:

1. Hrnčiar B., Blahuta V., Vandlíčková M.: *Tactics and Medicine*; MediTak, s.r.o Žilina; ISBN 978-80-974270-0-9, p. 20-22.
2. Štefan, J., Hladík, J., [et all]. 201;. *Forensic medicine and its modern trends*; Grada Publishing a.s.; Praha; ISBN 978-80-247-3594-8.
3. Held Jade Team. Blast Injury; 2020; *Held Jade*; [online] ; [cit. 2023-07-24] ; Available at: https://healthjade.net/blast-injury/
4. Jangl, Š., Kavický, V., Figuli, L., Zvaková; Z. *Explosions, part II.* 2021; Žilinská univerzita v Žiline; EDIS UNIZA; ISBN 978-80-554-1812-4, p. 30.
5. Michalica, R. Methods and Means of Disposal of Explosive Systems; [online]. [cit. 2023-07-24] ; Available at: file:///C:/Users/mhole/Downloads/metody_a_prostriedky_cz%20(2).pdf

Information and data security in healthcare

Dr. habil. NÉGYESI Imre PhD, prof. dr. Kóródi Gyula

Abstract:

Technological advances and the widespread deployment of networked information systems are resulting in an increasing number of information and cyber security challenges, threats, and risks. The biggest challenge is to respond to incidents quickly, efficiently, and effectively within our capabilities, and information security awareness has become increasingly important. Information infrastructures face increasing threats, and protection requires ensuring the confidentiality, integrity and availability of data and information managed in electronic information systems. Healthcare processes generate a significant amount of digital information and data is one of the most important resources today. Healthcare stores many types of data that require advanced information technologies to manage, but these technologies also pose risks. Ensuring the integrity, confidentiality, and availability of data, avoiding incidents and data loss is a high priority and critical, so one of the biggest challenges in healthcare is to ensure an adequate level of data protection. As cyber-attacks against healthcare institutions are becoming more common, this article is devoted to an overview of this area.

Keywords:

HEALTH, INFORMATION SECURITY, DATA PROTECTION, CYBER SECURITY INCIDENTS

INTRODUCTION

As people's health information has become more and more sought after on the dark web, healthcare organizations are increasingly under attack and there is a need to ensure increased protection of personal and health data handled in the healthcare sector. Cybersecurity firm Trustware has set the black-market value of medical records at a record $250 per record. In contrast, a credit card number sells for $5. According to the Fundamental Law of Hungary, "Everyone has the right to physical and mental health." and "Everyone has the right to the protection of personal data". This requirement is in contrast to the value of the data, which makes the storage/processing of large amounts of health data in one place a very high risk. Data generated in the healthcare sector should be classified as sensitive data, subject to strict rules and protection is a priority. Compliance with data protection requirements is a key element of the legislation. In many countries, the digital evolution of healthcare has seen spectacular progress as a result of the COVID-19 phenomena. In these countries, digitalization has evolved over years in a matter of months under the pressure of the pandemic. However, ongoing digital developments have also brought the issue of security to the forefront, with patient data protection being ensured under a single set of guidelines and protection against cyber-attacks being defined as a core task. The year 2021 was a high year for health data incidents, with studies showing that a significant number of incidents were due to low levels of information security awareness among hospital staff.

Health information security is the assurance of the confidentiality, integrity and availability of data and information managed in information systems, and the full and continuous protection of the integrity and availability of the elements of the system. Information security is achieved through prevention, detection, early response, and incident management. In all areas of security, measures and activities shall aim at complex security.

CYBERSECURITY OF MEDICAL DEVICES

The vulnerability of medical devices creates opportunities for data breaches. Manufacturers and purchasers need to check not only the compliance of the devices, but also the reliability of the software, electronics and components that go with them. Healthcare providers should pay particular attention to the settings when purchasing used devices. Cyber-attacks exploit the vulnerability of IT systems, so professional maintenance and upgrade support for these devices is important. The latest medical devices are remote-controlled, and the security configuration and control software of the communication devices used for this purpose also make the health information system vulnerable.

Malfunctioning medical devices can put patients at risk, even to the point of life or death. According to a 2021 report by the ECRI[1] Institute (the independent authority on health technology and security), the main health technology threats will come from the proliferation of telemedicine, vulnerabilities in third-party software and remote operation of medical devices.

VULNERABILITY OF MEDICAL DEVICES

In this chapter, let's take a look at some examples of how big the vulnerability of medical devices was in practice, expressed as a percentage.

Research by Palo Alto Networks Unit 42 Threat Research found that 75% of infusion pumps, 51% of X-ray, MRI and CT equipment were vulnerable, and 20% of imaging devices were running unsupported versions of Windows. McAfee researchers analyzed 200,000 B.Braun infusion pumps, discovering significant vulnerabilities in two types that could allow attackers to deliver potentially lethal doses of drugs into a patient's body. The vulnerability was discovered by researchers, no incidents have been reported. To address critical vulnerabilities, experts recommend access control with fewer privileges and tighter controls with continuous monitoring.

The fact that 91% of healthcare providers use remote monitoring use remote is definitely a significant step forward. Experts from Kaspersky 2021 studied the protocol for transmitting data from wearable devices used to remotely monitor patients and identified 33 vulnerabilities, including 18 critical vulnerabilities that could allow data to be obtained by unauthorized parties. Patients are monitored using wearable devices, which can be used to monitor their condition or, for example, heart function. The most common data transmission protocol for wearable devices is the MQTT[2] protocol. The protocol does not include proper authentication or encryption. Kaspersky researchers have found vulnerabilities not only in the protocol, but also in the platform of the devices (Qualcomm Snapdragon Wearable). As these devices not only monitor health data, but also track the location and movements of the patient, this information, if in the wrong hands, could not only be a privacy issue, but also a threat to personal security. Experts have found that security gaps remain open for specific healthcare applications, wearable devices, implantable sensors, cloud-based databases.

The National Cyber Defence Institute has published the following vulnerability on its website, based on a briefing issued by the US ICS[3]:

[1] European Commission against Racism and Intolerance
[2] A standard for IoT messaging
[3] CERT Industrial Control Systems Cybersecurity Incident Response Team

- implantable defibrillators[4] are a critical classification vulnerability for medical devices manufactured by Medtronic. The protocol used to communicate with the devices does not use authentication or encryption. By exploiting the vulnerability (if RF[5] communication is enabled on the device), attackers can gain access to the devices, modify the communication, interfere with the operation of the device, obtain sensitive patient data. For such a device, it is truly a matter of life and death to ensure proper operation.
- the manufacturer has issued a security update on the stricter handling of communications, but also proposes to introduce additional security measures.

The United States Cybersecurity and Infrastructure Security Agency (CISA) published a security flaw in Philips Healthcare's e-Alert MRI imaging software on March 29, 2022. The software could allow unauthorized persons to remotely shut down the system. A warning has been issued that previous versions of the software do not perform authentication and may be accessible to attackers. The vulnerability was discovered by cybersecurity analysts, no attack was detected, and no reports were made. Philips has announced that the e-Alert hardware solution is not a medical device, its shutdown does not pose a risk to patient safety, and in the event of an unauthorized shutdown due to a security vulnerability, the hardware must be restarted, but has improved the cybersecurity of medical devices. At the Singapore Cybersecurity Summit on 13 April 2023, ISACA Director Serge Christiaans proposed a proven technology to improve cybersecurity in aviation. He said that accepting that humans make mistakes, but treating mistakes as learning opportunities, looking for the cause of the mistake, determining whether the mistake is systemic (just culture), has contributed to improving aviation safety (fatalities have been significantly reduced).

The safety of medical devices is a major challenge for the industry. Equipment breakdowns and malfunctions can put patients at risk, which is why it is crucial to develop an appropriate medical device safety strategy. In my opinion, risk assessment and management, access rights regulation, cyber security training, compliance with device procurement standards can reduce cyber security risks associated with medical devices and services. The use of cloud-based technology in healthcare is steadily increasing, and given the nature of the information, data protection is also a priority in this area, and the risk of patient data being accessed by unauthorized persons can be reduced by appropriate password protection and two-step identification.

[4] life-saving devices that help to keep the heart beating in the event of a serious cardiac arrhythmia
[5] radio frequency

INFORMATION SECURITY REGULATION IN MILITARY HEALTH

The medical system for military health is the MedWorks health IT system, which provides IT support for inpatient, outpatient, and curative care with its modules. Its patient flow system provides integrated and modular functions for the documentation of patient care. The patient flow system collects and organizes patient care data in patient records, all data being linked to the patient.

The diagnostic modules of the software are: X-ray, ultrasound, CT, MRI, angiography, endoscopy, pathology. A specific data recording interface supports work in the diagnostic specialities. The operation and administration of the medical system is carried out by an external operator. The Operations Department is responsible for the operational supervision of the external operator. The information security requirements for the military medical system shall be those laid down in the Regulations. Information Security Policies:

- Electronic Information Security Policy;
- Electronic Emergency Plan;
- Electronic Information Security Policy.

Key policies related to the medical system:

- Personal and health data must be processed only by those involved in the care of the person concerned;
- Those who are not involved in the care of the patients concerned are not entitled to process the data.

FEASIBILITY OF INFORMATION AND DATA SECURITY IN THE FIELD OF OPERATIONS

Health insurance is also part of the military crisis response operation. In the performance of operational tasks, telemedicine can assist military health, and in the performance of mission tasks, it provides the possibility to perform remote monitoring systems and diagnostic procedures. The operation of telemedicine requires an adequate health IT system and equipment. In my view, operational healthcare is a priority for data and information protection. Data on the scope and composition of the population of care carry important information that can be targeted by attackers. The supply must be maintained at all times, so a possible outage could have unforeseen consequences. Vulnerabilities can occur in the infocommunication system, medical devices and human resources are also a significant risk. With the use of telemedicine, vulnerabilities may also occur in the patient monitoring devices and IT systems, and the databases transmitted by the transmitting sensors and

their servers may become targets. The data and information security of the field hospital's operations must be ensured by establishing, maintaining, and enforcing appropriate rules and security measures. Access rights management should be a priority. The information awareness of those serving in the operational unit should be assessed and trained to avoid incidents and to respond appropriately in the event of a cyber-attack.

DATA BREACHES IN HEALTHCARE

In recent years, the number of cyber attacks against healthcare institutions has increased significantly, mainly in the form of ransomware attacks. In this chapter, therefore, let's review some attacks that have compromised the reliable operation of healthcare systems.

Sophos, a UK-based security software and hardware company, has conducted a survey on the cyber threat to the healthcare sector, looking at nearly 400 healthcare organizations in 31 countries. They found a 69% increase in cyber-attacks, but an improvement in organizations' cyber-security preparedness. Of the organizations surveyed, 66% had experienced a ransomware attack, a 34% increase on the previous year. A high willingness to pay ransom was observed in the affected organizations, due to the fact that the loss of access to health data could put the life of the patient at risk, and in many cases the cost of recovery would have been higher than the ransom.

One specific type of attack is the ransomware attack, which can create a situation that threatens the security of patient care. On 10 April 2023, the Healthcare Information and Management System (HIMSS) consultancy released its 2022 Cybersecurity Survey. In the past year, the healthcare sector has been "attacked" by the following ransomware: BianLian, Blackcat & Royal, Cobalt Strike, LockBit 3.0, Karakurt, RansomHouse, Zeppelin. The survey found that while healthcare organizations have made significant progress in improving their cybersecurity, challenges remain. The biggest vulnerability is the human factor. Healthcare organizations need to do more to implement cybersecurity programmes.

In October 2020, the University of Vermont Medical Center's Oncology Unit suffered a cyber-attack that rendered the cancer patient information system inaccessible. Complex chemotherapy protocols had to be reconstructed from memory, and hundreds of patients could not be treated. The damage caused by the attackers to sick people was unimaginable. Staff had to tell patients that they could not receive lifesaving or life-extending treatment because of a lack of documentation. Nearly a month after the attack, the hospital's electronic medical records system was only 75 percent restored. More than 300 specialists worked to "clean" and reinstall 1,300 servers and 5,000 computers.

There were 52,224 data breaches involving individuals in the state of Kansas. According to the Emporia hospital, email accounts were accessed between October 2021 and November 2021. The email accounts contained personal information, medical record numbers, email addresses, treatment information, social security numbers, financial information. A family doctor in North Carolina shared the following lessons learned from a ransomware attack: in October 2021, his cloud provider was hit by a ransomware attack. The cloud provider was negotiating with the FBI and a cybersecurity team to ransom the extortionists, while the practice management system was inaccessible. They demanded $5.1 million from the cloud provider. The GP was unaware at first how much information had been leaked from his practice. They reverted back to a paper-based system so they could continue to provide GP services. After three months of negotiation, the cloud provider paid the extortionists $500,000, they got the encryption key, but the GP stopped trusting the provider and signed a contract with a larger cloud provider.

On 19 April 2022, a hospital in France was hit by a cyber-attack. The incident involved the theft of administrative and patient data. When the attack was detected, the hospital's IT staff disconnected the Internet connection to prevent further data leakage. The IT system remained operational and patient care was able to continue. In March 2023, a cyber-attack hit one of the Clinic hospitals in Barcelona, a ransomware attack crippled the centre's computer system, forcing the cancellation of non-urgent surgeries (150) and patient examinations (nearly 3,000). Computers were also down in laboratories, the emergency department, and the pharmacy, in the three main centres and in outside clinical areas. Patient records were inaccessible and communication between units was also down. Case management was paper based, with urgent cases now being referred to the city's hospitals.

On a Friday in April 2016, the department of a county hospital with 700 active beds and 200 chronic beds, with outpatient specialties, reported that Excel files saved on the "desktop" were disappearing, replaced by unknown files. The IT department employee immediately shut down the servers, notified the department heads, requested all machines to be shut down. The emergency plan was put into effect. The IT department prepared an incident report and launched an investigation. It turned out that the incident was caused by an e-mail opened by the secretariat. The e-mail was sent from abroad. When the e-mail was opened, malicious programs started running in the background. The IT department started troubleshooting the error, the data was backed up properly, it was restored, no patient data was lost due to the timely response, no other data was lost. The firewall settings were set according to stricter rules and were subsequently operated accordingly. More restrictions on the

use of wifi were introduced, training was organized, specifically on social engineering methodology. Training for the IT specialist was provided by external experts.

On Friday, 13 December 2018, a subcontractor of a county hospital with 800 active beds and outpatient services (the hospital has contracted with several contractors to ensure continuity of care) reported that its computer data was inaccessible due to encryption, and then 11 other workstations and the server were also inaccessible. The person who detected the incident notified the hospital's IT department that the machines and the network were working "slowly". The extortionist displayed a screen message indicating the fact of the attack. Immediately after the incident was detected and reported, the workstations were shut down, notifications were made, the physical connection to the hospital system was immediately severed, and the two networks were isolated. A virus scan was started on the hospital servers. The ransomware was most likely introduced into the company's network from the data processor's secretarial machine and spread from there. As a result of the attack, data was lost, and data from February 2017 to December 2018 was not available electronically. No backup had previously been made. Until the system was restored, further business was conducted on a paper basis, and previous data was also available on paper. Some of the data was successfully restored, others had to be re-recorded from paper documentation.

Phishing attacks are also a significant risk, a common attack strategy against the healthcare system and its employees. Researchers conducted a phishing simulation on a sample of 6 US healthcare institutions, sending 2.9 million simulated emails to employees. 14.2% of the emails were clicked. Based on the content of the emails, emails with different content were more likely to be responded to. Repeated phishing campaigns were associated with a decreased chance of a subsequent click.

SUMMARY

Security is not only about protecting information, but also about protecting the information services and the IT systems that provide them, which are of significant value in their own right. ICT networks are targets for cybercrime, they pose a threat, but in the healthcare sector they also pose a risk of failure due to malfunction or breakdown (whether intentional or accidental). The health system's ICT networks, information systems and data protection are of paramount importance. As health information has become increasingly sought after by cybercriminals and attacks on healthcare organizations are on the rise, there is a need for increased protection of personal and health data. Complex security solutions covering the entire health information infrastructure must be put in place to ensure the integrity of information. Information security policies and measures must be developed

and implemented to prevent unauthorised access to information and to respond quickly, effectively and appropriately in the event of an incident. The vulnerability of medical devices also creates the potential for data breaches, and the sector faces increasing cybersecurity challenges with the spread of telemedicine and cloud computing. Achieving the right level of cyber security is a major challenge for healthcare and military health organizations. The number of cyber-attacks is constantly increasing, and new attack techniques and technologies are emerging. Attackers exploit the vulnerability of information systems and the human factor. It is therefore essential to continuously improve information security. A key element of cyber security is the development of an appropriate level of security awareness. Appropriate measurement techniques can be used to estimate the risk of the human factor, and the results of these assessments can be used to prevent and manage vulnerabilities. As part of military health care, cyber security in operational health care is of paramount importance. In the operational domain, vulnerabilities can arise in the infocommunications system, medical devices, cloud technology, telemedicine, and human resources are also a significant risk.

REFERENCES:

1. Paul Nadraq: Industry Voices-Forget credit card numbers. Medical records are the hottest items on the dark web, Capsule Technologies 26.01.2021., Helathcare Cybersecurity Review, https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web?utm_source =sendinblue &utm_campaign=Kiber _20221021&utm_medium=email (Download time: 21. 10. 2022.)
2. The Basic Law of Hungary 2011. https://net.jogtar.hu/jogszabaly?docid=a1100425.atv, (Download time: 21. 05. 2023.)
3. D. o. H. a. H. S. (. (USA), „Insider Threats in Healthcare," HHS, https://www.hhs.gov, (Download time: 21. 05. 2023.)
4. F. e. a. Gioulekas, „pubmed.ncbi.nlm.nih.gov," National Library of Medicine, 09. 02. 2022. https://pubmed.ncbi.nlm.nih.gov/35206941/. (Download time: 08. 01. 2023.)
5. National Health Insurance Fund Manager, 02. 05. 2018. https://www.neak.gov.hu/felso_menu/lakossagnak/adatvedelem/ elektronikus_informaciobiztonsag. (Download time: 01. 12. 2022.)
6. O. Fodorné Zagyi, Health data protection in the light of e-health technologies, Rendészet-Tudomány-Aktualitások, pp. 159-168., 2021. https://tudasportal.uni-nke.hu/, (Download time: 01. 02. 2023.)

7. 2021 Top Health Technology Hazards executive Brief, ECRI, 2021. https://assets.ecri.org/PDF/Solutions/Device-Evaluations/ECRI-Top10Hazards_2021_EB.pdf. (Download time: 01. 04. 2023.)
8. Xu Zou: Protect every connected device with Zero Trust IoT security, tailor-made for medicine, Healthcare Cybersecurity Review, 14. 04. 2023. https://www.hhs.gov. (Download time: 01.06.2023.)
9. Kaspersky: Tracking your heartbeat… and payment data? 33 vulnerabilities found in the data transfer protocol for wearable devices, www.kaspersky.com," Kaspersky, 01. 02. 2022.. https://www.kaspersky.com/about/press-releases/2022_tracking-your-heartbeatand-payment-data-33-vulnerabilities-found-in-the-data-transfer-protocol-for-wearable-devices. (Download time: 05. 04. 2023.)
10. Rikk János: Kutatásmódszertan; Budapest, Szerzői kiadás, 78 p. (2014), ISBN: 9789630894951
11. National Cyber Defense Institute: Medtronic healthcare devices vulnerabilities, nki.gov.hu," 22. 03. 2019. https://nki.gov.hu/warnings/emergency-emergency-new/medtronic-healthcare-devices-erinto-emergency-emergency/ (Download time: 01. 02. 2023.)
12. Greg Slabodkin: CISA warns about cyber flaw in Philips MRI monitoring software, „https://www.healthcaredive.com/news/cyber-flaw-philips-mri-monitoring-software /621350/, Healthcaredive, 01. 04. 2022. https://www.healthcaredive.com/news/cyber-flaw-philips-mri-monitoring-software/621350/. (Download time: 10. 01. 2023.)
13. Serge Christiaans: Safety awareness is worth learning from pilots, 14. 04. 2013., https://bitport.hu/pilotavizsgas-isaca-vezeto-a-biztonsagtudatossagot-a-pilotaktol-erdemes-tanulni. (Download time: 18. 04. 2023.)
14. Zsolt Fejes: A new opportunity in defense health care: telemedicine, Hadmérnök, XI. évf. 1. szám, pp. 233-239., 2016. www.hadmernok.hu, (Download time: 18. 04. 2023.)
15. National Cyber Defense Institute: Situation: The healthcare industry is under considerable pressure from ransomware, 04. 07. 2022.. https://nki.gov.hu/ it-security/news/situation-picture-significant-extortion-virus-pressing-under-the-healthcare-sector/ (Download time: 15. 01. 2023.)
16. HIMSS Healthcare Cybersecurity Survey Report 2022. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey. (Download time: 14. 04. 2023.)

17. E. Barry és N. Perlroth, „Patients of a Vermont Hospital Are Left ‘in the Dark’ After a Cyberattack,” https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html, The New York times, 26. 11. 2020. (Download time: 15. 01. 2023.)
18. J. McKeon, „healthitsecurity.com,” Xtelligent Healthcare Media, 19. 04. 2022. https://healthitsecurity.com/news/data-breach-goes-unnoticed-for-nearly-1-year-at-ks-hospital. (Download time: 30. 10. 2022.)
19. Török Péter, Négyesi, Rikk János: BASH scripting, Henderson (NV): DEVLART, LLC, 68 p. (2017), ISBN: 9780997721065
20. J. McKeon, „healthitsecurity.com,” Xtelligent Healthcare Media, 24. 01. 2023. https://healthitsecurity.com/features/how-an-independent-practice-recovered-from-a-third-party-ransomware-attack?utm_source=sendinblue&utm_campaign=Kiber_II6_20230414&utm_medium=email. (Download time: 14. 04. 2023.)
21. Bill Toulas: French hospital group disconnects Internet after hackers steal data, https://www.bleepingcomputer.com/news/security/french-hospital-group-disconnects-internet-after-hackers-steal-data/. (Download time: 18. 01. 2023.)
22. Associated Press: Cyberattack Hits Major Hospital in Spanish City of Barcelona, 06. 03. 2023. https://www.securityweek.com/cyberattack-hits-major-hospital-in-spanish-city-of-barcelona/?utm_source=sendinblue&utm_campaign=Kiber_II6_20230414&utm_medium=email. (Download time: 14. 04. 2023.)
23. Tamás Palicz Dr. és e. al: Cases of ransomware attacks occurring in Hungarian hospitals, IME – Journal of Hungarian Interdisciplinary Medicine, XX. évfolyam, 2021/1. number, pp. 32-38., 2021. (Download time: 14. 04. 2023.)

Toxic Properties of Hazardous Substances Arising from Fires

Miroslava Vandlíčková, University of Žilina, Faculty of Security Engineering, Slovakia, miroslava.vandlickova@uniza.sk, ORCID: 0000-0002-3271-1603

Abstract

Many of interventions by firefighters and rescuers bring with itself a possible risk of intoxication by combustion products. The fumes threaten not only firefighters and rescuers but also persons present in areas with risk of fire or in their immediate vicinity. The question of the toxicity of hazardous substances is still up to date and its actuality is supported by the constant development of the chemical industry and sectors whose business or job content is related to hazardous substances. An essential aspect of intoxication is the type of toxic substances produced during a particular fire, their duration of action and the way they are absorbed into the body. The article deals with the toxicity of hazardous substances produced at fires and with the effective protection against them.

Keywords: hazardous substances, fire, toxicity of hazardous substances, protection of firefighters and rescuers, chemical substances, combustion products

Corresponding author: Ing. Miroslava Vandlíčková, Ph.D., vice-dean for education, University of Žilina, Faculty of Security Engineering, 1. May Street 32, 010 26 Žilina, Slovakia

Introduction

During the burning of any material a whole range of chemical substances harmful to health, combustion products, which can cause mass or individual intoxication, is created. In addition to the most well-known combustion products of carbon monoxide or carbon dioxide, chemical substances such as hydrogen chloride, ammonia or sulfur dioxide are also produced during industrial accidents resulting in fire. [1]

Combustion products can be divided according to their state into solid, liquid and gas. The solid particles remain in the form of ash or they are part of the smoke. Liquid products are released in the form of steam or as an aerosol in the smoke at the same time as gaseous products of combustion.

1. Table: Division of combustion products [2]

Combustion products	Solid	Ash	Complete combustion	oxides, carbonates, diphosphates, sulphates
			Incomplete combustion	partially degraded material
		Smoke	Complete combustion	oxides, phosphates, ash particles
			Incomplete combustion	soot, unburned particles of burning substance
	Gas	Smoke	Complete combustion	CO_2, SO_2, hydrogen halides, nitrogenous gases, nitrogen
			Incomplete combustion	CO, HCN, hydrocarbons
	Liquid	Vapor, mist	Complete combustion	water vapor
			Incomplete combustion	hydrocarbons, alcohols, aldehydes, ketones, carboxylic acids

Combustion products and their toxicity

Fires produce a large amount of fire emissions - combustion products. Their amount depends on the amount and type of flammable substances and materials, their chemical composition or burning conditions. Furthermore, the formation of fumes may depend on the stage of combustion or on the concentration of the oxidizing environment, especially the air, that supports combustion or on the method of oxidation, whether it is complete or incomplete, and on many other factors.

- **Carbon monoxide (CO)**

Carbon monoxide is a colorless, tasteless, odorless gas that is poorly soluble in water and is produced during the incomplete combustion of any substance containing carbon. It is the main component of explosive gases. CO intoxications mostly occur as a result of accidents in mines and closed spaces. Most commonly by inhaling motor vehicle emissions or in industry by inhaling methyl chloride present in solvents, paint removers and degreasers. [1,3] Carbon monoxide poisoning is often overlooked or misdiagnosed. We absorb it through the lungs into the blood, where it binds to hemoglobin, which prevents it from carrying oxygen to the tissue. Poisoning occurs when inhaling a contaminated atmosphere even at a low concentration of CO, while a concentration of 4.6 mg/l for

30 minutes leads to death. The largest number of deaths occur in fires or suicide attempts - exhaust gas poisoning. [1,3] When providing first aid, we must be aware that CO affects the human body over time. At a concentration of 1% CO in the air, 50 is formed in the blood % COHb after 2-7 minutes. At a concentration of 5% in the air, 30-90 seconds are enough. The newly formed carboxyhemoglobin then flows through the body. The body can react to the presence of CO later, when the intoxicated person is relatively safe in the fresh air. The involvement of the nervous system can be manifested even after 3 weeks. [4]

- **Carbon dioxide (CO_2)**

Carbon dioxide is a colorless non-explosive, odorless, heavier than air. It is well soluble in water, easily liquefiable and does not support combustion. It is a normal component of the atmosphere. It transforms its state at 80 °C like dry ice from a solid state directly into a gas state with the formation of cold water vapor. Carbon dioxide is also produced as an end product of the combustion of organic and carbon-rich substances. It is part of explosive gases. It also occurs during fermentation or rotting. [3] At a low concentration, CO_2 can cause irritation of the respiratory tract, but at an inhaled content of 5-10 vol. % suppresses breathing, which means it has a narcotic effect. CO_2 intoxication manifests itself as a headache, dizziness, a feeling of weakness or rapid breathing. Inhaling air with a CO_2 concentration in the range of 10-15 vol% leads to convulsions and unconsciousness. At an air concentration above 15 vol.%, it occurs the stroke. If the air concentration is higher than 20 vol.%, breathing stops and death occurs. [1]

- **Hydrogen Chloride (HCl)**

Hydrogen chloride is a non-flammable, colorless gas. It is highly toxic with an irritating odor, easily absorbed in water to form hydrochloric acid, well soluble in organic solvents. Gaseous hydrogen chloride reacts with red-hot metals to produce explosive hydrogen; it reacts with fluorine to produce a flame. It reacts with atmospheric oxygen only in the presence of a catalyst and at a temperature higher than 600 °C. [5] HCl is a product of burning any substance that contains chlorine, for example PVC - toys, floors, cable insulation, etc. Finishing work after fires in warehouses, shops, drugstores or households is also very dangerous. Even after the fire has been extinguished, there is a lot of gaseous HCl in the air, which will negatively affect the organism of the firemen who intervene and people who do not protect themselves from it with breathing apparatus. [4] The effect of hydrogen chloride has serious consequences in the case of long-term and repeated irritation of the respiratory

organs. It can cause frequent nosebleeds, damage to the mucous membrane of the mouth and nose, perforation of the nasal septum or the development of chronic bronchitis. Skin and teeth also suffer from irritation - tooth enamel is etched. [5]

- **Ammonia (NH_3)**

Ammonia is ranked as the third most frequently produced chemical compound in the world, which is used in the production of artificial fertilizers, animal feed, but also for cooling. It is most often found in toxic concentrations in pig farms. As a combustion product, it is created during the burning of artificial fibers, silk or furniture made of synthetic materials. [6] It is a toxic, corrosive, colorless gas with an irritating odor, which strongly irritates the mucous membrane even at low concentrations. At a high concentration, it causes corrosion of the mucous membrane of the respiratory tract and lungs, or even death. It is well soluble in water, forming ammonium hydroxide, which causes a burn of the oral cavity, esophagus and stomach when ingested. [1]

- **Hydrogen Cyanide (HCN)**

Chemically pure hydrogen cyanide is a colorless, volatile liquid with a characteristic bitter almond odor. It is highly poisonous and forms an explosive mixture with air. [1]

It is produced to a small extent by some types of bacteria, fungi and plants. It also appears in the kernels of almonds, cherries and apricots. It is used in the disinfection and extermination of grain warehouses and railway wagons, in the production of acrylics, dyes, synthetic fibers and plastics. At the same time, insect and rat poisons are made from it. It was used as a chemical warfare agent during the First World War and during the genocide in the concentration camps during the Second World War. [1,7] Hydrogen cyanide is ranked among the most toxic substances, the so-called systemic or blood poisons. We are at risk of intoxication by inhalation, absorption through the skin or ingestion. Its basic effect is blocking cellular respiration, which is the main way of oxygenation from the blood to the tissue. Inhalation of a small amount is manifested by headaches, dizziness, fainting, palpitations, pain in the chest and heart area, and even unconsciousness. Inhaling a higher concentration will cause accelerated breathing, loss of consciousness, convulsions. Intoxication is also indicated by dilated pupils and skin covered with cold sweat. Finally, breathing and blood circulation stop. [8]

- **Phosgene ($COCl_2$)**

Phosgene is a colorless, tasteless, highly poisonous gas with an unpleasant odor. It is formed when cooling liquids containing freon are burned. It easily reacts with water, producing hydrochloric acid. Its thermal decomposition starts at 200 °C and ends at 800 °C. [5]

Phosgene has strong irritant effects, and its toxicity is fully manifested several hours after exposure to its effects. Symptoms during its action are irritated eyes, mucous membranes, cough. It poses a serious danger to the respiratory system, as it easily reacts with water in the lungs, which are always moist, creating strongly corrosive hydrochloric acid. This damage becomes apparent only after a certain period of approx. 3-4 hours. [4,5]

- **Sulphur dioxide (SO_2)**

Sulfur dioxide is a poisonous, colorless, non-flammable gas that has a sharp, irritating and pungent odor. It is heavier than air and forms sulfuric acid (H_2SO_3) and sulfuric acid (H_2SO_4) when it comes into contact with water. It turns into a liquid state at -10 °C. [7] It is formed during the combustion of fuels and oils containing sulfur, mainly in thermal power plants, during metal casting, kerosene refining or during the production of sulfuric acid. It is used in the production of cellulose and paper, for packing wool, disinfecting containers or as a stabilizing agent in refrigeration. [1,7] It enters the body by inhalation. Its irritating effects on the conjunctivae and the respiratory system are manifested immediately. At lower concentrations, it causes an irritating cough and suffocation. In high concentrations, it can cause obstruction of the upper respiratory tract, pulmonary edema or extensive mucosal damage. When used in gastronomy, it can cause allergic reactions or exacerbation of asthma. [1,8]

Protection against hazardous combustion products

The best possible measure against intoxication by combustion products for persons who are not equipped with protective equipment, such as firefighters or other emergency services providing assistance in case of fires, is a protective escape mask or balaclava. Their function is to protect the airways or eyes of affected persons during the escape or evacuation from the threatened area to a safe zone. One of the possible means of protection can be the protective escape mask S-CAP. Its use is possible wherever people are at risk of smoke or combustion products. The escape mask provides protection for the eyes, head, and respiratory tract and thus enables the self-rescue of disabled persons. It serves as an additional preventive fire protection measure and can increase safety in buildings with

a higher incidence of people such as administrative buildings, hospitals, hotels and other gathering spaces.

4. *Figure: Escape mask S-CAP [9]*

The protective escape mask is a yellow-green balaclava with a large polycarbonate lens. Inside the hood is a half-mask that can adapt to different head and face sizes. It is connected to a multi-purpose filter that has a wide range of protection. The hood filter protects against inhaling a large amount of dangerous substances. It cleans the air from inhalation of poisonous and irritating smoke and gases produced by fires, such as carbon monoxide, hydrogen cyanide, sulfur dioxide and against particles of less toxic substances. The filter is designed to remain in place for fifteen minutes, which is sufficient time to escape the space under normal conditions. The duration of the filter function depends on the concentration of harmful substances. Using the mask is not difficult. Handling it is simple and fast, and it can be used even by people with glasses. The disadvantage of the mask is its one-time use. The mask has a total weight of approx. 540 g, inhalation resistance approx. 1.2 mbar and exhalation resistance approx. 0.5 mbar. When properly stored in the original packaging, the mask will last for 4 years without maintenance. After 4 years, the mask needs to be checked. The maximum permitted storage period of the escape mask is 10 years. [9]

As another possible means of protection, it can be can used the Dräger Parat C escape hood. The Dräger Parat C fire hood serves as a means of protection against inhalation of combustion products when escaping from a danger area to safety. It provides effective protection against toxic gases and substances produced during fires for fifteen minutes, which is enough time to move to safety. Dräger Parat C is a hood that can be easily and quickly put on to protect the respiratory tract, eyes, ears, head and neck. The escape hood with a half mask ensures perfect tightness and enables simple and comprehensible communication with the environment. We seal it using a single-point belt. The panoramic visor with anti-fog protection ensures good visibility and recognition of the wearer.

The size of the mask is universal, so both adults and children can use it. Glasses, a big beard or long hair are not a problem either. [10]

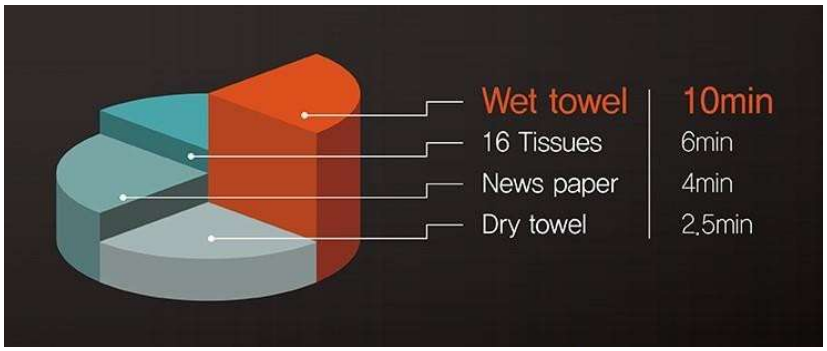
5. *Figure: Dräger Parat C escape hood [10]*

The hood is designed so that the filter can be easily replaced after use, which also extends its lifespan to 12 years. If the filter is not opened, the storage period is up to 6 years without the need for inspection.

The options for wearing a hood are different. It can be in a hard case clipped to a belt or in a soft case in a breast pocket. The hood can also be placed on the walls of escape routes, where it can be easily found thanks to the fluorescent marking of the mask cover. [10] In addition to the escape mask or balaclava, which should be available to firefighters, persons in workplaces where a fire may occur should also protect themselves against intoxication. Water mask dispenser or water mask container is one of the latest innovations that can ensure escape from the fire area and inhalation of combustion products before the arrival of rescue services. To prevent suffocation, one option is to cover the nose and mouth with a wet cloth, preferably a towel. This can be a problem in offices, large halls. Another problem can be the panic that takes over after a fire breaks out. Therefore, this device is suitable for spaces where more people stay and there is a possibility of a fire.

3 *Figure: Reservoir for a water mask [11]*

Compared to a gas mask or protective hood, it is faster to use. When placing these reservoirs in the areas of escape routes from the place of danger, there is a high probability of using them faster than searching for a warehouse with gas masks or escape hoods.When comparing respiratory protection with things blocking the inhalation of toxic substances and gases, a wet towel is 4 times more effective than a dry towel, sleeves, sweatshirt.



4 *Figure: Comparison of the effectiveness of respiratory protection [11]*

The container forms a cover that can be attached to the wall in which the water tank is located. Masks or cloths made of highly absorbent material are placed under the tank. The container is closed by a transparent opening on which a handle is fixed, which is connected to the lid of the water tank.

5 *Figure: Reservoir construction [11]*

Conclusion

During many fires health - damaging substances with toxic properties are created to which persons working or present in the particular environment are exposed, as well as the firefighters who intervene there. The fastest way of intoxication during fires is inhalation of combustion products, where the respiratory tract and nervous system are mainly at risk. For this reason, we have focused

our proposals on respiratory and head protection. The proposals are a suitable means for firefighters to use when evacuating people from a threatened environment, and at the same time they are suitable as preventive measures for the protection of workers working in given objects with a probable occurrence of fires.

References:

6. Štetina, J. a kolektiv, 2014; *Healthcare and integrated rescue system in mass accidents and disasters*; Praha: GRADA; 2014; ISBN 978- 80-247-4578-7
7. Sikora, H., 2007. *Toxicology of Combustion Products*; Diploma Thesis. Online. Available at: https://theses.cz/id/jxlrr4/downloadPraceContent_adipIdno_7335
8. Dobiáš V., *Repetitorium of Urgent Medicine – Intoxication by combustion products*; 2007; [online] ; Available at: http://www.solen.sk/pdf/32de418b26ded45b2e8a2f2a2836cb15.pdf
9. Lukeš, M., *Combustion products – basis of fire tactics*;. *2016*; [online] ; Available at: https://docplayer.cz/4647357-Produkty-horeni-zaklady-pozarni-taktiky.html
10. Janásek et all, *Hazardous substances*; EDIS; Žilina 2004; ISBN 80-8070-243-8
11. Dobiáš V., *Repetitorium of Urgent Medicine – Intoxication by combustion products*; 2007; [online] ; Available at: http://www.solen.sk/pdf/32de418b26ded45b2e8a2f2a2836cb15.pdf
12. Buchancová, J. et all; *Work medicine*; Martin: OSVETA; 2003; ISBN 80-8063-113-1
13. Kurucz, J.,; *Industrial toxic substances*; Banská Bystrica: BELIANUM; 2017; ISBN 978-80-557-1263-5
14. *Escape Mask S-CAP in a case*; 2019; [online] ; Available at https://www.hasicskavyzbrojna.cz/maska-unikova-s-cap-v-pouzdre/d-190619/
15. *Escape Hood Dräger Parat C.* 2019; [online]; Available at: http://www.webareal.cz/bimbohas/Unikova-kukla-Drager-Parat-C- d475.htm?tab=description#anch1
16. Water Mask Dispenser; [online]; Available at https://www.jamesdysonaward.org/2018/project/water-mask-dispenser/

The importance of the singles category in teqball, in the youth age group

János Tóth jr., Martin Csereklye
Hungarian University of Sports Science

Abstract

Teqball's dinamical improvement and rise in popularity can be seen more and more in the world and more than 10 thousand people have tried it out either out of curiosity or thanks to an ongoing or previous sports experience. There is a large number of people who not only gets to the table to have fun or just to kick the ball for a few times but in the hopes of a semipro or professional career they train themselves and put their outmost skill to be able to achieve succes on boat and national and international levels. They held the first ever World Championship of teqball in the year 2017, of which gave a steady rise to the number of competitions all over the world. They have intorduced the World Ranking List and they also entice players with different cash prizes as well to take part. These amounts are on the rise, because of this the player numbers and registered ones have multiplied since the begining. Based on this one of the most important aspects of the sport should be to create clubs and cultivate new players especially from the youth age group. The aim of our case study was to find out that teqball's two most prominent category how much more training for the singles ones benefints the youth group than practice for the doubles. We have investigated different groups, namely the top worlwide players of teqball, youth groups and amateur players. The results fall in line with the technical parts of the hypothesis, on the mental side we have recieved partialy resounding feedback.

Keywords: teqball, singles category, youth age group

Introduction

I have joined teqball at its infancy. Two years after the official release on a Hungarian event where I discovered the table and fallen in love at first sight. The game has a distinct peculiarity that I would like to promote to anyone who have yet to try it out. In our opinion the next generation of players who wants to take this sport to a higher level they would have to dedicate more effort to the singles category as this gives the sport its technical foundation. It is also supported by the modern technologies.[1] We hope our investigation brings light to that training to this category is a key element both in technical and mental aspect to the sport. In teqball situations are constantly changing, both singles and in doubles, it is extremely important to read the game, to have the right decision-making ability and to think quickly, just like in team sports. 0 When analyzing soccer talent [3][4], Reilly and his colleagues 0 highlight research that focuses on anticipation or decision-making, which makes it possible to notice the difference between good and less good players.

We believe it is important that in this young age group players should prepare propotional to their goals. Even as teqball garnered explosive succes and is dinamicaly improved nowadays the training of the younger generation is still in its infancy.

In our thesis we would like to prove that training for the singles category has a heavy importance in a competitors life both mentally and technically. Everyone is moving upwards in life, and this involves the development of character that can also be observed in sports, since this is when our personality also develops. 0 It can be observed among teqball players at the top level and at the forefront of the youth that motivation is a great driving force, which can change someone's attitude and dedication to the goal. 0 Positive reinforcement, attention and this kind of good relationship between coach and player are part of the road to success. 0 It turns out from the previous research that athletes who carry out their activities through internal motivation can be particularly successful. 0 We find it neccessary to look into how much the top players and forerunners of the international field value this category. We want to help those coaches at teqball who works with the younger generation or would like to in the future, to get a realistic view of each area so that they could create the most suitable training method for their needs.

Introducing teqball

Teqball is a soccer-based sport played on a specially curved table (Teq table) by a new generation of athletes or keen amateurs (teqers) who aim to improve their technical skills, concentration and stamina. 0

The most important rules:

- Teqball can be played with any size 5 soccer ball.
- Teqball can be played individually or in doubles, that is by two or four players.
- A teqball match lasts up to 2 winning sets.
- The final set must be won with a difference of at least two points, if the score is 11:11. It is enough to reach 12 points to win all other sets.
- Players or teams have 2 chances to complete a successful serve.
- Players or teams change serves after every 4 points.
- It is forbidden to touch the ball with the same part of the body twice in a row.
- It is forbidden to return the ball twice in a row with the same part of the body.
- Each player or team can touch the ball a maximum of 3 times with any part of the body - except the arms and hands - before returning it to the opponent's half.
- During doubles play, at least one pass is mandatory before returning.
- It is forbidden to touch the table and the opponent during the game.

Hypothesis

One of our hyopthesis we presume that during a match chance to interact with the ball is higher in the singles category than in the doubles. In the second part we presume that mentally it is harder to play a match in the singles one than in the doubles.

Methodology

Match analysis

We have studied four matches from the singles category and four from the doubles, we will present two of each. As in every match with every rally at the end of the point there is sometimes preparation before a serve, we have taken the time from the recieve of the serve until the conclusion of the point as the net time played. Measurements of the time were done with a stopwatch to get in

more precise idea of how many times a player gets in contact with the ball in a singles or a doubles match in the span of a minute. In the tables below you will find the player names along with the respective contacts with the ball broken down by the minute.

For the first match we chose the singles final of the Italian Eurpoean Tour held in Naples, where one of the representatives was the Hungarian, four times world champion Ádám Blázsovics, and on the other side was the Romanian, currently world champion Apor Györgydeák. The end results were 2:1 (7:12, 12:11, 13:11) to Györgydeák. On average there were between 24-28 contacts with the ball in the measured net time per player.

1. table: Singles Match 1

	Time	Apor Györgydeák	Adam Blázsovics
1st set	60 sec	31	25
1st- 2nd set	60 sec	29	24
2nd set	60 sec	28	20
2nd set	60 sec	24	27
2nd- 3rd set	60 sec	22	22
3rd set	60 sec	34	21
3rd set	60 sec	33	28
3rd set	60 sec	21	31
3rd set	30 sec	15	11
Total	510 sec	237	209
Average		**27,9**	**24,6**

For the second singles match, we examined a women's match from the 2022 World Championship, between the Brazilian Rafaella Fontes and the French Amelie Julian, who fought each other for the third place. The Brazilian lady was able to triumph with a spectacular game 2:0 (12:6, 12:6). In a women's match, it can also be observed that there are fewer undefended attacks than in men's matches, so the ball stays in play longer on average, and a rally is longer. On average, the players made 26-28 contacts here per minute, measured in net time. By the end of the second set, a female player had roughly more contacts than a male player at the same time.

2. table: Singles Match 2

	Time	Rafaella Fontes	Amelie Julian
1st set	60 sec	27	27
1st set	60 sec	27	29
1st- 2nd set	60 sec	33	22
2nd set	60 sec	28	30
2nd set	60 sec	27	24
2nd set	50 sec	23	26
Total	350 sec	165	158
Average		**27,5**	**26,33**

We chose the first doubles match from a World Series tournament in Kraków, Poland played by Ádám Bakó-Ádám Blázsovics against the duo Balázs Katz-Csaba Bányik. The numbers of contact can be observed here broken down by each player. Bányik and Katz won the final in 2 sets (12:11, 12:3). On average, a player in the final made 10-13 contacts per a minute broken down into net time.

3. table: Doubles Match 1

	Time	A. Bakó	A. Blázsovics	B. Katz	Cs. Bányik
1st set	60 sec	13	9	11	13
1st set	60 sec	16	15	8	8
1st- 2nd set	60 sec	11	6	12	13
2nd set	60 sec	10	10	14	13
2nd set	42 sec	10	8	6	6
Total	282 sec	60	48	51	53
Average		**12,75**	**10,2**	**10,85**	**11,3**

For the second doubles match, we chose another women's match, which was also played by the duos at the 2022 World Championships in Nuremberg. In the semi-final between American Carolyn Greco, Margaret Osmundson and Transylvanian women, Kinga Barabási and Katalin Dakó, who started in Romanian colors, the American double triumphed 2:0 (12:11, 12:10) and reached the final. The average number of contacts per minute by women is between 9 and 15, calculated in net time.

As we mentioned before in the singles, there are even fewer attacks in the women's field that could not be saved, so longer rallies can be observed.

4. table: Doubles Match 2

	Time	C. Greco	M. Osmundson	K. Dakó	K. Barabási
1st set	60 sec	15	11	8	16
1st set	60 sec	12	9	12	16
1st set	60 sec	7	13	10	11
1st set	60 sec	11	14	9	16
1st- 2nd set	60 sec	16	10	7	12
2nd set	60 sec	11	15	7	11
2nd set	60 sec	9	12	10	16
2nd set	60 sec	15	13	10	16
2nd set	60 sec	11	13	9	16
2nd set	60 sec	8	16	9	16
2nd set	55 sec	8	10	9	13
Total	655 sec	123	136	100	159
Average		**11,2**	**12,4**	**9,1**	**14,5**

Interviews

We had the opportunity to conduct interviews several people who play an important role in the world of teqball, either as a player or as an individual responsible for the development of an area. Barna Németh, the manager responsible for coach training at the International Teqball Federation, Ádám Blázsovics with 4x world teqball champion, Csaba Bányik with 2x world champion, who is the most successful teqball player in terms of international achievement, Apor Györgydeák, the current individual world champion, and Balázs Varga, who is with the Hungarian Teqball Federation and is responsible for the development of supply were our subjects. During our questions, we also addressed our individual hypotheses, as we wanted to examine them from a different point of view. There were several different opinions regarding technical skills, but all our subjects agreed that it is essential for an amateur or junior player who starts playing this sport and wants to develop in it, should not only play doubles.

According to them, the success of technical development must be achieved mainly through preparation for the singles category. Nevertheless the feeling of success, cooperation and the development of communication skills through the doubles are important, but the singles is what gets a player to the point where he is adequately trained. Regarding mental preparation, the views are already divided, but a direction can be taken from them that it is not possible to decide whether one is better than the other, but both have an important role. They develop different areas and at the same time add to the increase of a player's skill level from a mental point of view. A mental coach is essential nowadays for the top players at the highest levels.

Quantitative research

During our investigation, we interviewed teqball players. A total of 153 (n=153) players answered the survey. This can be said to be a significant number, since we are talking about a new sport and most of the respondents belong to the top of the world rankings. During our survey, we asked 10 questions related to the singles category, both physically, technically and mentally. We were wondering how they, as top competitors in this sport, see the roles of each category. We present 3 of the questions that brought us closer to answering our hypotheses.

In our first question we asked in regard to the technical qualification, we were curious as to whether it is possible to achieve a better technical qualification with the singles or doubles category. Most of the respondents think that those who train more for the singles will be more technically qualified.

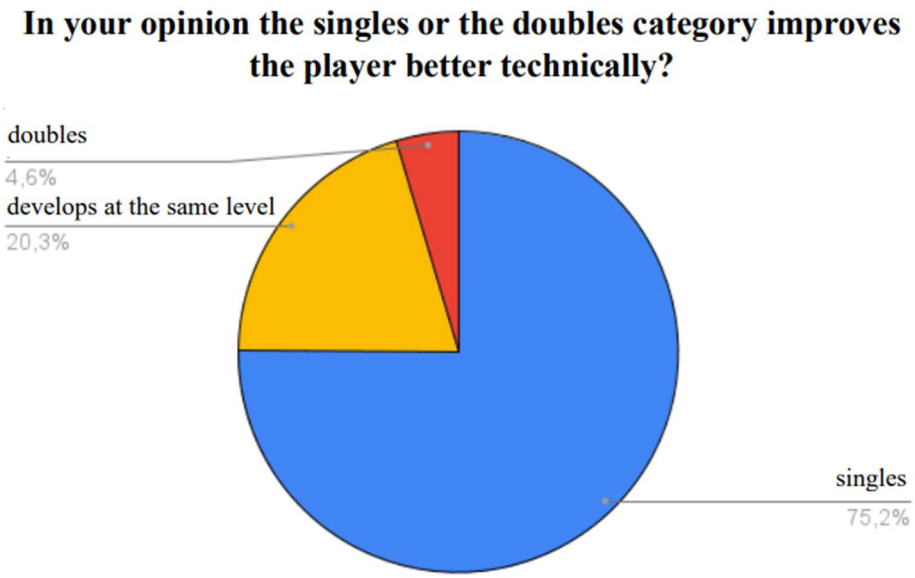


Figure 1. More technically advanced category

For the second question, we were interested in the decision-making part in which category they think it is more difficult to make a decision during a match. These factors help a coach better focus, when designing training sessions. It is clear that they do not differentiate, but place the two categories on the same level.

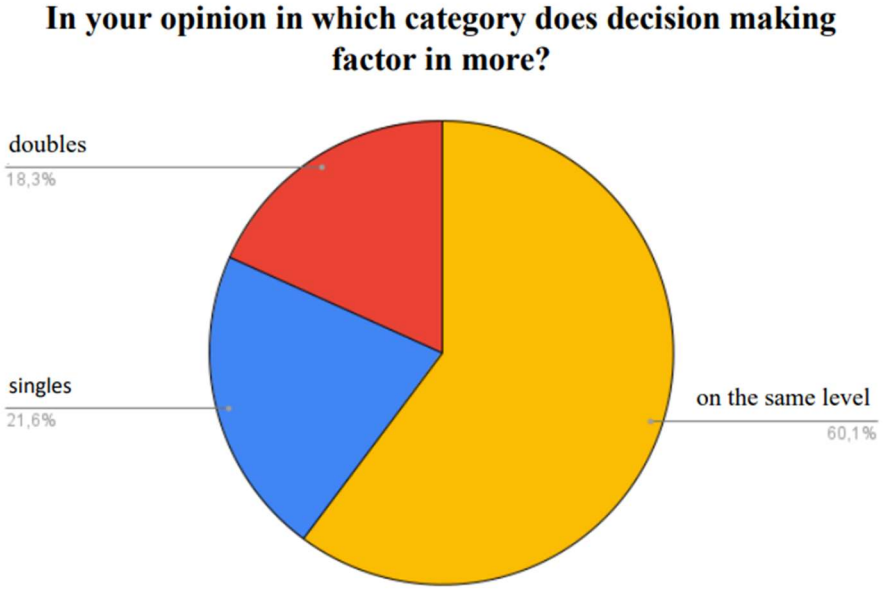


Figure 2. Decision making

In the third presented question, we were wondering in which category they think it is more difficult to play a match mentally. The answers showed us that neither category is ahead of the other in this regard, but both are equally important for a player's preparation.

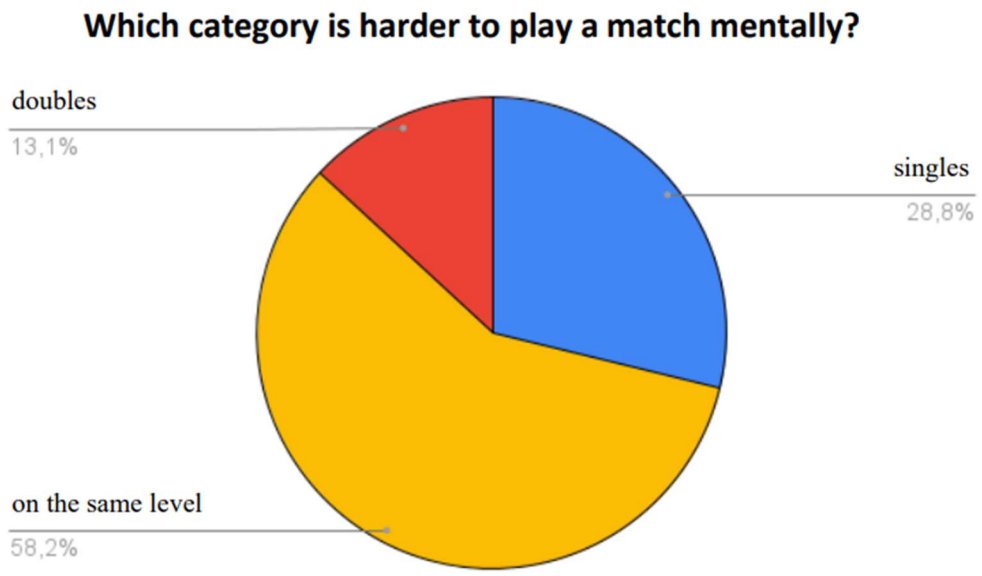


Figure 3. In a match mentally

Conclusion

In this part of our thesis, we answer our hypotheses based on the results obtained after our investigation. **We assumed that during a match, the density of a player's number of touches is higher in the singles category than in the doubles category.** This assumption of our **turned out to be correct**, because based on the results of the observed 4-4 match, it can be said that in the singles category, the density of the number of contacts per player is higher than in the doubles category, based on one minute of net time. Players have more contact with the ball more when playing singles than when playing doubles. During singles matches, an average of 20-28 touches could be measured in one minute of net playing time, while in the doubles category, players used only 9-14 touches. Furthermore, while observing the matches, it was noticeable that in doubles the teams already arrange themselves for different tactics in advance and most often divide the roles among themselves. It is worth noting that in Szalkai's 0 studies, women had much lower numbers of touches than men, this has clearly changed nowadays. Based on efficiency and also because of the attitude, it is common when there is a more attacking and a more defensive side within a pair. In this case, the attackers touch a large percentage of the same part of their body during a rally, while during the singles game,

in order to comply with the rules, different body parts are touched several times. This means that the player who practices the singles more often can have a larger technical repertoire. **We assumed that it was mentally more difficult for a teqball player to play a match in the singles category than in doubles.** During our investigations, we asked teqball players through a questionnaire, and with the help of in-depth interviews, we tried to map the correctness of our assumption. Based on the results, this **did not turn out to be correct**, since after evaluating the answers, most of the contestants mentally put the playing of a singles and doubles match on the same level, there is no significant difference. We can only support this with the interviews, where our subjects emphasized that although you have to prepare a lot for the singles, the mental factors are just as important in the doubles. For a player, different, complex factors arise during the match. This was justified by the fact that communication between them is very important, so that the chemistry works well, you can motivate the player, or you can lift your partner up if he is mentally down. It is a complex question, but we think this ability is essential for a player in both categories.

Summary

The sport of teqball suddenly exploded into the public consciousness and became popular worldwide. More and more people are dealing with it both as a hobby and competitively as well, and hopefully we will soon be able to meet this Hungarian invention at the Olympics. The aim of our thesis was to examine the role the singles category plays in the life of teqball and in the development of a youth player. In our thesis, we examined teqball players based on mental and technical aspects through questionnaires, measurements, we presented the density of contact numbers through match analysis, and with the help of in-depth interviews we got a clearer picture of our hypotheses. We presented the results using tables and figures, where we got clearly visible results. After the tests, the results show that the singles category is of great importance in terms of technical development, as it helps the player to a great extent not only physically and mentally, but also technically. Furthermore, in the doubles category, mental preparation also plays a big role, and due to certain factors, it is sometimes more difficult to play a match in this category. Training for singles is important in the preparation of a youth player, so we recommend it to all teqball players who want to take up the sport more seriously, but doubles is just as important to competitive sports.

References

[1] Négyesi, I; Tóth, J. (2022): AI and Sports. American Journal of Research Education and Development 4. pp. 35-43.

[2] Bognár J. (2009): Tanulmányok a kiválasztás és a tehetséggondozás köréből. Budapest.

[3] Tóth, J; Dósa, A. (2022): The study of the Hungarian Sport University's football team from the aspect of technical movements. American Journal of Research Education and Development 4. pp. 12-18.

[4] Tóth, J; Oros, Zs; Prukner, L. (2020): Analysis of the extra time of matches in the knockout phases of the Campions League and the Europa American Journal of Research Education and Development 2. pp. 25-35.

[5] Reilly T, Williams A. M, Richardson D. (2003): Science and Soccer. London.

[6] Réthy E. (1999): Motiváció: felfogások, elképzelések, hitek. Budapest.

[7] Atkinson C. R, Hilgard E. (2005): Pszichológia. Budapest.

[8] Kozéki B. (1975): Motiválás és motiváció. Tankönyvkiadó, Budapest.

[9] Deci L. E, Ryan M. R. (1985): Intrinsic Motivation and Self-Determination in Human Behavior. New York.

[10] https://www.teqballhungary.hu/teqball

[11]Szalkai K. (2016): A Teqball sportág bemutatása technikai elemek szempontjából. Budapest, Dissertation.

Changes in playing minutes of foreign players in Hungary and Central Europe.

János Tóth jr., Levente Virág

Hungarian University of Sports Science, Football Research Institute.

Abstract

In the first division of Hungarian football, the proportion of playing time of foreign athletes has increased significantly. This assumption is confirmed by the fact that since the NB1 was reduced to twelve teams, the time spent by foreign footballers on the field has increased every year. While the ratio was 70.8% - 29.2% in the 2015/16 season, it rose to 49.8% - 50.2% in the 21/22 season in favor of the legionnaires. In the last season, Vasas FC and Paksi FC, which have been employing only domestic footballers for many years, are positive examples.

A counterexample is Kisvárda FC, which provides 90.6% of the total playing time to foreign players. In my opinion, it is extremely difficult for the talented Hungarian footballers coming out of the academies to get into the topflight under these conditions.[1]

Keywords

Football, foreign players, playing minutes

Introduction

My interest in my topic was aroused by the fact that it is visible to the eye that the playing time of foreign players in the first division of Hungarian football increased. An increasingly frequent subject of discourses about our football is questions the validity of signing a foreigner in certain cases.

Since I work as a youth coach, I consider it a matter of my heart that as many Hungarian children as possible should be able to play sports at the highest possible level, which helps a

long-term development of our football, creating a strong hinterland in the future for the national team.

Previously, the government declared sport a national strategic sector, thereby huge sums have flowed and are flowing into our football. It can be stated that the corporate tax grants within its

framework are worth a lot and are a great help for sports associations, as long as they are placed in the appropriate places.

In my research, I am looking for the answer how the legionnaires and the domestic players formed the ratio of playing minutes of our players in the past period, and what trends can be observed in other Central European countries, compared to the Hungarian data. My above-mentioned suggestion is confirmed by the fact that since the narrowing of NB1 to twelve teams, the time spent by foreign footballers on the field has increased year by year. For the creation of these trends the fact that MLSZ canceled restrictions of number of legionnaires in the 2020/2021 season probably had a stimulating effect.

According to Giulianotti R. and Robertson R, we understand modern football more as a representation of globalization. Important conditions for its spread are its simple rules and relatively low equipment costs.[2]

Based on the research by Balogh and Bába, Hungarian football has undergone significant development since 2010 (infrastructure, number of active football players). The OTP Bank League (NB1) was compared with the Czech Fortuna League, along various variables (UEFA coefficient, size of player squads, actual size of player squads, average age of player squads, proportion of foreign legionnaires, average market value of players, transfer balance of leagues). Based on their research, it can be said that the Hungarian championship failed to show progress between 2010 and 2020, if we take the ranking of the championships as a basis. Looking at the average ages, it can be concluded that both leagues typically use players under the age of 25 based on the composition of the squads. OTP Bank League clubs can be said to be unprofitable in terms of player transfers, as they spent more on players than they were able to sell in several seasons checked. The Czech first-class teams prefer to participate in the player market (they use a transfer strategy) as sellers, thereby gaining significant income, in contrast to the behavior of Hungarian teams as buyers.[3]

The "top 5" leagues were investigated by Poli, Ravenel and Besson. Until 1985, the proportion of foreign players never reached 10%. From that year onwards, there has been a steady increase. The biggest increase happened in the 1995/96 season (before the Bosman rule) and the 2000/2001 season, where the number of foreign footballers rose from 18.6% to 35.6%.[4]

Péter Benedek and Andrea Gál emphasize that player migration became more intense after joining the European Union in 2004. Primarily, individual clubs sign legionnaires in the position of inside defender or striker. Despite significant private and state grants, not many Hungarian players reach the level of being able to sign contracts abroad, and the demand for them has dwindled recently. In terms of football migration, Hungary can be considered more of a receiving country than a donor country (therefore, there are many more "imported" football players from abroad than our domestic "exported" football players abroad). Their research revealed that Hungarian clubs often look for players who can be signed cheaply or can be acquired for free, so it is common for players with weak skills to enter the National Championship (NB1).[5]

In his research, Csécs examined the operating system itself, which takes place within the framework of the Hungarian Football Association (MLSZ). The player base is following a growing trend, and more and more associations are applying for the grants provided within the framework of the corporate tax. He emphasizes this type of support must remain, because this is the only way to ensure the development of the sport at a sufficient pace (youth training, infrastructural developments, quality education of sports experts).[6]

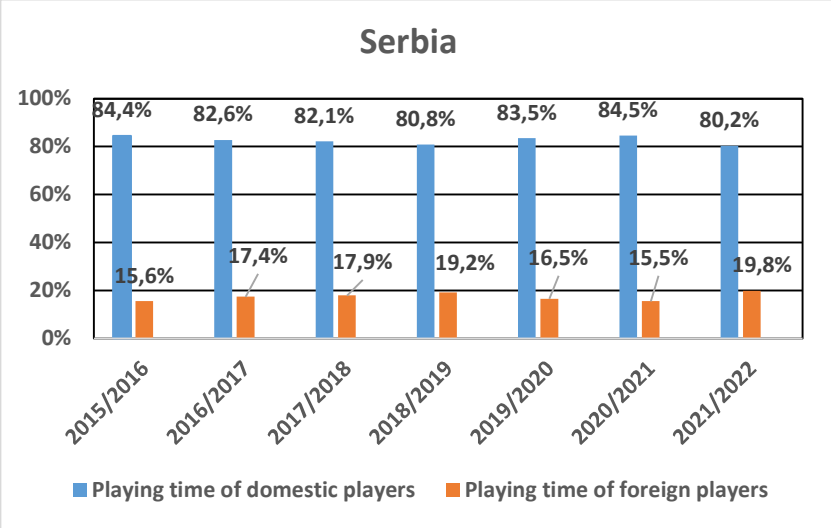
Methods

Playing possibilities (in minutes) of domestic and foreign players of first-class clubs in countries which have a similar economic situation and geographical location like Hungary are compared.

Countries examined: Austria, Slovenia, Slovakia, Czech Republic, Ukraine, Serbia, Romania, Croatia and Hungary.

A linear regression model was adjusted to the annual evolution of foreign player minutes. At the evaluation of results, a significance level of 5% was used.

Results

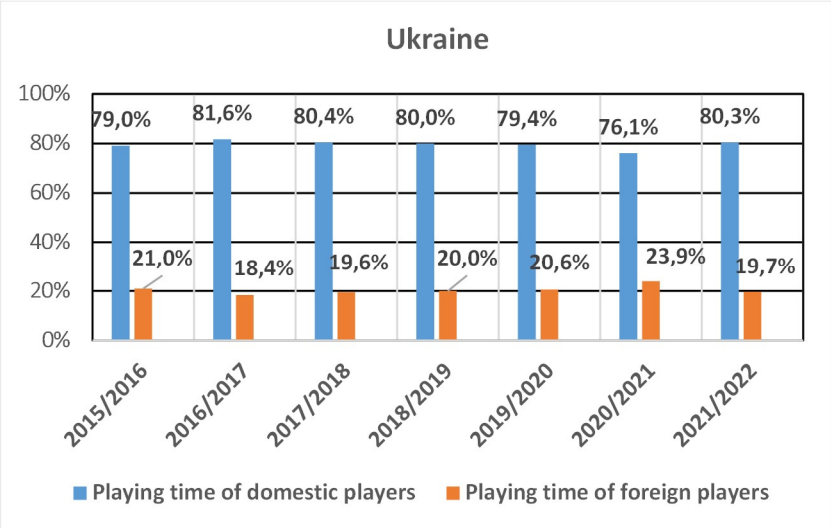


1. Figure: Playing minutes of Serbia

In the case of Serbia, domestic players received more than 80% of playing minutes in all the examined years, in terms of playing time ratio.

Number of championship teams: 16 teams.

Matches per team: 30 matches.



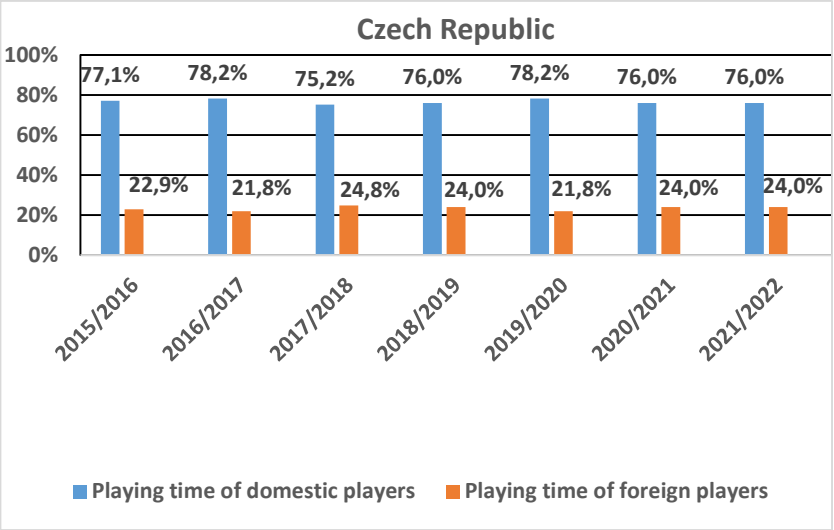
2. Figure: Playing minutes of Ukraine

Regarding Ukraine, the ratio of domestic playing time is also high, also around 80%.

A significant drop, was seen only in the 2020/2021 season.

Number of championship teams: 16 teams.

Matches per team: 30 matches.



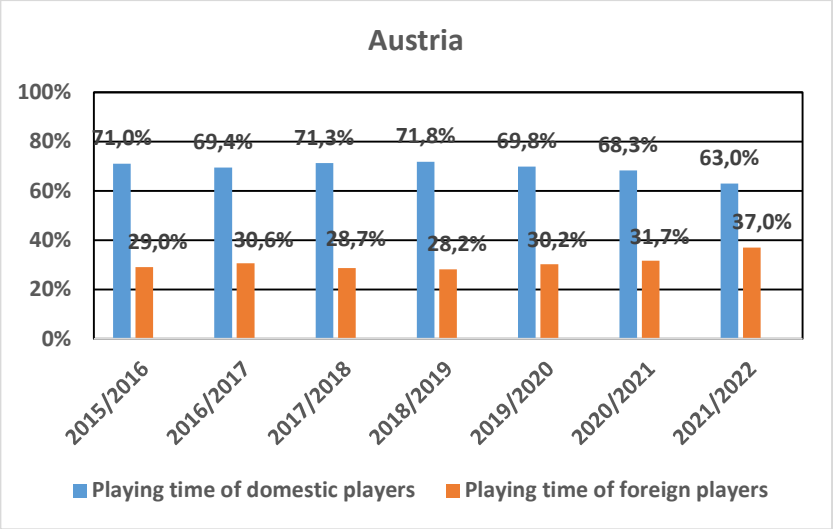
3. Figure: Playing minutes of Czech Republic

In the Czech Republic, the rate is high, around 75%.

In every examined year, over 75% of playing time was given to domestic players.

Number of championship teams: 16 teams

Matches as a team: 30 matches

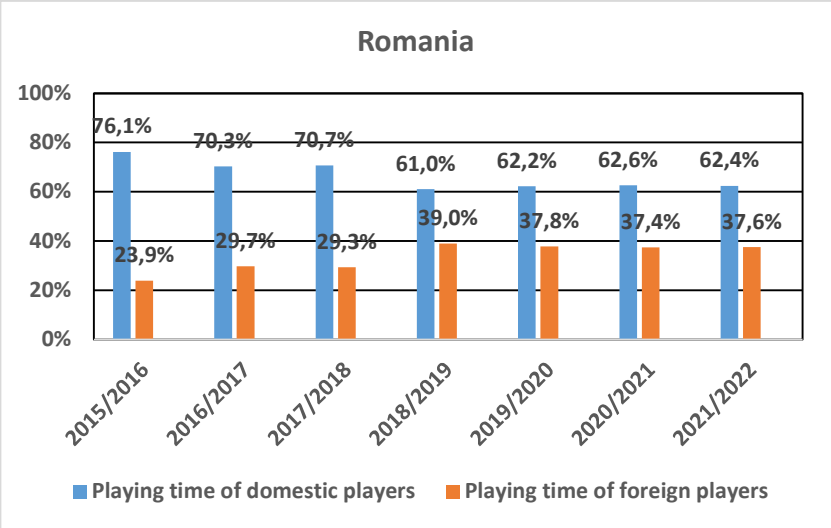


4. Figure: Playing minutes of Austria

In the case of Austria, the playing time ratio fluctuated in the first six examined seasons, and then in the last examined season the playing time ratio of the domestic players decreased significantly.

Number of championship teams: 12 teams.

Matches per team: 22 (+ lower-upper house).

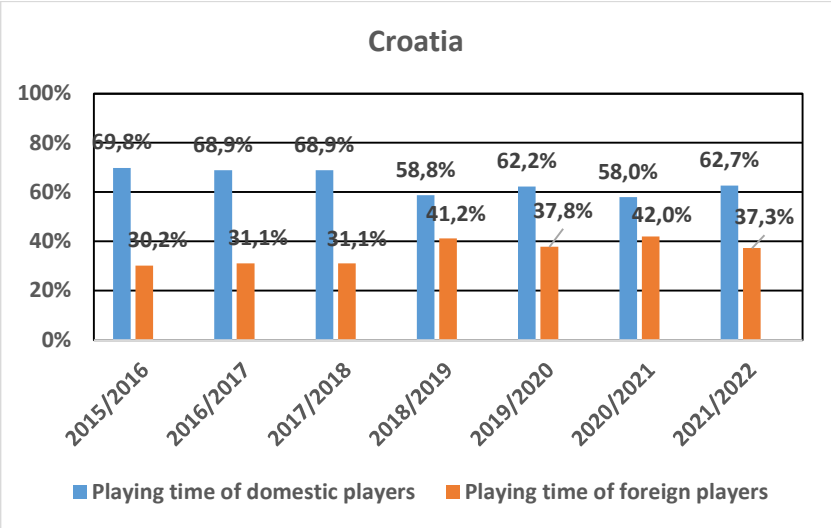


5. Figure: Playing minutes of Romania

In connection with Romania the 2018/2019 season has to be highlighted, where a bigger amount of decrease can be seen regarding the previous year (Apart from Romania in the same year the same amount of decrease was experienced in terms of playing time of domestic players in two other countries.

Number of championship teams: 16 teams.

Matches per team: 30 (+ lower-upper house).

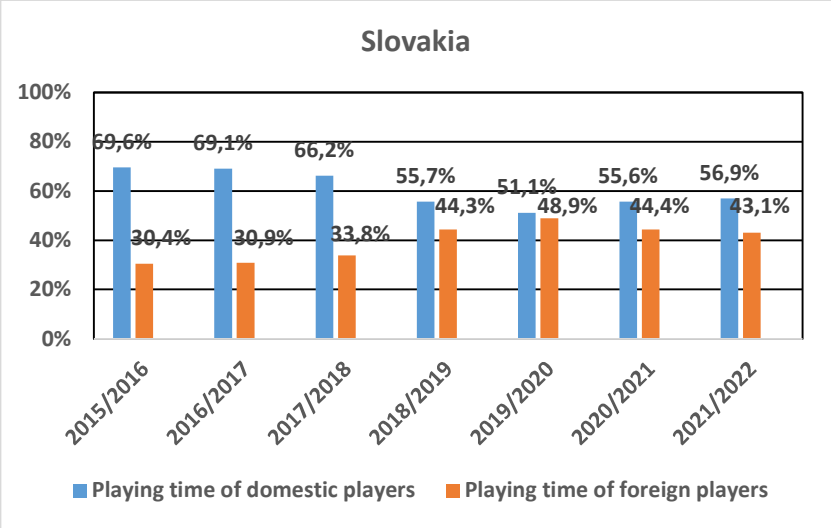


6. Figure: Playing minutes of Croatia

Croatia is the next country where in the year of 2018/2019 there was a decline similar to Romania (around 10%) in the playing time ratio of domestic players.

Number of championship teams: 10 teams.

Matches per team: 36 matches.

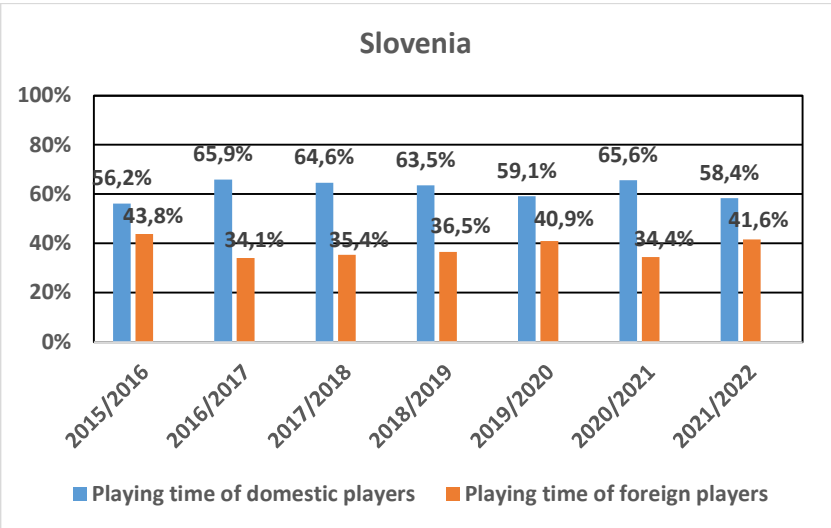


7. Figure: Playing minutes of Slovakia

Slovakia is the third country where the mentioned "bigger" decline in the proportion of domestic players' playing time was experienced in the 2018/2019 season.

Number of championship teams: 12 teams.

Matches per team: 22 (+lower-upper house).



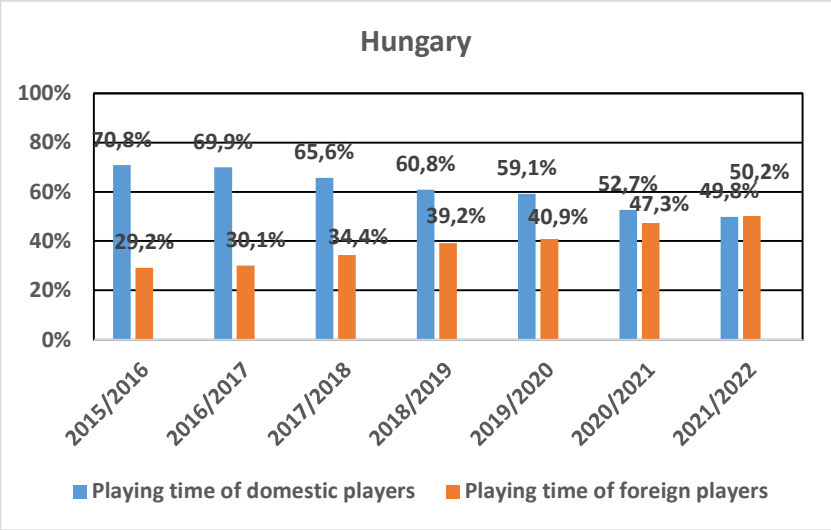
8. Figure: Playing minutes of Slovenia

Looking at Slovenia, we can discover a continuous fluctuation in the proportions, in all seven years examined.

Slovenia is the only country among the examined countries where the playing time ratio of domestic players is higher in the last examined season (2021/2022) than in the first examined year (2015/2016).

Number of championship teams: 10 teams.

Matches per team: 36 matches.



9. Figure: Playing minutes of Hungary

Hungary is the only country among the examined countries where the proportion of domestic players' playing time is constantly decreasing.

In the 2015/2016 season, the ratio was 70.8% - 29.2%, for the 2021/2022 season it became 49.8% - 50.2%.

Based on the mentioned data, it can be stated that only in Hungary foreign players get more playing time than domestic players among the countries examined.

Number of championship teams: 12 teams.

Matches per team: 33 matches.

Country	Axle section difference	Axle section difference p value	Slope difference	Slope difference p value

Austria	54,839	0,001	-0,027	0,001 *
Czech Republic	71,341	< ,001	-0,035	< ,001 *
Croatia	38,961	0,018	-0,019	0,018 *
Romania	27,983	0,084	-0,014	0,083
Serbia	69,335	< ,001	-0,034	< ,001 *
Slovakia	17,087	0,286	-0,008	0,287
Slovenia	75,236	< ,001	-0,037	< ,001 *
Ukraine	68,861	< ,001	-0,034	< ,001 *

1. Table: statistical data about certain countries (created by the author)

The playing minutes of foreign players show an increasing trend between the seasons of 2015/2016 and 2021/2022 in the examined countries ($F(1;61)=6.10;p=0.016$). Taking all countries into consideration, the regression line of the trend is as follows: -27.421 + 0.014 * the start year of the season. By examining Hungary, we get the following regression line: -74.495 + 0.037 * the start year of the season. Analyzing the other examined countries regarding Hungary, we see that Hungary has the steepest trend. Among the examined countries, The growth rate of Romania and Slovakia does not differ from Hungary's, so it in these countries and in our country, the rising of playing minutes of foreign players is the biggest.

Summary and conclusions

As a summary, it can be said that playing minutes of foreigners is constantly increasing year by year in the domestic first-class league, which can become one of the biggest problems in our football in 21st century.

Based on the data, it can be stated with 100% certainty that the 2015/2016 reduction of first-class clubs in the season (from 16 teams to 12 teams) had no positive effect on playing opportunity of the Hungarian, and within that, the young Hungarian footballers, the teams visibly started to prefer the "ready" foreigner football players, in order to achieve the desired better result.

I believe that we can sow the seeds of a different approach, which gives more opportunities for domestic players. However, for this the widely used so-called circle of success strategy by the Hungarian clubs must be rejected, which means that the clubs make a preliminary investment to achieve a better result, which will later generate profit for them.

In Romania, as of the current season, a maximization was introduced in terms of the number of legionnaires, which means that at least 40% of the players on the pitch must be Romanian citizens, it is conceivable, this can be a workable way for the Hungarian championship which can serve as an example.

References

(1) Transfermarkt: Football transfers, rumours, market values and news - 2022. october 3. Available: https://www.transfermarkt.com/, 2022. october 3.

(2) Giulianotti R., Robertson R. (2004). The globalization of football: A study in the glocalization of the “serious life.” The British Journal of Sociology, pp. 545–568. https://doi.org/10.1111/j.1468-4446.2004.00037.x

(3) Balogh R. és Bácsné B. É. (2021). A magyar labdarúgó-bajnokság fejlődésének elemzése a játékospiacon keresztül. Regiokutatas Szemle, 6(1).

(4) Poli R., Revenel. L., Besson R. (2016). Foreign players in football teams. CIES Football Observatory Monthly Report Issue no. 12

(5) Négyesi, I; Tóth, J. (2022): AI and Sports. American Journal of Research Education and Development 4. pp. 35-43.

(6) Rikk János: Kutatásmódszertan; Budapest, Szerzői kiadás, 78 p. (2014), ISBN: 9789630894951

(7) Péter B. és Gál A. (2016) "Idegenlégiós futballisták itthon és külföldön: a hivatásos magyar labdarúgás migrációs csatornáinak azonosítása és elemzése." Utánpótláskorú sportolók 5.

(8) Csécs, M (2023). A magyar labdarúgás fejlődése. Dissertation.

Implications of Relevant Attributes and Characteristics of Nuclear Facilities for their Physical Protection Systems

Muhammad Khaliq Nuclear and Radiological Regulatory Commission (NRRC) Riyadh, Kingdom of Saudi Arabia mkhaliq56@gmail.com 0000-0001-6391-2531

Abstract

The recommended requirements of the International Atomic Energy Agency (IAEA) Nuclear Security Series (NSS) publications do not provide specific guidance for the different types of nuclear facilities, these are generally applicable at nuclear facilities. The evaluation of the applicability of these recommended requirements to any facility type requires the assessment whether and how the nuclear security relevant attributes and characteristics of the different types of facilities influence the physical protection systems and measures of these facilities. The publication systematically identifies and describes the elements of the physical protection systems and measures of nuclear facilities as recommended by the IAEA NSS publications, and then provides an assessment of the implications of the nuclear security related attributes and characteristics therefor.

Keywords: nuclear security, nuclear facilities, security relevant characteristics, IAEA, physical protection, physical protection systems and measures

Corresponding authors:

Kristof Horvath, International Atomic Energy Agency, dr.kristof.horvath@as-services.hu 0000-0001-8979-9995

Jozsef Solymosi, National University of Public Service, Faculty of Military Science and Officer Training, Professor Emeritus, jozsef.solymosi@uni-nke.hu 0000-0003-3737-1932

Mate Solymosi, mate.solymosi@somos.hu 0000-0002-6302-0370

Introduction

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorised access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the publications of IAEA Nuclear Security Series.

IAEA Nuclear Security Series No. 13 [1] requires the consideration of specific facility characteristics when implementing physical protection.

Answering the question whether operators of different nuclear facilities would need to take account of the specific relevant characteristics of their facilities when implementing IAEA recommended requirements includes the identification of the nuclear security relevant attributes and their characteristics and the identification of the elements of a physical protection system of nuclear facilities, and the assessment whether and how these relevant attributes affect the physical protection system elements.

Attributes of Security Relevance

The different types of nuclear facilities with regard to the implementation of physical protection measures can be characterised according to the following attributes [2]:

- Security vulnerabilities inherent in design and operational practice;
- Specific safety design;
- Attractiveness of material;
- Colocation with other facilities;
- Openness of access, exchange of information;
- Variety of uses;
- Funding;
- Regulatory and operator issues;
- Site location;

- Facility ageing;
- Number of employees;
- Public acceptance, rejection;
- Potential radiological consequences;
- Complexity of the site;
- Specific nuclear material accounting and control requirements.

Early Consideration of Physical Protection in Site Selection and Design of a New Facility - Security by Design

For a new nuclear facility, the physical protection aspects should be taken into account as early as possible from both points of view: how the elements of the future physical protection system (e.g. physical barriers, detection devices, off-site response capabilities) would affect the site and the design of the plant, as well as how the site characteristics (e.g. complexity, topography, geology, meteorology, extreme water levels, use and population of nearby area), and the future design of the plant (e.g. size, accessibility, sabotage targets) would affect the realisation of the elements of the physical protection system. Integration of the design of the physical protection system into the overall design of the nuclear facility is also called as security by design. [3]

Security by design is an overall principle, it affects each elements of the physical protection system and thus it is affected by every security relevant attributes. The assessments made in the below sections should be all integrated when implementing this principle.

Development and Implementation of the Physical Protection System

The operator has primary responsibility for the development and implementation of the physical protection system for the nuclear facility. The operator should prepare a facility specific security plan describing the entire physical protection system, including the physical protection measures that is the basis for the licensing of the nuclear facility by the State, and implementation of the

security plan is a condition of the licence to conduct operations at the nuclear facility. [1]

Identify the objectives and requirements / Risks to be taken into consideration

The physical protection requirements to protect against both the unauthorized removal of nuclear material and sabotage should be implemented in an integrated manner, implying that the physical protection system should be a single system, effective against both threats. It is recommended designing the physical protection system in a manner that will ensure effectiveness against whichever risk, unauthorized removal or sabotage, requires the more stringent physical protection requirements. For an integrated approach to the implementation of physical protection, the operator of a nuclear facility identifies all potential targets for unauthorized removal and sabotage and implements all the required protection measures in a graded manner. Depending on the type of nuclear facility, either the sabotage or the unauthorized removal targets may require a higher level of protection, but in all cases the appropriate levels of protection should be implemented for all targets.

Target identification

The operator should identify both the targets for unauthorised removal and sabotage. Therefore, all nuclear and other radioactive material material used and stored in the facility should be categorised. Furthermore, if the potential radiological consequences of sabotage exceed the State's threshold for unacceptable radiological consequences, then the operator should identify as potential sabotage targets the structures, systems and components, and/or the nuclear material, the sabotage of which could directly or indirectly lead to such radiological consequences. As a result, the operator should develop a target list for the facility, including a description of each target to be protected, its category and location. [4]

Security vulnerabilities inherent in design and operational practice, the specific safety design, the attractiveness of the material and the potential radiological consequences, the openness of the facility and the variety of its use are all significantly impact the result of the target identification; however, the process itself follow the same methodology.

Threat assessment and definition

As part of the identification of the objectives and requirements for the physical protection system, the threat to the facility should be defined by the State by developing a design basis threat. Relevant information should be provided to the operator, who should use this information as a basis for designing and evaluating its physical protection system. [5]

The threat assessment process does not depend on the type of the facility. However, its result may depend on the co-location of other facilities on the site or adjacent to, the location of the site whether it is close to populated areas, potential adversary routes or far from off-site response, as well as the supportive or rejecting opinion of the public mainly regarding demonstrations against the facility.

Design/re-design of the physical protection system

Physical protection system designers will need detailed knowledge of processes and operations within the facility, locations of the facility boundary and buildings, floor plans, structure elevations and access points, and, for an existing facility or design, identifying existing features or systems that may be used as elements of the physical protection system, as well as any facility specific constraints (such as safety constraints) that may be encountered during design. The next step is to design the new system or redesign the existing system to provide physical protection measures for detection, delay and response sufficient to meet the objectives of the system, taking into account the principles of defence in depth, balanced protection an robustness. After the physical protection system is designed

or characterized, it should be analysed and evaluated to ensure that it meets the physical protection requirements. [3]

The design or re-design process of the physical protection system should take into account all specific security attributes; however the process itself follows a standard methodology.

Defence in depth

Defence in depth means that the adversary needs to deceive, avoid or defeat several protection measures in sequence to succeed. Defence in depth is generally implemented by placing a series of layers of protection around targets, which may include a combination of physical measures and administrative measures. This approach may involve taking advantage of the strengths of each physical protection component and using equipment in combinations that complement the strengths or compensate for the limitations of each other.

Balanced protection

Balanced protection means that the adversary encounters comparably effective measures of the physical protection system whenever, wherever or however the malicious act is attempted. A balanced design includes balanced delays for the different adversary paths and scenarios, and physical barriers are carefully planned to fit the particular location and are positioned in the path of the adversary.

Robustness

Robustness means that the physical protection system will have a high probability of operating effectively during a wide range of types of adversary attack, which is typically accomplished by incorporating redundancy and diversity into the design. For detection and assessment systems, robustness can be achieved by a combination of multiple complementary sensors and human surveillance.

Key security functions

The physical protection system meets physical protection requirements and accomplishes physical protection objectives by deterrence and a combination of detection, delay and response. The physical protection system might be evaluated as effective, if the delay provided after detection is sufficient for response. [3]

The key security functions are the same in every nuclear facility. Nevertheless, the actual realization of these functions is highly dependent on several security relevant attributes. The security vulnerabilities inherent in design and operational practice as design features may not support nuclear security, the specific safety design may provide robustness against malicious acts, the site location and the complexity of the site may require specific equipment for detection and delay, the ageing of the physical protection system may jeopardize the effective realization of detection and delay, while strict nuclear material accounting rules may support the detection function against insider threat.

Deterrence

Deterrence is achieved if potential adversaries regard a facility as an unattractive target and decide not to attack it because they estimate the probability of success to be too low (or the potential negative consequences for themselves to be too high). To promote deterrence the operator may use observable protection measures, such as a visible presence of guards patrolling the facility, bright lighting at night, bars on windows and vehicle barriers.

Detection

Detection is a process in a physical protection system that begins with a potentially malicious or otherwise unauthorized act or the presence of an adversary being sensed and an alarm being raised. The process is completed when the cause of the alarm has been assessed. The detection function depends on the capabilities of the systems for sensors, alarm signal activation, alarm reporting and assessment, as well as the performance of the staff of the central alarm station and any guards

or response force members who have a role in detection. Technology can increase the efficiency of all stages of the detection process. Where technology is used, the detection system should employ sensors and video systems to provide data on sensing and assessment.

Delay

Delay is the function of the physical protection system that seeks to slow an adversary's progress towards a target, thereby providing more time for effective response. Delay can be accomplished simply by distances and areas that have to be crossed and by barriers that need to be defeated or bypassed, such as fences, gates, portals, doors, locks, cages and activated delay systems. Barriers may deter or defeat adversaries if they are unable to penetrate the barrier. Each type of barrier takes time for the adversary to penetrate or defeat. These delay times are factors to be considered when designing the physical protection system. Guards or response forces may provide further delay if they are appropriately positioned, armed and protected.

Response

Response is the function of the physical protection system that seeks to interrupt and neutralize an adversary before the completion of a malicious act.

Physical Protection System Elements

The physical protection system compose of various measures and elements aimed to ensure the key security functions taking account of the objectives and design principles.

Protection areas

Protection areas are physically separated and each having its own protection layer, including detection, delay and response measures. [6]

Protection areas should be designated taking into consideration the safety design of the facility, the attractiveness of the material used and stored within the facility, as well as the potential radiological consequences of a successful sabotage.

Central Alarm Station

A central alarm station is recommended for any nuclear facility holding Category I and II nuclear material and/or having sabotage targets with potential consequences above the high radiological consequences threshold. An alarm communication and display system is a primary component of the central alarm station that facilitates the monitoring and assessment of alarms at the central alarm station. [3]

The equipment of the central alarm station is highly dependent on the available funding, while slightly dependent on the established physical protection system, but its installation follows a standard approach in nuclear facilities.

Physical barriers

Physical barriers should be placed such that an adversary is delayed by the need to defeat or bypass them, thereby allowing the response forces sufficient time to interrupt the adversary before completion of a malicious act. The degree of delay depends on the nature of the barriers employed. Multiple layers of different types of physical barrier along all possible adversary paths, consistent with the threat assessment or the design basis threat, are suggested as ways to complicate and therefore delay the adversary's progress by requiring — in addition to increased time — the use of a variety of tools and skills. In addition, to minimize the probability of any secured area being breached, vehicle barriers can be designed and installed in appropriate locations on land and water. [3]

The placement of physical barriers should consider the safety design of the facility and its operational needs.

Access control systems

Access control systems comprise the equipment, people and procedures used to verify entry authorization and to control the movement of people and material into and out of each area. Access control systems are used to manage who is allowed to enter, when they are allowed to enter and where the access can occur, as well as to apply conditions for authorized entry. Access control systems can be designed to support the smooth and continual entry and exit of authorized persons, material and equipment via normal routes while detecting and delaying the movement of unauthorized persons and prohibited items. [3]

The solution selected for access control should take into account the number of employees and visitors in the facility.

Response forces

The response forces need to be able to interrupt and neutralize an adversary that has the resources and capabilities described in the threat assessment or the design basis threat. Interruption begins with communication to the response force that a potential adversary has been detected and is completed when a sufficient number of appropriately trained and equipped members of a response force arrive at the appropriate location in time to stop the adversary completing a malicious act. Neutralization is the act, following interruption, of gaining control of adversaries before their goals are accomplished or otherwise causing the adversaries to abandon the attempt. To be reliable in achieving effective neutralization, the response force needs to be superior to the adversary in terms of numbers, equipment and/or training. [3]

The equipment provided to the on-site response force is highly dependent on the available budget; their human resources should be proportional with the size, location and complexity of the site. Off-site response are typically provided the state organisation; thus good cooperation between the operator and the competent authority providing off-site response is a must.

Protection measures for stand-off sabotage attacks

Protection measures that may protect against or mitigate the consequences of a stand-off attack include: increasing the distance from the facility within which a stand-off attack could be attempted so as to exceed the range of weapons the adversary might use; obscuring lines of sight to the target from areas from which stand-off attacks might be attempted; increasing detection and deterrence through off-site patrols and surveillance; using barriers capable of intercepting missiles or absorbing blasts or fragments; modifying layouts of facilities to protect sensitive targets; hardening facilities to resist such attacks. [4]

The potential of a stand-off attack is dependent on the site location. As the effective protection against it may require off-site actions, thus the cooperation with the competent authority necessary.

Protection measures for airborne and water-borne attacks

Radar, acoustic and seismic sensors can all provide some detection capability for airborne attacks but need to be carefully located to provide good coverage with few nuisance alarms. Some types of aircraft may be prevented from landing at the site of a nuclear facility because of the facility's small and/or congested area. This effect may be enhanced by the strategic positioning of poles or other physical barriers. [4]

The potential of an air-borne or water-borne attack is dependent on the site location. As the effective protection against it may require off-site actions, thus the cooperation with the competent authority necessary.

Compensatory measures

Whenever the physical protection system is determined to be incapable of providing the required level of protection, the operator, shipper and/or carrier should immediately implement compensatory measures to provide adequate protection. Compensatory measures are short term actions taken to compensate

for degraded or inoperable security related structures, systems and components until they can be repaired or replaced. [7]

The need for and extent of compensatory measures grows with the ageing of the facility, as more system components may require

Transport of nuclear material

The operator of a nuclear facility, as the shipper or receiver, has certain responsibilities for providing advance notification of planned shipments, searching conveyances, protecting the confidentiality of transport information, checking the integrity of packages on arrival and notifying the shipper of such arrival, and making prior arrangements with the carrier concerning the transfer of physical protection responsibilities. [8]

The implementation of security measures depends on the location of the site and the routes used for approaching it. The public rejection may require more robust security arrangements.

Evaluation of Effectiveness

The effectiveness of the physical protection system should be evaluated in order to verify that the physical protection system as designed, or as characterized (for an existing system), satisfies the physical protection requirements; to identify any system deficiencies; to analyse possible upgrades that may be necessary to address identified deficiencies and improve system performance.

Appropriate parts of this evaluation and testing should be considered throughout the lifetime of the nuclear facility (i.e. during design, construction, licensing, operation, changes or upgrades, and decommissioning and management of radioactive waste and spent fuel).

Evaluations may include path analysis and simulations, and regular performance testing and appropriate exercises to test the guards and response forces. [9]

The effectiveness evaluation, especially the performance testing needs sufficient funding, support from the competent authorities and the nearby population.

Sustaining the Physical Protection System

After its implementation, the physical protection system should be operated, maintained and sustained. Accordingly, operators should ensure that the necessary resources, including trained and knowledgeable personnel, reliable equipment, associated infrastructure, quality assurance and funding are provided. The sustainability programme should encompass security procedures, operating procedures (instructions), human resource management, training and qualification, equipment updating, maintenance, repair and calibration, performance testing and operational monitoring, configuration management, and ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation. Comprehensive written procedures should cover, among others, structure of the physical protection organization, duties of all physical protection staff, duties for all security posts, employee, visitor and vehicle access and egress control, searches, patrolling, shift turnover, testing and maintenance, event reporting, incident response. In order to ensure confidence in the physical protection system elements, quality assurance policy and quality assurance programmes should be established and implemented. [10]

The sustainability programme should be facility specific and should impact every element of the physical protection system; nevertheless the development and the implementation of the programme is based on similar elements. The scope of the programme is strongly dependent on the available funding, its realization becomes more complicated with ageing system components, and it may get greater attention from the operator, if it is taken seriously by the competent authorities.

Security Organization

The security organisation having responsibilities for physical protection related duties may be divided into three complementary units: a security management unit that has the overall responsibility for physical protection, a security operations unit that is responsible for security relating to personnel and visitors, information security, computer security, and the guards and response forces, and a technical security unit that includes technical staff — who conduct installations and upgrades, performance testing, preventive maintenance, unscheduled repairs and replacement. [3]

The size of the security organisation is highly dependent on the complexity of the physical protection system that is in line with the attractiveness of the material and the potential radiological consequences, the variety of uses of the facility, the site location, the ageing of the system, the number of employees, and the complexity of the site.

Nuclear Security Culture

Security Culture means all organizations involved in implementing physical protection should give due priority to the security culture; to its development and maintenance necessary to ensure its effective implementation in the entire organization. The human factor is generally a contributor to all nuclear security related incidents as well as malfunctions related to activities involving radioactive material, including deliberate malicious acts, unintentional personnel errors as well as ergonomic issues related to the design and layout of software and hardware, inadequate organizational procedures and processes and management failures. Nuclear security culture refers to the personal dedication and accountability and understanding of all individuals engaged in any activity which has a bearing on the security of nuclear activities. The characteristics of nuclear security culture are the beliefs, attitudes, behaviour and management systems, the proper assembly of which leads to more effective nuclear security. [7]

Accordingly, nuclear security culture is an overall concept that affects the entire physical protection system. The characteristics and the measures aiming to enhance the characteristics can be generally determined; however a facility specific assessment may identify the areas for improvement [12, 13].

Establishment, assessment and enhancement of nuclear security culture, involving the human factor is highly dependent on the number of employees, and regulatory and operatory issues providing lower relevance for physical protection.

Insider Threat Prevention and Protection

In addition to external adversary threats, the physical protection system should be effective against threats meant by insider. An insider is defined as one or more individuals with authorized access to nuclear facilities or related sensitive information who could attempt unauthorized removal or sabotage or who could aid an external adversary to do so. Insiders may include managers, regular employees, contractors and service providers, inspectors and some visitors. The capabilities of an insider are typically defined by extent of authorized access, level of authority and knowledge. Insider threats present different problems from external adversaries because they can take advantage of these insider attributes to bypass some technical and administrative physical protection measures to commit or facilitate unauthorized removal or sabotage. Insiders can also complete their contributions to a malicious act through a series of separate actions over an extended period of time, which may reduce their chance of detection and therefore increase their likelihood of success. Insiders may also have more knowledge and/or opportunity to select the most vulnerable target and the best time to perform the malicious act. [3]

Preventive measures (e.g. identity verification, trustworthiness assessment, escort of infrequent workers, security awareness) are aimed to preclude or remove possible insider threats, or to minimize threat opportunities, or to prevent a malicious act from being carried out; while protective measures (e.g. security sensors,

monitoring of personnel, two person rule, tracking movement, physical barriers, event investigation, emergency planning) are aimed to detect, delay and respond to malicious acts that are carried out, and to mitigate or minimize their consequences. [14]

The preventive and protective measures against insider threat are highly dependent on the number of employees. These measures are supported by more stringent nuclear material accounting and control measures.

Security of Sensitive Information

Adversaries wishing to plan or carry out any malicious act involving nuclear material or nuclear facilities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with appropriate measures. Sensitive information is information, in whatever form (including software), the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security. Operators need to establish internal policies and procedures for protecting the confidentiality, integrity and availability of the sensitive information the operators hold or handle, in compliance with the national security policy and the relevant national laws and requirements. [15]

As the information classification system as well as the information protection regulations are established on national level and the sensitive information related to the physical protection system are very similar (i.e. threat documentation, security plan, design documentation, security instructions), thus the implementation of information security does not depend greatly on the security characteristics of the specific facility, if both the regulator and the operator take this issue seriously.

Protection of Computer Based Systems

The State has the responsibility to provide requirements on computer security and ensure that operators provide assurance that computers and computer based systems are adequately protected against cyber attacks. Operators have responsibility for implementing a computer security programme in compliance with

these requirements. The overall goal of computer security in the physical protection of nuclear material and nuclear facilities is to protect computer systems against attacks aimed at facilitating the unauthorized removal of nuclear material or sabotage. The operator is responsible for identifying those computer based systems that need protection against compromise so as to help prevent a successful adversary attack. The operator then needs to establish a computer security policy and its implementation plan. 16]

A cyber attack could have an immediate impact, causing damage to equipment or degradation in security functions, be ongoing, such as covert information collection, include a delay, producing a timed or separately triggered effect, and be synchronized with other adversary activities, which may include physical attack. Defence against such attacks needs to follow an approach based on defence in depth that uses technical, administrative and physical security controls. Computer security therefore needs to be integrated within the overall framework of the physical protection system. [17]

Computer based systems are widely used at nuclear facilities. The implementation of computer security measures at nuclear facilities follows the same principles and considerations. The ageing of computer based system makes them vulnerable to cyber attacks.

Safety-Security Interface

The physical protection interface with safety should be managed in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive [1].

The operator has primary responsibility for the safety of the nuclear facility and for physical protection measures at the facility. It is suggested that operators adopt, through their integrated management system, an integrated and coordinated approach to reviewing proposed changes before they are implemented to ensure that changes proposed for reasons related to safety or to physical protection do not

result in the unintended degradation of arrangements in the other area. When possible adverse interactions are identified, the operator will need to communicate them to appropriate personnel within the organization and consider alternative measures or take compensatory and/or mitigating actions. The operator needs to recognize safety-security interface issues and manage them appropriately during design, construction and normal operations, as well as during nuclear security events and emergencies, and during decommissioning. [3]

Security interface with safety may describe those safety measures, which support security (e.g. robust safety design, radiation detectors, including radiation portals at gates, safety analyses identifying sabotage targets) and those safety measures, which may challenge security (e.g. safety first principle, rapid evacuation, transparency). Safety interface with security may describe those security measures, which support safety (e.g. two person rule, tracking of transport) and those security measures, which may challenge safety (e.g. access/regress control in the case of an emergency, protection of information). Interface between safety and security may include those measures (e.g. emergency arrangements for the protection of the public, integrated management system, promotion of organizational culture), which are for the benefit for both safety and security.

The management of the safety-security interface requires a thorough approach; its implementation is similar in each nuclear facility based on its safety design.

Nuclear Material Accounting and Control

A nuclear material accounting and control system is designed to maintain knowledge of the quantity, type, location, use, movement and transformation of all nuclear material at a facility. The nuclear material accounting function provides deterrence against and detection of the unauthorized removal of nuclear material by maintaining an inventory of all nuclear material and its location. An effective nuclear material accounting and control system enhances the ability of the

operator to detect insider activities and to correctly assess any irregularity involving nuclear material, whether initiated by insiders or external adversaries. If nuclear material is removed from the facility, the nuclear material accounting and control system should be able to identify the quantity and characteristics of the nuclear material that has been removed. [3]

The elements of the nuclear material accounting and control system at facility level includes managing the system, records, physical inventory, measurements, nuclear material control, nuclear material movements, detection, investigation of irregularities, and assessment and performance testing. [18]

More stringent nuclear material accounting and control requirements support the effectiveness of detection of unauthorised removal of nuclear material.

Contingency Planning and Response

The goals of contingency planning are to ensure a timely and effective response at all levels to any nuclear security event involving a malicious act involving or directed at a nuclear facility and to maintain physical protection during other events, such as an accident involving a release of radionuclides, a medical emergency or a natural disaster. The correct actions need to be taken and decisions made at the right time to adequately respond to the event and resolve the situation. [3]

In developing a contingency plan to meet these goals, the operator should ensure that the contingency plan provides clear guidance for the actions that would need to be undertaken in the case of a nuclear security event: determining the credibility of the nuclear security event and the scope of potential consequences for the facility and personnel; activating appropriate response plans, personnel and resources to address the nuclear security event; taking appropriate actions to protect the facility and personnel and mitigate the consequences of the nuclear security event; ensuring that the ability to effectively implement the response plan is maintained throughout the nuclear security event; and determining

the criteria for the termination of nuclear security events so that operations can be restored.

The execution of the contingency plan may require the operator to conclude agreements with local law enforcement, national police, military and other organizations having role in responding to nuclear security events. Complexity of the site may require more complex attack scenarios and protection approach.

Locating and Recovering Missing or Stolen Nuclear Material

The operator should, depending on the State's legal and regulatory framework, perform a number of steps in support of measures to locate and recover missing or stolen nuclear material. The first step for the location and recovery of missing and/or stolen nuclear material is to detect that the nuclear material is not in its authorized location. After the operator has confirmed that nuclear material is no longer in its authorized location, the relevant competent authorities within the State should be promptly notified. In accordance with the contingency plan, the operator may then continue an on-site search for the material and may also initiate an off-site search, as appropriate, in coordination with the relevant competent authorities. All response actions should be conducted in accordance with the contingency plan and coordinated with the appropriate competent authorities. [3]

More stringent nuclear material accounting and control requirements support the effectiveness of detection of unauthorised removal of nuclear material. Complexity of the site may make an on-site search more complicated.

Mitigating or Minimizing Radiological Consequences of a Sabotage

The operator should prepare facility personnel to act in full coordination with guards, response forces, law enforcement agencies and safety response teams for implementing the contingency plans. Immediately following an act of sabotage, the operator should take measures to prevent further damage, secure the nuclear facility and protect emergency equipment and personnel. The operator should notify, in a timely manner, the competent authority, response forces and other

relevant State organizations of sabotage or attempted sabotage as specified in the contingency plan in order to start the implementation of the emergency plan. Response to the sabotage and response to a resulting emergency may involve actions in the same places and at the same time, but with different goals. Therefore, it is necessary for contingency plans and emergency plans to be complementary and jointly exercised regularly to help ensure their effectiveness and compatibility. Care needs to be taken to verify that activities of the response forces do not adversely affect safety and that physical protection is not adversely affected during the implementation of safety measures. [3]

The plans and their execution for mitigating and minimising radiological consequences requires support from the affected population and benefits from their support.

Conclusion

As it is shown by the below Table compiled on the basis of the compressive assessment, the various nuclear security attributes may have significant effect on certain elements of the specific physical protection system of specific nuclear facilities.

Elements and measures of the physical protection system	Nuclear security relevant attributes														
	1. Security vulnerabilities inherent in design and operational practice	2. Specific safety design	3. Attractiveness of material	4. Colocation with other facilities	5. Openness of access, exchange of information	6. Variety of uses	7. Funding	8. Regulatory and operator issues	9. Site location	10. Facility ageing	11. Number of employees	12. Public acceptance, rejection	13. Potential radiological consequences	14. Complexity of the site	15. Specific nuclear material accounting and control requirements
1. New facility - early consideration of physical protection in site selection and design / security by design	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2. Development and implementation of the physical protection system															
a. Identify the objectives and requirements / Risks to be taken into consideration															
i. Target identification / categorization	x	x	x		x	x							x		
ii. Threat assessment and definition				x					x		x	x			
b. Design/re-design of the physical protection system	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
i. Defense in Depth															
ii. Balanced Protection															
iii. Robustness – redundancy and diversity															
c. Key security functions	x	x							x	x	x			x	x
i. Deterrence															
ii. Detection															
iii. Delay															
iv. Response															
3. Physical protection system measures															
a. Protection areas		x	x				x						x		
b. Central Alarm Station															
c. Physical barriers		x			x						x				
d. Access control systems															
e. Response forces							x	x	x					x	
f. Protection measures for stand-off sabotage attacks								x	x						
g. Protection measures for airborne and water-borne attacks								x	x						
h. Compensatory measures										x					
i. Transport of nuclear material									x			x			
4. Evaluation of effectiveness							x	x				x			
5. Sustaining the physical protection system							x	x		x					
6. Security organization			x			x			x	x	x		x	x	
7. Nuclear security culture								x			x				
8. Insider threat prevention and protection											x				x
9. Security of sensitive information								x							
10. Protection of computer based systems										x					
11. Safety-security interface		x													
12. NMAC															x
13. Contingency planning and response								x						x	
14. Locating and recovering missing or stolen nuclear material														x	x
15. Mitigating or minimizing radiological consequences of a sabotage												x			

Table 1. Impact of nuclear security relevant characteristics on physical protection system elements

At the same time, the assessment also revealed that the physical protection system elements are identical in different nuclear facilities; and the concept and methodologies, even if their realisation and outcomes may differ, are applicable in general. Accordingly, the recommended requirements established for the physical protection of nuclear material and nuclear facilities are applicable to each types of nuclear facility; however, the implementing guides and technical guidance should provide methodologies that are able to consider the impact of the different characteristics of the various nuclear security attributes.

References

[1] International Atomic Energy Agency, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna, 2011.

[2] M. Khaliq, A. Hagemann, K. Horváth, J. Solymosi Nuclear Security Related Attributes and Characteristics of Different Types of Nuclear Facilities, Nuclear Security Related Attributes and Characteristics of Different Types of Nuclear Facilities- HADMÉRNÖK (1788-1919): 14 2019/3 pp 53-64 Paper DOI: 10.32567/hm.2019.3.5. (2019)

[3] International Atomic Energy Agency, Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna, 2018.

[4] International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna, 2007.

[5] International Atomic Energy Agency, Development, Use and Maintenance of the Design Basis Threat , IAEA Nuclear Security Series No. 10, IAEA, Vienna, 2009.

[6] International Atomic Energy Agency, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna, 2012.

[7] International Atomic Energy Agency, Security during the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna, 2019.

[8] International Atomic Energy Agency, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna, 2019.

[9] International Atomic Energy Agency, Preparation, Conduct and Evaluation of Exercises to Test Security Contingency Plans at Nuclear Facilities, IAEA Non-serial Publications TDL-008, IAEA, Vienna, 2018.

[10] International Atomic Energy Agency, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna, 2019.

[11] International Atomic Energy Agency, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna, 2008.

[12] International Atomic Energy Agency, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna, 2011.

[13] Csurgai, Jozsef & Solymosi, Mate & Kristóf, Horváth & Vass, Gyula. (2015). Nuclear Security Culture Self-Assessment in a Radioactive Material Associated Facility. Academic and Applied Research in Military and Public Management Science. 14. 265-273. 10.32565/aarms.2015.3.1.

[14] International Atomic Energy Agency, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna, 2008.

[15] International Atomic Energy Agency, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna, 2015.

[16] International Atomic Energy Agency, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna, 2011.

[17] International Atomic Energy Agency, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna, 2019.

[18] International Atomic Energy Agency, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, IAEA Nuclear Security Series No. 32-G, IAEA, Vienna, 2019.

ISSN 7234561-6